VIRGINIA COMMONWEALTH UNIVERSITY
BOARD OF VISITORS
AUDIT, INTEGRITY AND COMPLIANCE COMMITTEE MEETING
DECEMBER 7, 2023
12:00 p.m.
James Branch Cabell Library
901 Park Avenue – Room 311
Richmond, VA

AGENDA

1. CALL TO ORDER

Peter Farrell, *Chair*

2. ACTION ITEMS:
(1 MINUTE) 12:00-12:01

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

Approval of Minutes September 14, 2023

FOR INFORMATION:

3. AUDITOR OF PUBLIC ACCOUNTS-REPORTS FOR THE FISCAL YEAR ENDING JUNE 30, 2023
(14 MINUTES) 12:01-12:15

Mike Reinholtz, *Director,*
Auditor of Public Accounts

4. RESULT OF EXTERNAL QUALITY ASSURANCE REVIEW
(20 MINUTES) 12:15-12:35

Richard Tarr, *CISA, CIA*

5. REPORT FROM EXECUTIVE DIRECTOR OF AUDIT AND COMPLIANCE SERVICES
(10 MINUTES) 12:35-12:45

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

a. Committee Dashboard Measures
b. Internal Audit Reports
    i. Records Management
    ii. President’s Office Internal Control Compliance Review
    iii. Audit Findings Status Update
c. Handout: FY24 Audit Workplan and Special Projects

5. ERM UPDATE
(15 MINUTES) 12:45-1:00

Tom Briggs, *Assistant VP,*
Safety and Risk Management

CLOSED SESSION

6. Freedom of Information Act Section 2.2-3711 (A) (7) and (19), specifically:

a. **Audit Report for Discussion** **(15 MINUTES) 1:00-1:15** i. School of Pharmacy IT Security Review ii. President's Discretionary Fund Review	**Karen Helderman,** *Executive Director* *Audit and Compliance Services*
b. **University Counsel Litigation Update** **(10 MINUTES) 1:15 – 1:25**	**Jake Belue,** *Associate* *University Counsel*
2. RETURN TO OPEN SESSION AND CERTIFICATION Approval of Committee action on matters discussed in closed session, if necessary	**Peter Farrell,** *Chair*
3. ADJOURNMENT	**Peter Farrell,** *Chair*

RICHARD H. TARR, CIA, CISA

October 16, 2023

Ms. Karen Helderman
Executive Director, Audit and Compliance Services
Virginia Commonwealth University (VCU) and VCU Health System
918 West Franklin Street, Stokes House
Richmond, VA 23284

Dear Ms. Helderman:

Attached please find the report from the Full External Quality Assurance Review (QAR) that I conducted of Audit and Compliance Services (ACS) at Virginia Commonwealth University and VCU Health System in August and September 2023. The primary objective of the QAR was to assess ACS's conformity to The Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing (Standards)*, the IIA's Code of Ethics, and to determine whether ACS is meeting the needs of management.

The assessment consisted primarily of reviewing documents required by IIA Standards and reports and other communications to the management of both VCU and VCU Health System and their respective Boards. Surveys and Interviews were conducted with various executives and senior leaders of VCU and VCU Health System as well as ACS staff and leadership.

Based on the work that was conducted, it is my opinion that the internal audit activity at Virginia Commonwealth University and VCU Health System **generally conforms** with the IIA *International Standards for the Professional Practice of Internal Auditing*. This opinion, representing the best possible evaluation, means Audit and Compliance Services at both Virginia Commonwealth University and VCU Health System have, in place, relevant structures, policies, procedures, and processes that comply with the requirements of the professional standards and that their work can be relied upon.

This report contains a recommendation that, if implemented, should improve the effectiveness, enhance the value of ACS, and further strengthen conformity with *the Standards.*

I want to thank you and your staff for your support and the opportunity to conduct this review.

Sincerely,

Richard H. Tarr, CIA, CISA

Virginia Commonwealth University

(Including VCU Health System)

AUDIT AND COMPLIANCE SERVICES

QUALITY ASSURANCE REVIEW REPORT

October 16, 2023

Prepared by:
Richard Tarr, CIA, CISA
P.O. Box 19466
Sarasota, FL 34276-2466
Phone: 407.896.2760
E-mail: rtarr@racar.com

OVERVIEW

As required by the Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing* (*IIA Standards*), a Full External Quality Assurance Review (QAR) was conducted on the internal audit activity at Virginia Commonwealth University (VCU) and VCU Health System. The primary objective of a QAR is to provide reasonable and objective assurance that the internal audit work being performed by Audit and Compliance Services (ACS) conforms with the requirements of the *IIA Standards,* the IIA Code of Ethics, is meeting the expectations of the governing Boards, and to identify whether there are opportunities that would enhance the functionality of the audit process and improve the value of the internal auditing (IA) activity.

The scope of the review, conducted during August and September 2023, included an evaluation of:

- The Executive Director, Audit and Compliance Services' reporting relationship and her communication with the University Board of Visitors Audit, Integrity and Compliance Committee; the Health System Board of Directors Audit and Compliance Committee; and the President of VCU.
- The independence and objectivity of the audit work performed.
- Existing internal audit policies and procedures.
- The risk assessment and annual audit planning process.
- The planning process for individual audit projects.
- The audit methodologies used in performing the work.
- A representative sample of audit files and reports; the documentation that supported the work performed; and the support in the workpapers for the conclusions and recommendations in the audit reports.
- How the results of audit projects are communicated.
- The procedures for following up on audit recommendations.
- The knowledge, skills, discipline, and training of the audit staff.

In addition, interviews were conducted with selected individuals, who included, among others, the Chair of the University Board of Visitors, Audit Integrity and Compliance Committee; the Chair of the Health System Board, Audit and Compliance Committee; the University, Senior VP and Chief Financial Officer; the Health System, VP and Chief Financial Officer; the Executive Director of ACS; the Director, Audit and Management Services for the University and the Health System; the Interim Deputy Director, University Audit and Management Services; the Deputy Director, Health System Audit and Management Services; and other senior members of the audit staff.

OPINION

The IIA's review methodology allows for a three-level rating system of conformance when expressing an opinion for a review:

- "Generally, conforms" (the best) means that the Department of Audit and Compliance Services has policies, procedures, and a charter in place, and follows practices that were judged to be following applicable *IIA Standards*; however, opportunities for improvement may exist.
- "Partially Conforms" means deficiencies in practice were found that deviated from professional standards; however, these deficiencies, while they might impair, did not prohibit the Department of Audit and Compliance Services from carrying out its responsibilities.
- "Does Not Conform," means there were deficiencies in practices found that were considered so significant, as to seriously impair or prohibit the Department of Audit and Compliance Services from carrying out its responsibilities under the *IIA Standards*.

Based on the work outlined above, the reviewer believes that the internal audit activity conducted by Audit and Compliance Services **Generally Conforms** overall to the IIA *International Standards for the Professional Practice of Internal Auditing*.

This opinion, which is the best possible evaluation rating, means that there are in place relevant structures, policies, and procedures, including the processes by which they are applied, that follow the *IIA Standards* in all material respects. It is important to note that the *IIA Standards* are expressed in terms of broad concepts and objectives rather than detailed procedures, and their application requires the exercise of professional judgment. The extent of IA policies and procedures and how they are implemented will depend upon several factors, such as an audit activity's size and organizational structure, the nature of its audit responsibilities, its philosophy concerning the degree of operating autonomy appropriate for its staff, and the expectations of its governing body.

The recommendation in this report is not aimed at addressing any significant deficiencies in the IA activity but is intended to build on the foundation already in place. The *IIA Standards* require that this report be shared with the Chairs of the Audit Committees and the President of VCU.

Richard H Tarr

Richard H. Tarr, CIA, CISA

OBSERVATIONS

The Executive Director of Audit and Compliance Services (ACS) is a CPA (Certified Public Accountant), a CISA (Certified Information Systems Auditor), a PMP (Project Management Professional), has an MBA from Virginia Tech., and has over 37 years of audit and compliance experience.

She reports functionally to both the Audit, Integrity, and Compliance Committee of the VCU Board of Visitors (BOV), and the Audit and Compliance Committee of the Board of Directors (BOD) at the Health System, is well respected and has a good working relationship with both Committees. This reporting structure enables the internal auditing activity at VCU and the Heath System Board to be independent and objective as required by their Charter and *IIA Standards.* She reports administratively to the VCU President.

The functional reporting line is the ultimate source of independence and authority for the Executive Director of Audit and Compliance Services. Administrative reporting is the reporting relationship that facilitates the day-to-day operations of Audit and Compliance Services including budgeting and management accounting; human resource administration; internal communication and informational flows; and administration of internal organizational policies and procedures.

ACS senior staff is very experienced and holds numerous audit and compliance certifications. The Director, of ACS, for the University and VCU Health, is a CPA (Certified Public Accountant), a CISA (Certified Information Systems Auditor), a CGFM (Certified Government Financial Manager), a CGEIT (Certified in the Governance of Enterprise IT), is a CRMA (Certification in Risk Management Assurance), and has over 29 years of IT, internal audit, and compliance experience. The three Deputy Directors and the Manager, Social Media Governance and Audit Quality of ACS have an average of over 20 years of internal audit experience and hold internal audit certifications.

As required by *IIA Standards*, ACS has a strong Audit and Compliance Services Charter that establishes it as an independent and objective activity and clearly defines its purpose, authority, and responsibility. The Charter gives ACS authority for unrestricted access to all institutional activities, records, property, and personnel. It also authorizes full access to the BOV and BOD Audit Committees to allocate departmental resources; set audit frequencies; determine the scope of work; apply the techniques necessary to accomplish audit objectives; and obtain the necessary assistance of personnel in the University and Health System departments where they perform audits.

As required by *IIA Standards,* ACS develops annual risk assessments that, along with input from the President of VCU, vice presidents, and others both from the University and the Health System, are used to create annual audit work plans. In developing the plans, ACS has identified key risks for consideration in the audit plans going forward and has developed an identification model that is used to risk rank key business process/audit areas based on several risk factors. These audit work plans are then presented to the appropriate audit committee for their approval.

During management interviews, the Executive Director and the ACS staff received high praise and strong support for the work that the department conducts. Those interviewed also believed that the scope and type of projects that are undertaken by the department are adding value to both the University and the Health System.

A confidential survey of audit customers conducted during the review showed that 93% of those surveyed rated the department excellent or good on 18 different criteria. Given the turnover of the staff and the challenges of the pandemic, this is a very positive rating and speaks well of the professionalism and ability of ACS and the audit staff.

A sample of audit workpapers was reviewed and verified that the audit work was appropriately planned, the work performed was appropriately documented following *IIA Standards*, and that conclusions and opinions communicated in the audit reports are appropriately supported. Evidence in the workpapers showed that the audit work was conducted at a very professional level. The audit programs were appropriately referenced to the audit steps. The tests performed during the audits and the conclusions contained in the audit reports were supported by the work documented in the workpapers. There was evidence that the workpapers are thoroughly reviewed by audit supervision and the Director of Audit and Management Services reviews all the audit reports before they are issued.

BEST PRACTICES OBSERVED

During the review, several practices were observed that, while not required by the *IIA Standards*, demonstrate ACS's commitment to the highest level of quality and professionalism. The following are practices or processes that have been found to have a positive impact on internal auditing activities and are considered by many to be examples of best practices:

- ACS has mapped each Audit Committee's responsibilities, (University and Health System), to each committee's meeting schedule and agenda for the year. This information is then shared with the Committees to provide assurances that it is fulfilling its responsibilities as outlined in the Charter. The Audit, Integrity, and Compliance Committee (University) and the Audit and Compliance Committee (Health System) have documented committee meeting planners that tie each committee responsibly and ACS reporting requirements to specific committee meetings during the year.
- The Executive Director has full access to the respective Board committees.
- The Executive Director, the Director of ACS, or the deputies attend each full Board meeting and select committee meetings, including closed sessions, to stay abreast of significant developments and decisions.
- There are standing meetings for the Executive Director with the President and each senior management team member at VCU and the Health System.
- The ACS Charter is approved by the BOV Audit, Integrity, and Compliance Committee, the Health System BOD Audit and Compliance Committee, and the University President.
- The Charter authorizes ACS to obtain the necessary assistance of personnel

in departments when performing work plans and initiatives, as well as engage other specialists.

- ACS tracks, ages, and reports on the action plan status of audit recommendations to each audit committee until issues are closed.
- In addition to required professional continuing education, the department schedules routine training for audit staff and management to highlight IIA standards and recent changes to audit processes. Staff are encouraged and incentivized to obtain professional certifications and masters degrees.
- ACS has implemented standardized templates in their workpaper management tool to ensure that each audit project adheres to the appropriate planning and execution steps.
- ACS has a dedicated quality assurance manager who conducts an ongoing quality assurance workpaper review process.
- For areas that may fall below the risk threshold, ACS conducts limited-scope Internal Control Reviews that are an innovative approach to identifying where there may be opportunities to improve business processes and compliance activities.
- When appropriate and possible, data analytics is used to identify exceptions within the entire population (dataset) and compare/validate whether the control is working.
- ACS uses an agile auditing approach to adjust the annual audit plan, audit project scope, and audit testing methods as necessary in response to changing risk environments.

OPPORTUNITY FOR IMPROVEMENT

While the internal audit activity at VCU and the Health System generally conforms with the *IIA Standards*, the following recommendation should be considered by both the University Board of Visitors Audit, Integrity, and Compliance Committee, and the Health System Board of Directors Audit and Compliance Committee. This recommendation is intended to build on the foundation that is already in place to further ensure the independence, depth, and effectiveness of the audit work being performed.

Annually, in closed session, the Audit Committees should formally review the performance of the Executive Director, and the reporting level within the University, and directly determine and approve his/her annual compensation and any appropriate salary adjustment or bonus.

While it's impractical for the VCU Board of Visitors and the Health System Board to directly manage the internal audit activity day-to-day, they need to ensure there are no impairments to the ability of the Executive Director to operate independently and that there is an appropriate flow of information that would enable them to make informed decisions.

The committee charters for both the University Audit Integrity and Compliance Committee; and the Health System Audit and Compliance Committee require that they must review and concur in the appointment, replacement, reassignment, or dismissal of the Executive Director. While this ensures that the position cannot be affected without the Committees approving the change, it does not prevent the salary level of that position from being influenced by VCU management. Functional reporting should include the direct involvement of the Committees in the performance review and setting of the compensation for the Executive Director to eliminate this potential impairment to independence.

Currently, only the Audit Committee Chairs are providing comments back to the VCU President on the Executive Director's performance and are not involved in determining or reviewing the Executive Director's salary.

When evaluating impairments to reporting lines and relationships with organizational officials to whom the chief audit executive (Executive Director) reports, including evaluating potential impairments to independence and/or objectivity, consideration needs to be given to understanding who judges the performance, sets compensation levels, and determines the organizational placement of the chief audit executive within the University structure.

This involvement by governing boards in the compensation and the reporting level of the individual who is considered the Chief Audit Executive under the *IIA Standards* has been endorsed by the Institute of Internal Auditors as a best practice for complying with *IIA Standard* ***1110 – Organizational Independence.*** Organizational independence is effectively achieved when the chief audit executive reports functionally to the Board. Functional reporting includes setting compensation levels.

Attachment A: Summary of IIA Standards

		GC	PC	DNC
Overall Evaluation		✓		
	ATTRIBUTES STANDARDS			
1000	**Purpose, Authority, and Responsibility** The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework (the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the *Standards*, and the Definition of Internal Auditing). The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.	✓		
1010	Recognition of the Definition of Internal Auditing, the Code of Ethics, and the *Standards* in the Internal Audit Charter.	✓		
1100	**Independence and Objectivity** The internal audit activity must be independent, and internal auditors must be objective in performing their work.	✓		
1110	Organizational Independence	✓		
1111	Direct Interaction with the Board	✓		
1120	Individual Objectivity	✓		
1130	Impairments to Independence or Objectivity	✓		
1200	**Proficiency and Due Professional Care** Engagements must be performed with proficiency and due professional care.	✓		
1210	Proficiency	✓		
1220	Due Professional Care	✓		
1230	Continuing Professional Development	✓		
1300	**Quality Assurance and Improvement Program** The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.	✓		
1310	Requirements of the Quality Assurance and Improvement Program	✓		
1311	Internal Assessments	✓		
1312	External Assessments	✓		
1320	Reporting on the Quality Assurance and Improvement Program	✓		
1321	Use of "Conforms with the *International Standards for the Professional Practice of Internal Auditing*"	✓		
1322	Disclosure of Nonconformance	✓		

		GC	PC	DNC
	PERFORMANCE STANDARDS			
2000	**Managing the Internal Audit Activity** The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.	✓		
2010	Planning	✓		
2020	Communication and Approval	✓		
2030	Resource Management	✓		
2040	Policies and Procedures	✓		
2050	Coordination	✓		
2060	Reporting to Senior Management and the Board	✓		
2070	External Service Provider and Organizational Responsibilities for Internal Audit	✓		
2100	**Nature of Work** The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive, and their evaluations offer new insights and consider future impact.	✓		
2110	Governance	✓		
2120	Risk Management	✓		
2130	Control	✓		
2200	**Engagement Planning** Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.	✓		
2201	Planning Considerations	✓		
2210	Engagement Objectives	✓		
2220	Engagement Scope	✓		
2230	Engagement Resource Allocation	✓		
2240	Engagement Work Programs	✓		
2300	**Performing the Engagement** Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.	✓		
2310	Identifying Information	✓		

2320	Analysis and Evaluation	✓		
2330	Documenting Information	✓		
2340	Engagement Supervision	✓		
2400	**Communicating Results** Internal auditors must communicate the results of engagements.	✓		
2410	Criteria for Communicating	✓		
2420	Quality of Communications	✓		
2421	Errors and Omissions	✓		
2430	Use of “Conducted in Conformance with the *International Standards for the Professional Practice of Internal Auditing*”	✓		
2431	Engagement Disclosure of Nonconformance	✓		
2440	Disseminating Results	✓		
2450	Overall Opinions	✓		
2500	**Monitoring Progress** The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.	✓		
2600	**Resolution of Senior Management’s Acceptance of Risks** When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.	✓		

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 new Associate Vice Provost for Institutional Research and Decision Support joined VCU in earlier this Fall. Efforts are underway to strengthen the policy and process infrastructure around data governance and to reconstitute the data governance committee to better cover all data domains. Priority has initially been placed on standardizing and enhancing the collection and maintenance of faculty data, with active projects underway to revitalize the system used to collect faculty credentials and report those as necessary.

🟨 **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

Security Incidents and Trends: VCU has not directly experienced any cybersecurity incident in the past quarter that led to any significant impact. However, threat actors are leveraging new alternative tactics to bypass modern organizational cyber defense mechanisms. VCU is aware of cybersecurity incidents affecting at least three of its vendors (though none have indicated that VCU information is affected). As such, additional risk-based adjustments to our defensive capabilities are in progress to help address these new tactics.

Next generation security architecture: VCU completed the rollout of its Secure Access Server Edge (SASE) security platform earlier this year. The implementation of this platform has significantly increased the cyber defense capabilities for the university, and with the location agnostic nature of this platform, consistent security protections can be extended to both on-premise and remote users; which is not something the traditional VPN can provide. From July to September of 2023, the platform has examined over 3.5 billion network transactions conducted using VCU-issued and managed devices and helped to stop over 1.8 million potential threats from affecting our assets and employees. Continued efforts are being made to further enhance and configure this platform so that VCU can utilize additional capabilities from the platform.

Secured Research Environment: Through a collaborative effort between the VCU Health System and VCU, a new on-premise secured research computing environment has been set-up to help provide computational support to both high-sensitivity and general research projects that utilize data from the health system. The environment is currently being piloted with limited researchers and additional validation testing is being performed with the goal of validating the high-sensitivity environment against industry standards adopted by the federal funding agencies for controlled unclassified environments. The successful validation of controls can provide needed infrastructure for research projects

Gramm-Leach-Bliley Act (GLBA) Compliance: VCU has successfully reviewed and addressed the additional gaps between its practices and the new GLBA safeguards rule. A security penetration test is scheduled for the GLBA covered systems and environments. The test will help to identify security vulnerabilities and recommended actions for strengthening the security controls for these areas.

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 voted three (3) risks previously out of tolerance back within tolerance. This decision will be reviewed by the Cabinet in September for approval and presented to the Board in December.

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; however we are short one university auditor position and plan to hold on filling the position to accomodate FY24 budget cuts. The audit team is assessing how the vacancy will affect our workplan schedule and will defer lower risk audits until later in the year. Investigations have been increasing and this work further affects our workplan schedule, but currently we are managing this work effectively.

INSTITUTIONAL COMPLIANCE PROGRAM

🟩 **Compliance requirements compared to known material violations**

🟩 **Compliance Program Oversight & Effectiveness**

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

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

🟥 Significant challenges to institutional compliance strategy or resolution encountered

Notes: There are no known material compliance violations 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. Also good progress in building trust with departments and schools so that they understand how we can support them with independent reviews and guidance. (examples: School of Nursing, School of Pharmacy, VCU Police, VCU Arts Qatar, OVPRI, Office of the Provost).

VCU

VIRGINIA COMMONWEALTH UNIVERSITY

Records Management

Final Report
September 7, 2023

Audit and Compliance Services

Overview

The Records Management Office is a sub-unit of the Central Services department, a division of Technology Services. Central Services consists of 14 staff, led by the director of central services and the university's Designated Records Officer (DRO). The Records Management Office has one staff, a records management coordinator who oversees the records management program. Both the DRO and the records management coordinator are well versed in the Library of Virginia Records Management regulations and requirements.

The State Library Board is responsible for the state records management program under the Virginia Public Records Act (VPRA), which delegated the operation of the program to the staff of the Library of Virginia. As a state agency, Virginia Commonwealth University is required to implement and maintain an effective records management program that will adhere to the Library of Virginia's record retention and disposition schedules, proper documentation of record destruction, and training of employees.

The DRO serves on behalf of VCU as a liaison to the Library of Virginia implementing and overseeing the records management program at VCU. The university's Records Management policy communicates the general responsibilities of the DRO, department heads, department records coordinators, and employees in managing, retaining and disposing of records in accordance with the VPRA.

The DRO and the Records Management Office provide numerous services to support the university's faculty and staff with records management compliance and destruction of university records to include the following:

- Administering the records management program at the university
- Advising employees on accessing and using the records retention schedules
- Collaborating with department record coordinators (DRC)
- Assisting DRCs in the surveying of records (inventory)
- Records management training, including
    - Preservation of records that have historical, legal, fiscal, or administrative value or that must be preserved by law
    - Disposition of public records that no longer serve administrative, legal, fiscal, or historical purposes
- Completion of RM-3 forms (request for destruction approvals and maintenance)

Each major budget unit is required to have at least one DRC to assist with records management compliance. The university has approximately 140 DRCs designated to assist with records management compliance within their departments, educating department employees on proper record management practices, and assisting with records destruction.

Purpose

The objective of the audit was to determine whether Central Services had policies and procedures in place to manage the Records Management Program.

Scope and Audit Procedures

Our scope of Records Management encompassed the Records Management Program and its policies and procedures; department record coordinators, paper and electronic records, and RM-3 forms for records destruction.

Our Audit procedures consisted of the following:

- Interviews with personnel in the Records Management Office and Collaboration Services
- Review of:
  - Records Management Policy
  - Records Management Program
  - Records management training
- Testing removal or transfer of shared network drives and google drives when an employee leaves VCU.
- Testing for completion of Certificate of Destruction forms (RM-3 forms)
- Evaluation of compliance with the Records Management Program

Summary of Major Business Issue and Management's Action Plan

Implement a Strategy to Encourage Compliance with the Records Management Policy

Over the last two years, Internal Audit has tested records management within nine units and found 33% of them were not destroying records in accordance with the records retention policy and 44% had not developed a records inventory. In addition, Central Services provided documentation showing that approximately 41% of all department record coordinators did not complete records management training. Noncompliance with the Records Management Policy could result in inefficiencies caused by responding to FOIA requests that include old records that should have been destroyed as well as unnecessary expenses for record storage, both electronic and physical.

Central Services has developed records management processes and communications (emails, TelegRAM, and website) that, if followed, will ensure departments comply with the Records Management Policy and state regulations. Unfortunately, Central Services has not seen a positive improvement in department compliance year over year. This is likely due to departments not viewing records management as a priority and the reluctance by employees to destroy records as they may perceive a future need for them.

Central Services should develop a strategy to improve compliance with the Records Management Policy and Program. The following are suggestions that could be included in a strategy:

- Require training for all DRCs
- Work with Human Resources to develop a smart goal that pertains to the duties of DRCs and require supervisors to include the goal in their performance evaluations
- Provide Vice-President's and Deans with routine statistics on Records Management for each of their areas of responsibility (quarterly or semi-annually)

DRCs are advocates for the Records Management Program and are tasked with assisting their departments with records management compliance. DRCs are to be knowledgeable about the records management policy and procedures, the Library of Virginia retention schedules, and educate employees within their departments about record management practices. The University community, as a whole will increase its awareness and compliance with the Records Management policy by having trained DRCs that can effectively educate staff in their respective departments. Additionally, holding DRCs accountable through their performance reviews will encourage them to make records management a priority, and providing leaders with routine statistics for the records management program will encourage compliance with the program.

Management's Action Plan: *Concur.*

- *Required training will be implemented for all department record coordinators. Completion date: September 1, 2023*
- *Partner with Human Resources to create a SMART goal template for DRCs in Talent and strongly encourage DRCs to add this goal beginning with the 2024 performance cycle. Completion date: December 1, 2023*
- *Partner with Human Resources and the Compliance Office who are building a mandatory training compliance dashboard in Talent. Routine statistics on Records Management will be made available to VPs and Deans for each of their areas of responsibility through this dashboard. Completion date: August 14, 2024*

Responsibility: University Records Officer

Conclusion

In our opinion, based on the results of our audit, Central Services had policies and procedures in place to manage the Records Management Program; however, they do not have an effective strategy implemented to strengthen compliance with the policies and procedures.

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:

Barry Lanneau, Jr.	Director of Central Services and University Records Officer
Alex Henson	Chief Information Officer
Meredith Weiss	Vice President for Administration

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

Karen K. Helderman

Executive Director
Audit and Compliance Services

VIRGINIA COMMONWEALTH UNIVERSITY

Office of the President

Internal Controls Compliance Review

Final Report
November 17, 2023

Audit and Compliance Services

Audit and Compliance Services
918 West Franklin Street
Box 842503
Richmond, Virginia 23284-2503
Phone: (804) 828-2336
Fax: (804) 828-2356

To: Michael Rao
President

From: Karen Helderman
Executive Director, Audit and Compliance Services

Date: November 17, 2023

Subject: Internal Controls Compliance Review of the Office of The President

---

Internal Audit has completed an Internal Controls Compliance Review of selected internal controls related to the Office of The President and have included the results in the attached Dashboard Report.

cc. Karol Gray, Senior Vice President and Chief Financial Officer
Pamela Lepley, Senior Advisor to the President

Internal Controls Compliance Assessment Dashboard

Audit name:	Office of The President

Reason for audit:	Provide management with assurance that selected financial and administrative processes were performed and monitored properly.

Conclusion by Process	**Risk Rating**
1. Financial Monitoring	
1.1. Forecast Monitoring of approved budgets was performed	🟩
1.2. Budgets were reviewed and negative variances were addressed	🟩
2. Banner Reconciliations	
2.1. Banner reconciliations were performed monthly or as required by the fiscal Administrator's Handbook	🟩
2.2. Reconciliations were signed and dated by both the reviewer and approver	🟪
2.3. Supporting documentation for transactions were readily available	🟩
3. Journal Vouchers	
3.1. JVs were approved by the appropriate position depending on dollar amount	🟩
3.2. Documentation to support JVs was maintained	🟩
4. Petty Cash	
4.1. Petty cash funds were secured according to the university Petty Cash policy	N/A
4.2. Custodian was the only authorized person with access to funds	N/A
4.3. Monthly and annual reconciliations were performed timely	N/A
4.4. Annual Trainings completed by the custodian, dean/department head or designee	N/A
4.5. Petty cash fund maintained at authorized amount at all times (combination of unreimbursed receipts and/or cash)	N/A
5. Purchases –	
5.1. Purchases had a valid business purpose and were reasonable	🟩
5.2. There was adequate documentation to support emergency or sole source purchases	🟩
5.3. Purchases >$10,000 were routed through Procurement Services for review and approval	🟩

5.4. Controls were in place to prevent the splitting of orders to avoid procurement rules 5.5. Supporting documentation was maintained electronically 5.6. Purchase orders were closed timely in RealSource	🟩 🟩 🟩
6. Travel 6.1. Travel > $500 or air/rail was approved prior to traveling and reimbursements were processed through Chrome River 6.2. Transportation (air and rail) was booked through Christopherson 6.3. Travel was for allowable business purposes 6.4. Hotel and meals were within the appropriate per diem range	 🟩 🟩 🟩 🟩
7. Purchase Cards (Pcards) 7.1. Granted to the minimum necessary number of cardholders and provide the minimum necessary spending and transaction limits 7.2. Applications were authorized by the cardholder’s supervisor 7.3. Only used by the cardholder and were not shared 7.4. Individual cardholders were tasked with securing their Pcards 7.5. Transactions allocated to the appropriate expense account timely 7.6. Transactions supported by receipts or valid invoices uploaded into the Pcard system 7.7. Reviewers and approvers were timely reviewing and approving transactions in BOA Works 7.8. Controls were in place to prevent Pcard holders from splitting transactions in to two or more transactions 7.9. Sales taxes were excluded from Pcard purchases where appropriate 7.10. Purchases were reconciled to receipts and to the cardholder’s monthly statement 7.11. Purchases had a valid business purpose and were allowable based on the Purchasing Card Program Procedures	 🟩 🟩 🟩 🟩 🟩 🟩 🟪 🟩 🟩 🟩 🟩
8. Record Management 8.1. Records were destroyed according to VCU’s Record Retention Policy 8.2. The unit identified a records custodian 8.3. Records custodian attended records retention training 8.4. The unit developed a records inventory	 🟪 🟩 🟩 🟪
9. Grants 9.1. Expenditures were in accordance with the grant agreement 9.2. Certified effort is in accordance with grant agreement	 N/A N/A

9.3. Performance/progress reports submitted to the sponsor timely where required	N/A
10. Fixed Assets 10.1. Annual inventory was completed and submitted to Fixed Asset Accounting Office 10.2. Assets were properly tagged 10.3. Assets stolen, traded-in, or transferred had the surplus forms completed 10.4. All HEETF purchases $500 and above were recorded as fixed assets	 🟩 🟩 🟩 N/A
11. ARMICS 11.1. Yearly ARMICS documentation was completed and submitted by the due date set by the controller's office 11.2. An appropriate level of testing was performed to provide sufficient evidence that controls were operating as intended 11.3. Supporting documentation for unit testing was readily available	 🟩 🟪 🟪
12. Local Applications 12.1. Annual access reviews for local applications were performed 12.2.Local Applications were inventoried according to the Passwords Authentication and Access Standard 12.3.Application server(s) were administered or supported by central IT through a SLA 12.4. Signed copy(s) of the Service Level Agreement with Technology Services were available	 N/A N/A N/A

Our assessment 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.

Note: Risk Classifications/Definitions and Issue Table, if applicable, are included on following page.

Risk Classifications and Definitions

🟩 **Full Compliance**	● Overall control environment representative of good practice, well-designed, effective, and functioning properly. ● No improvement opportunities identified. Full Compliance.
🟨 **Verbal Finding**	● Adequate control environment in most areas. ● Moderate risk improvement opportunities identified, which require corrective action ● Minor Findings of non-compliance. ● Finding and recommendation verbally communicated to management and no written corrective action required.
🟪 **Management Level Finding**	● Some key controls do not exist, or are not properly implemented, and there are improvement opportunities. ● Control environment is impaired. ● Partial non-compliance with a policy. ● Finding and recommendation communicated to management and written corrective action required.
🟥 **Board Level Finding**	● Control environment is unacceptable with critical issues, individually or in the aggregate, having been identified or major noncompliance with University policies. ● Control environment contains insufficient internal controls to address key risks and the impact may be substantial in size or nature or their effect cannot be quantified. ● Significant non-compliance with a policy. ● Immediate corrective action should be implemented. ● VP level involvement needed. ● Finding and recommendation communicated to the Board and written corrective action required.
N/A	● Function is not applicable to the reviewed department/division.

Report Title	Finding	Due Date	VP on Target[1]	VP	Revised Date or TBD
CBORD Systems Security	Establish a University Building Access Policy	September 2023	**N**	Meredith Weiss	Apr-24
Human Subject Research Data Security	Develop and Implement a Policy to Utilize the Honest Broker Service	Dec-23	**Y**	Srirama Rao	N/A
Human Subject Research Data Security	Conduct Periodic Data Security Monitoring and Oversight of Research Data	Dec-23	**Y**	Srirama Rao	N/A
Facilities Management Department IT Systems Review	Enforce Central Works Pro Fire Alarm Server Security Baseline Compliance	June 2024	**Y**	Meredith Weiss	N/A
Facilities Management Department IT Systems Review	Develop Operations Center Disaster Recovery Plan	June 2024	**Y**	Meredith Weiss	N/A
Microsoft Active Directory Security	Develop and Implement Processes to Manager Service Accounts	July 2023	**Y**	Meredith Weiss	N/A
Microsoft Active Directory Security	Perform Periodic Active Directory Password Reviews	March 2024	**Y**	Meredith Weiss	N/A
Fischer IAM Security	Disable Faculty and Staff eIDs Once They Reach Former Status	January 2024	**Y**	Meredith Weiss	N/A
COVID Data Security	Assign Data Responsibilities for Employee and Student COVID Data	Oct-23	**Y**	Meredith Weiss	N/A
Third Party Software Management	Gain Assurance Over all High-Risk Category 1 Third-Party Applications	December 2023	**Y**	Meredith Weiss	N/A
Third Party Software Management	Update Application Inventory and Develop Governance Processes to Maintain it	June 2023	**Y**	Meredith Weiss	N/A
Third Party Software Management	Review Cloud System Contracts and Ensure it Includes the Data and Intellectual Property Addendum	June 2024	**Y**	Meredith Weiss	N/A
Google Workspace Security	Disable the use of Less Secure Applications	December 2023	**Y**	Meredith Weiss	N/A
Google Workspace Security	Disable Insecure Email Protocols	December 2023	**Y**	Meredith Weiss	N/A
Google Workspace Security	Monitor Google Sites and Update TerminalFour Training	December 2024	**Y**	Meredith Weiss	N/A
Parking Billing and Reserves	Develop a Parking, Citations and Enforcement Policy	Apr-24	**Y**	Meredith Weiss	N/A
Real Source Supplier Management and Purchasing/Payments	Document Screening for Debarred Vendors	Oct-23	**Y**	Karol Gray	N/A
Grants and Contracts - Non-Federal	Improve Timely Resolution of Grants in Deficit	Jul-23	**Y**	Karol Gray	N/A
Budget Process	Enhance Training Opportunities for Revenue Units	Oct-23	**Y**	Karol Gray	N/A
Outside Professional Activities	Enhance Electronic Reporting of OPA and Require Its Usage	Nov-23	**Y**	Marlon Levy	N/A
Outside Professional Activities	Update the OPA Policy	Sep-23	**Y**	Marlon Levy	N/A
Outside Professional Activities	Require OPA Training	11/30/023	**Y**	Marlon Levy	N/A
School of Pharmacy Internal Control Compliance Review	Ensure Adequate Documentation for ARMICS Testing is Completed	Jun-23	**Y**	Marlon Levy	N/A
School of Pharmacy Internal Control Compliance Review	Improve Records Management Destruction	Jun-23	**Y**	Marlon Levy	N/A
Unused Scholarships	Explore Integration of Blackbaud and Banner Finance	Dec-23	**Y**	Jay Davenport	N/A

	A	B	C	D	E	F
1	Report Title	Finding	Due Date	VP on Target1	VP	Revised Date or TBD
27	Unused Scholarships	Evaluate and Improve Usage of the Blackbaud Award Management System Globally	Dec-23	Y	Jay Davenport	N/A
28	VCU Social Media	Develop Governance over Decentralized Social Media Accounts	Dec-23	Y	Grant Heston	N/A
29	Centers and Institutes (Non-Research Enterprise)	Establish Policy for Non-Research Centers and Institutes	May-24	Y	Fotis Sortiropoulos	N/A
30	Outside Professional Activities	Enhance Electronic Reporting of OPA and Require Its Usage	Nov-23	Y	Fotis Sortiropoulos	N/A
31	Outside Professional Activities	Update the OPA Policy	Sep-23	Y	Fotis Sortiropoulos	N/A
32	Outside Professional Activities	Require OPA Training	11/30/023	Y	Fotis Sortiropoulos	N/A
33	Unused Scholarships	Strengthen Policy Statements for Clarity and to Designate Process Ownership	Dec-23	Y	Fotis Sortiropoulos	N/A
34	Unused Scholarships	Explore Integration of Blackbaud and Banner Finance	Dec-23	Y	Fotis Sortiropoulos	N/A
35	Unused Scholarships	Evaluate and Improve Usage of the Blackbaud Award Management System Globally	Dec-23	Y	Fotis Sortiropoulos	N/A
36	University College Internal Control Compliance Review	Improve Banner Reconciliation Process	Aug-23	Y	Fotis Sortiropoulos	N/A
37	University College Internal Control Compliance Review	Improve ARMICS Testing and Documentation	Jul-23	Y	Fotis Sortiropoulos	N/A
38	University College Internal Control Compliance Review	Improve Records Management Process	Sep-23	Y	Fotis Sortiropoulos	N/A
39	Global Education Internal Control Compliance Review	Improve ARMICS Testing and Documentation	Apr-24	Y	Fotis Sortiropoulos	N/A
40	Global Education Internal Control Compliance Review	Improve Records Management Processes	Sep-23	Y	Fotis Sortiropoulos	N/A
41	Titanium IT Control Review	Update Titanium Contract Terms During the Next Renewal Cycle	January 2024	Y	Fotis Sotiropoulos	N/A

Audit and Management Services
Status of Fiscal Year 2023-2024 Audit Work Plan
November 15, 2023

Area	Status
Carryovers	
Prior Year Work Plan: Academic and Executive Administrator Contracts (replaced SCHEV Reporting)	Completed
Prior Year Work Plan: Records Management	Completed
Prior Year Work Plan: ERM RMM Plan Evaluation	Completed
Prior Year School of Pharmacy IT Review	Completed
Current Year Risk-based Audits and Assessments	
President’s Office ICCR	Completed
SCHEV Reporting	In Progress
Ancillary Systems Integrity	In Progress
Service Contract Management	In Progress
Massey Cancer Center IT Review	In Progress
Sunapsis (VISA Management) System Review - ICCR	In Progress
Human Resources – Compensation	Not Started
Facilities Management – Deferred Maintenance	Not Started
Online Distance Learning	Not Started
VCU Card Office	Not Started
Telecommunications	Not Started
Procurement Office ICCR	Not Started
College of Health Professions ICCR	Not Started
Qatar Campus ICCR	Not Started
Centers and Institutes Technical Review	Not Started
Canvas IT Security Review	Not Started
Pyramed (Student Health) System Review - ICCR	Not Started
Annual Engagements and Activities	
Audit Risk Assessment – FY24	Not Started
President’s FY 23 Discretionary Fund and Travel Activity Review	Completed
VCU Police Department – Unannounced Property Inspection – FY24 Part 1	Not Started

Audit and Management Services
Status of Fiscal Year 2023-2024 Audit Work Plan
November 15, 2023

VCU Police Department – Unannounced Property Inspection – FY24 Part 2	Not Started
Annual Review of Audit Recommendations Outstanding – FY24	Not Started

Special Project	**Status**
Continuing Projects	
State Employees Fraud, Waste, and Abuse Hotline	In Progress – 1; Closed – 0
University Compliance Helpline Investigations	In Progress – 1; Closed – 5
Other Projects	
Facilities Management and Accounts Payable Project	Completed

Board of Visitors
Audit, Integrity and Compliance Committee

December 7, 2023

VCU

Action Items

- Audit, Integrity and Compliance Committee Meeting held on September 14, 2023
- Motion to approve the Minutes

Auditor of Public Account Report

- Annual Audit for Year Ended June 30, 2023

  - Independent Auditor's Report (Opinion) on the Financial Statements
  - Report on Internal Control and Compliance
  - Required Communications

Results of External Quality Assurance Review

Richard Tarr, CISA, CIA

- Required by International Standards for the Professional Practice of Internal Auditing and last performed in 2019
- Received a "*generally conforms*" opinion, which is the best possible evaluation
- Observed several operationalized best practices
- Noted a best practice opportunity for the Audit Committee to review the CAE's performance and compensation

Dashboard Measures

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

Records Management Audit Report

Audit Scope:

- Records Management Program and its policies and procedures
- Department record coordinators (DRC)
- Paper and electronic records
- RM-3 forms for records destruction

Conclusion:

Central Services had policies and procedures in place to manage the Records Management Program; however, they do not have an effective strategy implemented to strengthen compliance with the policies and procedures.

One Board level recommendation to develop strategy that encourages Records Management policy compliance

Management concurs and will:

- *Require training for all DRCs (September 2023)*
- *Add goal to DRC performance evaluation template (December 2023)*
- *Collect and report stats on Records Management dashboard (August 2024)*

President’s Office Internal Control Compliance Review

Reviewed Selected Controls and Compliance Areas

e.g. Banner certifications, purchases, purchase cards, ARMICS, records management

No Board Level Findings

Audit Findings Status Update

VP’s attested that 40 of 41 audit recommendations outstanding are on target to meet their due date. Full schedule provided in handouts.

Finding	Due Date	Revised Due Date	VP on Target
Establish a University Building Access Policy	Sep 2023	April 2024	N

N – Target in Jeopardy or Already Missed

VCU Enterprise Risk Management evolution

Operational governance

2024: Clearly and purposefully connect ERM to drive organizational goal achievement

Risk survey

2022: Stakeholders surveyed to identify risks out of tolerance based on risk appetite

Risk appetite

2021: Risk appetite and survey methodology developed

Risk controls

2019: Risk controls added to departmental audits; risk mitigation plans are reviewed

Risk consolidation

2018: Workshops conducted to consolidate 122 risks to 19

Enterprise Risk Management charter

2016: VCU's ERM charter and process approved by the President's Cabinet

Risk identification

2013: VCU identified 122 risks through KPMG (consultant)

CLOSED SESSION