



VCU

**VIRGINIA COMMONWEALTH UNIVERSITY
AUDIT, INTEGRITY AND COMPLIANCE COMMITTEE MEETING
7:45 A.M.
DECEMBER 13, 2019
JAMES BRANCH CABELL LIBRARY
901 PARK AVENUE – ROOM 311
RICHMOND, VIRGINIA**

AGENDA

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

- 2. APPROVAL OF AGENDA** *Shantaram Talegaonkar, Chair*

- 3. APPROVAL OF MINUTES** *Shantaram Talegaonkar, Chair*
(September 13, 2019)

- 4. APPROVAL OF REVISED AUDIT, INTEGRITY AND COMPLIANCE COMMITTEE DASHBOARD MEASURES** *Karen Helderman, Executive Director
Audit and Compliance Services
Alex Henson, Chief Information Officer*

- 5. AUDITOR OF PUBLIC ACCOUNTS- REPORTS FOR THE FISCAL YEAR ENDING JUNE 30, 2019** *Mike Reinholtz, Director, Auditor of Public Accounts*

- 6. DATA GOVERNANCE UPDATE** *Monal Patel, Associate Vice Provost
Institutional Research and Decision Support
Alex Henson, Chief Information Officer*

- 7. REPORT FROM THE EXECUTIVE DIRECTOR OF AUDIT AND COMPLIANCE SERVICES** *Karen Helderman, Executive Director
Audit and Compliance Services*
 - a. Overview of External Quality Assessment
 - b. Ethics and Compliance Effectiveness Report Update
 - c. Audit Work Plan Status FY20

8. CLOSED SESSION

Freedom of Information Act Sections 2.2-3711(A)
(1) (7) and (19), specifically:

A. University Counsel Update

Jake Belue, *Associate University Counsel*

B. Audit Report for Information

- Review of President's Discretionary Funds

Karen Helderman, *Executive Director Audit and Compliance Services*

C. Audit Reports for Discussion

- ACH Corrective Action – Status Update
- Selected Employment Separation Processes
- Desktop Service Delivery

Karen Helderman, *Executive Director Audit and Compliance Services*

EXECUTIVE SESSION

9. RETURN TO OPEN SESSION AND CERTIFICATION

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

Shantaram Talegaonkar, *Chair*

10. ADJOURNMENT

Shantaram Talegaonkar, *Chair*



**Board of Visitors
Audit, Integrity and Compliance Committee
7:45 a.m.
September 13, 2019
James Cabell Library
901 Park Avenue, Room 311, Richmond, Virginia**

Minutes

COMMITTEE MEMBERS PRESENT

Mr. H. Benson Dendy III, Acting Chair
Ms. Pamela El, Vice Chair
Mr. Edward McCoy
Dr. Gopinath Jadhav
Mr. G. Richard Wagoner, Jr.

COMMITTEE MEMBERS ABSENT

Dr. Shantaram Talegaonkar

OTHERS PRESENT

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

CALL TO ORDER

Mr. H. Benson Dendy III, Acting Chair, called the meeting to order at 7:50 a.m.

APPROVAL OF AGENDA

Mr. Dendy asked for a motion to approve the agenda for the September 13, 2019 meeting of the Audit, Integrity and Compliance Committee, as published. After motion duly made and seconded the agenda for the September 13, 2019 meeting of the Audit, Integrity, and Compliance Committee (AICC) was approved.

APPROVAL OF MINUTES

Mr. Dendy asked for a motion to approve the minutes of the May 10, 2019 meeting of the Audit, Integrity and Compliance Committee, as published. After motion duly made and seconded the minutes of the May 10, 2019 Audit, Integrity, and Compliance Committee meeting were approved. A copy of the minutes can be found on the VCU website at the following webpage <http://www.president.vcu.edu/board/minutes.html>.

REPORTS AND RECOMMENDATIONS

Audit and Compliance Services Charter – Annual Update

Ms. Karen Helderman, Executive Director of Audit and Compliance Services, discussed proposed changes to the department charter for Audit and Compliance Services. Mr. Dendy asked for a motion to approve the revised department charter. After motion duly made and seconded, the Audit and Compliance Services charter was approved. A copy of the charter is attached hereto as **Attachment A** and is made a part hereof.

Audit, Integrity and Compliance Committee Dashboard Measures

Ms. Helderman presented the current status of the dashboard measures. Indicators for Data Security, Compliance Oversight and Planned Audits were yellow and other indicators were green.

Department Proposed Goals FY 2020, Budget, Staff Qualifications, and Audit Survey

Ms. Helderman presented the department's goals for fiscal year 2020, the audit and compliance staff qualifications, the ACS department budget and the results of the FY19 audit surveys.

Audit Update for Information

Ms. Helderman reviewed for informational purposes the following audit reports: Athletics – Year 3 NCAA Compliance Review, Consolidated Audit of Cardiology, Student Fees and Network Management Controls. She noted that each report showed positive conclusions and contained no audit recommendations.

Ms. Helderman indicated that the 2020 annual audit work plan is underway with four audits completed and four audits in progress. Ms. Helderman also mentioned that due to recent audit staff absences and new team members, there are still some delays in completing IT audits.

Ethics and Compliance Effectiveness Report Update

Ms. Helderman presented a prioritized action plan to address each of the recommendations contained in the 2019 compliance effectiveness report provided by Ethisphere. The committee reviewed and discussed the action plan and Ms. Helderman noted that she would include updates in future committee materials.

Enterprise Risk Management (ERM) Update

Tom Briggs, Assistant VP for Safety and Risk, provided an overview of VCU's ERM program and highlighted recent activities of the ERM Steering Committee.

Integrity and Compliance Annual Report FY 2019

Ms. Jacqueline Kniska, the university's chief integrity and compliance officer, presented the Integrity and Compliance Annual Report. Ms. Kniska provided an overview of the university-wide integrity and compliance activities highlighted in the report.

CLOSED SESSION

On motion made and seconded, the Audit, Integrity, and Compliance Committee of the Virginia Commonwealth University Board of Visitors convened into closed session pursuant to Sections 2.2-3711 (A) (1) and 2.2-3711 (A) (7) of the Virginia Freedom of Information Act to discuss certain personnel matters involving the performance of identifiable employees or faculty of the university, and to discuss the evaluation of performance of departments or schools of the university where such evaluation will necessarily involve discussion of the performance of specific individuals, including audit reports of individually identified departments and/or schools, and to consult with legal counsel and receive briefings by staff members regarding legal matters and actual or probable litigation relating to the aforementioned audit reports where such consultation or briefing in open session would adversely affect the negotiating or litigating posture of the university.

RECONVENED SESSION

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

Resolution of Certification

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

<u>Vote</u>	<u>Ayes</u>	<u>Nays</u>
Mr. H. Ben Dendy III, Acting Chair	X	
Ms. Pamela El, Vice Chair	X	
Mr. Edward McCoy	X	
Dr. Gopinath Jadhav	X	
Mr. G. Richard Wagoner Jr.	X	

All members responding affirmatively, the motion was adopted.

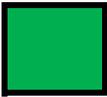
ADJOURNMENT

There being no further business Mr. Dendy, Acting Chair, adjourned the meeting at 9:15 a.m.

AUDIT, INTEGRITY, AND COMPLIANCE COMMITTEE

DASHBOARD MEASURES

INFORMATION TECHNOLOGY GOVERNANCE - DATA INTEGRITY



DATA GOVERNANCE PROGRAM (development of program)



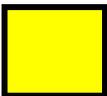
Program progressing successfully



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



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

Insert Update from Alex

ERM PROGRAM



Status of ERM mitigation plans



Program progressing on schedule



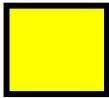
Program not on schedule; ERM Committee to address.



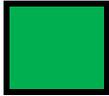
Program significantly behind schedule; Executive Management attention required.

Notes: The ERM Steering Committee (Committee) continues to review of the highest ranked Risk Mitigation and Management (RMM) Plans.

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



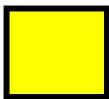
Some overload or barriers / challenges encountered that may require adjustment or reallocation of resources to resolve



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

Notes: Unplanned staffing absences continue to affected the audit schedule.

COMPLIANCE OVERSIGHT



Compliance requirements compared to known material violations



No known noncompliance



Challenges encountered that have an impact on resolution or implementation



Significant compliance challenge encountered

Notes: Institutional infrastructure to ensure compliance with the multitude of federal and state laws and regulations as well as university policies and procedures still requires attention.

AUI

INFORMA'
DATA INT

DATA



DATA



Insert Update fro

ERM PROC

Status



Notes: The ERM
Management (RM

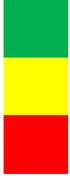
PLANNED



PLAN



SPEC
resou



Notes: Unplani

COMPLIAI



Comp



Notes: Instituti
well as

Revised

DIT, INTEGRITY, AND COMPLIANCE COMMITTEE

DASHBOARD MEASURES

INFORMATION TECHNOLOGY GOVERNANCE - INTEGRITY

INFORMATION TECHNOLOGY GOVERNANCE PROGRAM (Proving value and benefit)

Program progressing successfully

Barriers / challenges exist, but are resolved successfully by the Steering Committee.

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

INTEGRITY (number of security incidents / breaches)

Normal levels of minor security incidents or near misses occurred, but no significant data breaches have occurred or seem likely to occur; Security risks are understood, risk treatment options are applied or being prioritized for such risks. Some overload or barriers/challenges are observed and may require minor adjustment or reallocation of resources.

Elevated levels of security incidents or near misses observed, but no significant data breaches have occurred. The risk for significant incidents is elevated due to the shift in external or internal risk factors; adjustment or reallocation of resources and the development of risk treatment plans are needed.

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

Tom Alex

INTEGRITY

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.

Steering Committee (Committee) continues to review of the highest ranked Risk Mitigation and (ERM) Plans.

AUDIT STATUS

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

IAL 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

ned staffing absences continue to affected the audit schedule.

NCE OVERSIGHT

liance requirements compared to known material violations

Normal levels of immaterial noncompliance have occurred, but no significant noncompliance has occurred or seems likely to occur; Noncompliance risks are understood and compliance partners are applying reasonable actions to mitigate. Only minor compliance challenges exist.

Elevated levels of immaterial compliance have occurred or isolated material noncompliance has occurred and the internal compliance committee and compliance partners are collaborating on root cause analysis and applying reasonable mitigation plans. Some compliance challenges exist and are being resolved through the internal compliance committee.

Significant levels of noncompliance have occurred or significant compliance challenge encountered.

onal infrastructure to ensure compliance with the multitude of federal and state laws and regulations as university policies and procedures still requires attention.



**Virginia Commonwealth
University**

2019 Full External Quality Assessment Review

October 16, 2019

Karen Helderman
Executive Director – Audit and Compliance Services (ACS)
Virginia Commonwealth University (VCU) and VCU Health Systems
918 West Franklin Street – Stokes House
Richmond, Virginia 23284

We have performed a Full External Quality Assessment Review (QAR) for the Virginia Commonwealth University and VCU Health Systems Audit and Management Services (AMS). We were engaged by AMS to conduct a Full External Quality Assessment Review. The primary objective of the QAR was to assess AMS's conformity to The Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing (Standards)* and the IIA's Code of Ethics and to determine whether AMS is meeting the needs of management.

Our external assessment, conducted during August and September 2019, consisted primarily of reviewing documents required by IIA standards and reports and other communications to management of both VCU and VCU Health Systems and their respective Boards. We also conducted surveys and interviews with various executives and senior leaders of VCU and VCU Health Systems, and employees of AMS.

Based on our assessment, AMS generally conforms to the *Standards*, which is the highest possible overall rating for a full external assessment. This report does contain a few recommendations which, if implemented, should improve the effectiveness and enhance the value of AMS and support conformity to the *Standards*.

Dixon Hughes Goodman LLP

Richmond, Virginia

Report on Full External Assessment of VCU and VCU Health Systems Audit and Management Services (AMS)

Contents	Page
Summary Assessment on the Conformance with the <i>Standards</i> and the Code of Ethics	3
Objectives, Scope and Methodology	3
Observations Categories	4
Detail – Successful Internal Audit Practices	5
Detail – Gaps to Conformance with the <i>Standards</i> or the Code of Ethics	5
Detail – Opportunities for Continuous Improvement	5
Attachment A – Evaluation Summary and Ratings Definitions	8

Summary Assessment on the Conformance with the Standards and Code of Ethics

The *International Standards for the Professional Practice of Internal Auditing* requires that an external quality assessment review (QAR) of an internal audit activity must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization. The qualified assessor or assessment team must demonstrate competence in both the professional practice of internal auditing and the QAR process. We were selected by AMS to conduct a full external assessment of the VCU and VCU Health Systems AMS.

The AMS environment is well structured, where the *Standards* are understood, the Code of Ethics is being applied, and management endeavors to provide useful audit tools and implement appropriate practices. Consequently, comments and recommendations are intended to build on this foundation already in place in AMS.

Based on our assessment, AMS generally conforms with the *Standards* and the Code of Ethics. A detailed list of conformance with individual standards and the Code of Ethics is shown in Attachment A.

Objectives, Scope, and Methodology

Objectives

- Assess whether AMS was in general conformance with the Standards and the Code of Ethics.
- Identify successful internal audit practices demonstrated by AMS, gaps to conformance with the *Standards* and Code of Ethics, and opportunities for continuous improvement to enhance the efficiency and effectiveness of AMS.

Scope

- The scope of the QAR included AMS, as set forth in the internal audit charter and approved by the VCU and VCU Health Systems boards, which defines the purpose, authority, and responsibility of AMS.
- The QAR concluded on September 30, 2019 and provides senior management and the

- boards of VCU and VCU Health Systems with information about AMS as of that date.
- The *Standards* and the Code of Ethics in place and effective as of September 30, 2019, were the basis for the QAR.

Methodology

The following is a sample of key tasks we performed when conducting the QAR:

- Prepared a request list of required documentation.
- Identified key individuals at VCU and VCU Health System such as executive leadership, operating management, and other staff. Distributed surveys to the Internal Audit Leader, Internal Audit staff, and a sample of select individuals identified above. Surveys covered Internal Audit Governance, Internal Audit Staff, Internal Audit Management, and the Internal Audit Process.
- Summarized all survey responses and provided feedback to the Internal Audit Leader.
- Performed in-person interviews with select individuals identified above.
- Evaluated the Internal Audit function's audits and consulting engagements, reports, supporting documentation, policies, procedures, practices and records.
- Assessed the tools and techniques employed by the Internal Audit function.
- Assessed the mix of knowledge, experience, and disciplines within AMS staff.
- Evaluated reports and other communications with Management and the Board to assess the extent that the Internal Audit function meets objectives and adds value to the organization.
- Evaluated Internal Audit's conformance with the Standards, the Definition of Internal Auditing and the Code of Ethics.

Observation Categories

Observations are divided into three categories:

- **Successful Internal Audit Practices** – Areas where AMS is operating in a particularly effective or efficient manner when compared to the practice of internal auditing demonstrated in other internal audit activities. The identification of these items is intended to provide AMS stakeholders with a view by DHG on things AMS is doing in a leading practice manner when compared to other internal audit activities.

- **Gaps to Conformance with the *Standards* or the Code of Ethics** – Areas where AMS is operating in a manner that falls short of achieving one or more major objectives, with the *Standards* or the Code of Ethics that results in an opinion for an individual standard of “partially conforms” or “does not conform.” These items include recommendations offered to be implemented to achieve “generally in conformance” with the standard and include an AMS response and action plan to address the gap.
- **Opportunities for Continuous Improvement** – Observations of opportunities to enhance the efficiency or effectiveness of AMS’ infrastructure or processes. These items do not indicate a lack of conformance with the *Standards* or the Code of Ethics, but rather offer suggestions on how to better align with criteria defined in the *Standards* or the Code of Ethics. They may also be operational ideas based on the experiences of the external assessment team from working with other internal audit activities. A management response and an action plan to address each opportunity for continuous improvement noted is included.

Detail – Successful Internal Audit Practices

1. Based on the results of our interviews, it appears that AMS staff are good communicators, professional and knowledgeable of the areas that they are auditing. In addition, the Chief Audit Executive (CAE) is seen as an excellent communicator who can analyze complex situations and provide the respective Boards and the President with appropriate recommendations.
2. AMS played a major role with implementing an Enterprise Risk Management (ERM) program for the University. This program is widely regarded as a best practice for other universities in Virginia.

Detail – Gaps to Conformance with the *Standards* or the Code of Ethics

None noted

Detail – Opportunities for Continuous Improvement

1. During our analysis of eight audits, we found that two reports had audit findings that conflicted with the conclusion in the report. Specifically, the audit conclusions indicated that an objective

was satisfied, but the test work and “Other Business Issues” findings in the reports indicated that the objective was not satisfied.

Applicable Standards that Generally Conform:

- Standard 2310 – Identifying Information section B states “Sufficient information identified is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusion as the internal auditor.”
- Standard 2330 – Documenting Information section A states “Internal auditors document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions.”
- Standard 2410.A1 – Criteria for Communicating section B states “The final communication of engagement results includes applicable conclusions, as well as applicable recommendations and/or action plans.”
- Standard 2420 – Quality of Communications section A states “Communications are accurate, free from errors and distortions, and are faithful to the underlying facts.”
- Standard 2450 – Overall Opinions section A states “When an overall opinion is issued, it takes into account the expectations of senior management, the board, and other stakeholders, and it is supported by sufficient, reliable, relevant, and useful information.”

Note: In Attachment A, none of the standards are listed as Partially Conforms (PC). This is because all the above standards have multiple sections that AMS was rated as Generally Conforms (GC) and therefore we assigned an overall rating of GC for these standards.

Recommendation:

We recommend that AMS ensure that audit findings are properly reflected in the conclusion section of the audit report and that the conclusion agrees with the test work that was completed.

AMS Response and Action Plan:

Concur – For the two exceptions that were identified, the exceptions related to the same type of finding that had been previously communicated to the board in another audit. While audits were being performed for each of the report’s respective areas, AMS evaluated

whether any progress had been made. Since no progress had been made, only management level findings were issued in order to not repeat a board finding which was already under follow-up review. While the focus was not to be repetitive to the board in this issue communication, the associated conclusion in each standalone report did appear to be misrepresented. AMS will re-evaluate this communication process to ensure that each standalone report reflect the conclusion to each objective appropriately or the objective will be qualified.

2. Standard 1200 Proficiency and Due Professional Care checklist for conformance section 9a states “Evaluate whether the performance appraisal process is linked to continuing professional development. Review performance appraisal templates. Are development plans a required element?” as a measure to determine conformance with Standard 1200:

After every audit, surveys are sent to management for feedback, but the results are not routinely shared with the auditors who performed the audit. Based on interviews with AMS staff, they stated that they do not receive audit survey results routinely and felt that receiving this information would help them know what areas to improve on for future audits.

Recommendation:

We recommend that AMS management share the summary results of the management surveys with AMS staff.

AMS Response and Action Plan:

Concur – During the transition between ACS Executive Directors, audit survey results were not communicated timely to staff. This communication will be achieved as survey results are obtained in future audits.

Attachment A – Evaluation Summary and Rating Definitions

	GC	PC	DNC
Overall Evaluation	✓		

Attribute Standards (1000 through 1300)		GC	PC	DNC
1000	Purpose, Authority, and Responsibility	✓		
1010	Recognizing Mandatory Guidance in the Internal Audit Charter	✓		
1100	Independence and Objectivity	✓		
1110	Organizational Independence	✓		
1111	Direct Interaction with the Board	✓		
1112	Chief Audit Executive Roles Beyond Internal Auditing	✓		
1120	Individual Objectivity	✓		
1130	Impairment to Independence or Objectivity	✓		
1200	Proficiency and Due Professional Care	✓		
1210	Proficiency	✓		
1220	Due Professional Care	✓		
1230	Continuing Professional Development	✓		
		GC	PC	DNC
1300	Quality Assurance and Improvement Program	✓		

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 <i>International Standards for the Professional Practice of Internal Auditing</i> ”	✓		
1322	Disclosure of Nonconformance	✓		

Performance Standards (2000 through 2600)		GC	PC	DNC
2000	Managing the Internal Audit Activity	✓		
2010	Planning	✓		
2020	Communication and Approval	✓		
2030	Resource Management	✓		
2040	Policies and Procedures	✓		
2050	Coordination and Reliance	✓		
2060	Reporting to Senior Management and the Board	✓		
2070	External Service Provider and Organizational Responsibility for Internal Auditing	✓		
2100	Nature of Work	✓		

2110	Governance	✓		
2120	Risk Management	✓		
2130	Control	✓		
2200	Engagement Planning	✓		
2201	Planning Considerations	✓		
2210	Engagement Objectives	✓		
2220	Engagement Scope	✓		
2230	Engagement Resource Allocation	✓		
2240	Engagement Work Program	✓		
2300	Performing the Engagement	✓		
2310	Identifying Information	✓		
2320	Analysis and Evaluation	✓		
2330	Documenting Information	✓		
2340	Engagement Supervision	✓		
2400	Communicating Results	✓		
2410	Criteria for Communicating	✓		
2420	Quality of Communications	✓		
2421	Errors and Omissions	✓		
2430	Use of "Conducted in Conformance with the	✓		

	<i>International Standards for the Professional Practice of Internal Auditing</i>			
2431	Engagement Disclosure of Nonconformance	N/A	N/A	N/A
2440	Disseminating Results	✓		
2450	Overall Opinions	✓		
2500	Monitoring Progress	✓		
2600	Communicating the Acceptance of Risks	✓		

Code of Ethics		GC	PC	DNC
	Code of Ethics	✓		

Rating Definitions

GC – “Generally Conforms” means that the assessor or the assessment team has concluded that the relevant structures, policies, and procedures of the activity, as well as the processes by which they are applied, comply with the requirements of the individual standard or elements of the Code of Ethics in all material respects. For the sections and major categories, this means that there is general conformity to a majority of the individual Standard or element of the Code of Ethics and at least partial conformity to the others within the section/category. There may be significant opportunities for improvement, but these should not represent situations where the activity has not implemented the *Standards* or the Code of Ethics, and has not applied them effectively or achieved their stated objectives. As indicated above, general conformance does not require complete or perfect conformance, the ideal situation, or successful practice, etc.

PC – “Partially Conforms” means that the assessor or assessment team has concluded that the activity is making good-faith efforts to comply with the requirements of the individual standard or elements of the Code of Ethics or a section or major category, but falls short of achieving some major objectives. These will usually represent significant opportunities for improvement in effectively applying the *Standards* or the Code of Ethics and/or achieving their objectives. Some deficiencies may be beyond the control of the internal audit activity and may result in recommendations to senior management or the board of the organization.

DNC – “Does Not Conform” means that the assessor or assessment team has concluded that the internal audit activity is not aware of, is not making good-faith efforts to comply with, or is failing to achieve many or all of the objectives of the individual standard or element of the Code of Ethics or a section or major category. These deficiencies will usually have a significantly negative impact on the internal audit activity’s effectiveness and its potential to add value to the organization. These may also represent significant opportunities for improvement, including actions by senior management or the board.

DHG

DIXON HUGHES GOODMAN LLP

BEN SADY
Principal
Risk Advisory Services
Ben.Sady@dhg.com
804.474.1267

CHRIS KALAFATIS
Senior Manager
Risk Advisory Services
Chris.Kalafatis@dhg.com
804.474.1270

901 East Cary Street, Suite 1000, Richmond, VA 23219 | 804.282.7636 | dhg.com



VCU

Response Plan to Recommendations Resulting from Institutional Ethics and Compliance Program Design & Effectiveness

The chart below shows all itemized recommendations and our responses, including a plan of action. We ranked the recommendations using risk-based ranking criteria and available resources to establish the following tiers:

Tier 1 - actions have begun or will begin in FY20, to be completed by end of FY21

Tier 2 - actions are anticipated to begin in FY21 and completed by FY22-23

Tier 3 - actions are considered reaching the most mature point of a compliance program. We will assess these recommendations in FY22 and choose whether to begin an action or defer.

This update reports on the status of Tier 1 items only. Future updates will incorporate Tier 2 and 3 as their due dates draw closer.

Tier	Program Element Recommendation	Response to Recommendation	Status
Program Resources and Structure: 6 Recommendations			
1	Include the CECO in Cabinet level and senior staff meetings to provide program updates and coordinate with senior-most leaders.	Agreed. Cabinet access provided by the Executive Director of ACS who will coordinate with the CECO position as needed. Other senior staff meeting agendas are open for requests.	Complete
1	Document the access of the CECO to the appropriate committee of the Board of Visitors and the frequency with which the CECO should provide updates to that committee.	Agreed. Access is provided in practice but not documented to the expected level of detail. To be documented in the May 2020 update to AICC meeting planner and charter and ACS departmental charter.	On Schedule
2	Evaluate ICS staffing levels, given disparity between VCU and relevant peer groups. Consider the addition of 1 or 2 FTEs or grad-level intern program.	Delayed, resource issue. Developing a list of potential risk due to staffing limitations or funding limitations. In the interim, initiatives (work plans) and annual goals are leveraged against risk based needs and available staffing. The AICC will remain apprised of status and any unmitigated risks.	
3	Implement an ambassador program for Ethics and Compliance	Delayed, resource issue. Low risk, high reward if properly supported and incented.	

1	Continue to ensure effective use of the Compliance Advisory Committee (CAC) to address the possibility of silos of expertise as highlighted in the ERM section of the Integrity and Compliance Annual Report.	Agreed. Formalization of E&C function continues to support this recommendation – for example: inclusion of function in strategic university affairs; formal charter for the E&C function and oversight committee supplying regular reports to senior leadership.	On Schedule
1	Consider whether smaller CAC groupings for specific topics (subcommittees) might further work.	Agreed. Active for both training curriculum and communications per other recommendations. Safety, Conflicts of Interest and Improper Foreign Influence are pending.	On Schedule
Perceptions of Ethical Culture: 2 Recommendations			
3	Enhance the presence of leadership in training courses.	Delayed. Leadership presence is included in some training courses with planned expansion as we create new curriculum.	
1	Expand demographics and enhance participation in future culture survey initiatives.	Agreed. Have commitments to partner and share results with HR, Inclusive Excellence and Institutional Research.	Complete
Written Standards: 7 Recommendations			
-	Make Code of Conduct readily available on VCU's website on the home page or "Mission and History" page.	Disagreed. The Code is placed on the faculty and staff homepage as this is the audience to whom it most relates.	N/A
1	Consider addressing additional risk areas.	Agreed. An Ethics and Compliance Dashboard Initiative is underway which will help identify risk. E&C also has presence at ERM meetings to increase risk awareness.	On Schedule
-	Revise Code of Conduct to lower grade level and simplify language.	Disagreed. Readability is acceptable to our audience. Concepts like retaliation, Export Controls, International Presence and Foreign Corrupt Practices Act cause the readability score to rise.	N/A
1	Move the "decoding our code" page to the beginning.	Completed.	Complete
-	Lower grade level of policies.	Disagreed. Readability statistics are provided to policy drafters during review phase, goal is 11 th grade reading level. Some topics cause the readability score to rise.	N/A
1	Develop a Foreign Corrupt Practices Act or anti-bribery policy.	Agreed. In progress with Global Education Office.	On Schedule
1	Create a true Supplier Code of Conduct.	Agreed. In progress with Procurement Office.	On Schedule
Training & Communication: 9 Recommendations			
1	Create a multi-year training plan/curriculum and schedule.	Agreed. In progress. Training needs survey responses returned and currently being assessed.	On Schedule

2	Keep learners engaged through mature training mechanisms such as progressive course difficulty, pre-tests and self-directed topics.	Delayed, resource issue. Some aspects of this are implemented however not systemically.	
1	Review current systems to identify places where “just in time” training can be deployed.	Agreed. In progress with interdisciplinary group, subcommittee of CAC.	On Schedule
3	Use positive incentives to encourage training completion such as a reward for departments who complete the training first; consider an initiative that is led by senior personnel.	Delayed, resource issue.	
1 to 2	Further equip managers with information (and resources) about their responsibilities to support the program by means of a learning curriculum for current managers and onboarding new managers, as well as periodic refreshers; link completion to the performance evaluation.	Delayed, resource issue and complexity of recommendation. Efforts are being made to document required reporting of certain information and formalization of the ethics and compliance program responsibilities within the broader university community. Combining efforts with Human Resources and other training focused initiatives to develop and deliver curriculum for managers.	
3	Establish a mentor program for experienced managers to mentor newer managers.	Delayed, due to low risk.	
2	Deploy a two-year, cross-functional communications plan that incorporates training and communications strategies together.	Agreed. In progress with interdisciplinary group, subcommittees of CAC. Efforts needed before a coordinated plan can be finalized.	
3	Leverage the relationship with other leaders to diversify the voices delivering the integrity message around VCU.	Delayed. We are actively leveraging communication channels, such as the President’s Blog and compliance videos. More initiatives will occur as we develop new training curriculum.	
2	Measure training effectiveness through a routine survey to compliance partners asking for topics they are receiving the most questions about; spot-quizzes to employees to check for retention and/or click rates for policies and resources.	Delayed, due to low risk.	
Risk Assessment, Monitoring & Auditing: 8 Recommendations			
1	Bolster the current risk assessment process using systematic metrics, such as usage of ICS resources; consider adding questions to internal audits to assess awareness.	Agreed. Developed collective E&C Dashboard that Compliance Partners will use to measure the program. Metrics will focus on deviations from medians and benchmarks from peers. CECO also included in ERM and internal audit planning sessions.	Complete

2	Identify places where budget and risk appetite could be more closely aligned to bolster risk assessments.	Delayed, resource issue. Working with ERM and Internal Audit to increase understanding of high risk compliance areas.	
2	Perform root cause analysis on all substantiated and unsubstantiated cases.	Delayed. Insufficient resources to perform root cause analysis on unsubstantiated cases. Root cause analysis will be emphasized in response to recommendation below calling for us to develop a unified investigation process.	
1	Continue work to integrate case management systems so there is one system of record; if multiple systems are used, ensure rigorous coordination.	Agreed. Working to formalize the compliance program, including the mandated use of the case management system unless formal exception is granted. Ongoing consideration of merging student case management system into the larger, university-wide system, Convercent. This consolidation would entail an additional cost as well as the need to for additional reporting features, benchmarking, insights and lines of sight for responsible leadership in these areas.	On Schedule
1	Develop a unified investigation process.	Agreed. A policy setting unified and consistent minimum standards related to this work is in progress. The policy will include root cause analysis.	On Schedule
2	Ensure consistent root cause designation for all cases.	Duplicate item from above. Delayed – Insufficient resources to perform root cause analysis on unsubstantiated cases. Root cause analysis will be emphasized in response to recommendation above calling for us to develop a unified investigation process.	
1	Develop an online proxy report pathway for all managers.	Agreed. Pathway exists, however decisions need to be made regarding training and support and then roll out and a communication plan.	On Schedule
1	Continue implementation of new processes around individual and institutional conflicts of interest monitoring.	Agreed. Currently in pilot phase. E&C Annual Training provided in Fall 2019 will be on identification and disclosure of conflicts of interest.	Complete
Enforcement, Discipline & Incentives: 2 Recommendations			
1	Provide all managers with standalone manager-specific training on retaliation.	Agreed. Scheduled for delivery Spring/Summer 2020. Fall 2019 training will focus on Conflicts of Interest for all employees.	On Schedule
1	Review the current ways in which VCU is monitoring those employees who raise concerns for indications of retaliation across reporting channels, and consider a process where the organization explicitly and regularly checks back in with those individuals after the close of an investigation.	Agreed. Completed for investigations conducted by ICS and working with other functional and operations areas to monitor and share information this with ICS.	On Schedule

Audit and Management Services
Status of Fiscal Year 2019-2020 Audit Work Plan
November 30, 2019

Area	Status
<u>Risk-based Audits</u>	
Prior Workplan: Network Management and Security	Completed
Prior Workplan: School of Medicine – Cardiology - Consolidated	Completed
Prior Workplan: Student Fees	Completed
Prior Workplan: Technology Services Desktop Services Operations and Systems	Completed
Prior Workplan: Human Resources – Separations	Completed
IT Facilities Management Department Systems	In Progress
Budget and Resource Analysis	In Progress
Division of Inclusive Excellence	In Progress
Engineering and Utilities	Not Started
Degree Conference and Award	Not Started
VCU Card Office	Not Started
Office of Research and Innovation – Integrity and Compliance	Not Started
School of Dentistry	Not Started
Auxiliary Operations Forecasting	Not Started
Siegel Center Operations and Athletics Fiscal Processes	Not Started
IT Authentication Systems Management	Not Started
IT Office of Research and Innovation Technology	Not Started
IT Integrated Systems/ERP Management and Security	Not Started
Office of Strategic Enrollment Management	Postponed

Audit and Management Services
Status of Fiscal Year 2019-2020 Audit Work Plan
November 30, 2019

<u>Annual Engagements and Activities</u>	
Follow-Ups on Audit Recommendations Outstanding – FY19	Completed
Review of President’s Discretionary Accounts – FY18	Completed
Athletics – Year 3 NCAA Compliance Review	Completed
Review of President’s Discretionary Accounts – FY19 and Leave Analysis	Completed
VCU Police Department – Review of Evidence Room – Part 1	Completed
Follow-Ups on Audit Recommendations Outstanding – FY20	In Progress
ERM Emergency Preparedness – Selected Mitigation Controls Review	In Progress
VCU Police Department – Review of Evidence Room – Part 2	Not Started
Risk Assessment – FY21	Not Started
IT Technology Services Risk Assessment Management	Not Started

Special Project	Status
<u>Continuing Projects</u>	
State Employees Fraud, Waste, and Abuse Hotline	In Progress – 1; Closed – 1
<u>Other Projects</u>	
Prior Workplan: Enterprise Centers and Institutes	Completed
Financial Aid Work Study	Completed
Department of Psychology Purchase Card	Completed
College of Engineering Lab Usage	In Progress
Purchase Card PayPal and Amazon Analysis	In Progress
Authentication of Vendor Information	In Progress
Web Services and Application Security – Special Project	In Progress
University Internet of Things (IoT) – Special Project	Cancelled

DIRECTOR LIABILITY DEVELOPMENTS

The Delaware courts are sending an important new message on their expectations for boardroom attentiveness, and it's a message that corporate directors, executives and their advisors should take seriously.

For more than 20 years, those courts have applied the director-friendly *Caremark* standard of conduct for board risk-oversight duty. This standard of conduct supports the business judgment rule and requires allegations of bad faith in order to support a claim for breach of that duty by directors. Under that standard, misconduct could only be found (in simplest terms) if the directors either utterly failed to implement a risk information reporting system, or consciously failed to make sure that the system worked to get them the information they needed.

But that may now be changing, and not necessarily for the best interests of directors and their personal liability profile.

[Two recently decided Delaware cases](#) signal a significant shift in the application of the *Caremark* doctrine and its forgiving standard of director conduct. In both cases, the court allowed a breach of duty action to proceed based on allegations that the board missed or misinterpreted significant “red flags” of compliance problems. The fact that a compliance plan was actually in place wasn't enough to provide a defense for the board. The courts focused more on the quality of the plan and on the quality of the board's attentiveness, respectively. That's both new and disturbing.

The concerns raised in these cases can be addressed through a series of measures focusing on greater director engagement in oversight and monitoring activity, and increased board sensitivity for possible red flags. The health system's chief legal officer can be a significant resource in developing a plan of response for the board.

“Corporate Law & Governance Update: November 2019.” *McDermott Will & Emery*, Nov. 2019, <https://www.mwe.com/insights/corporate-law-governance-update-november-2019/>.



Board of Visitors
Audit, Integrity, and Compliance Committee
December 13, 2019



VCU

Agenda

1. Call to Order
2. Approval of Agenda
3. Approval of Minutes (September 13, 2019)
4. Approval of Revised Dashboard Measures
5. Auditor of Public Accounts – Audit Results FY2019
6. Data Governance Update
7. Report from Executive Director ACS

Item 2 – Approval of Agenda

- Audit, Integrity and Compliance Committee Meeting December 13, 2019
- Motion to approve the agenda

Item 3 – Approval of Minutes

- Audit, Integrity and Compliance Committee Meeting held on September 13, 2019
- Motion to approve the Minutes

Item 4 – Approval of Revised AIC Committee Dashboard Measures

Current Proposed

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

Item 5 – Auditor of Public Accounts (APA) Mike Reinholtz, Audit Director

Annual Audit for Year Ended June 30, 2019

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

Item 6 - Data & Information Management Council (DIMC)

**Board of Visitors – Audit, Integrity and Compliance Committee
December 13, 2019**

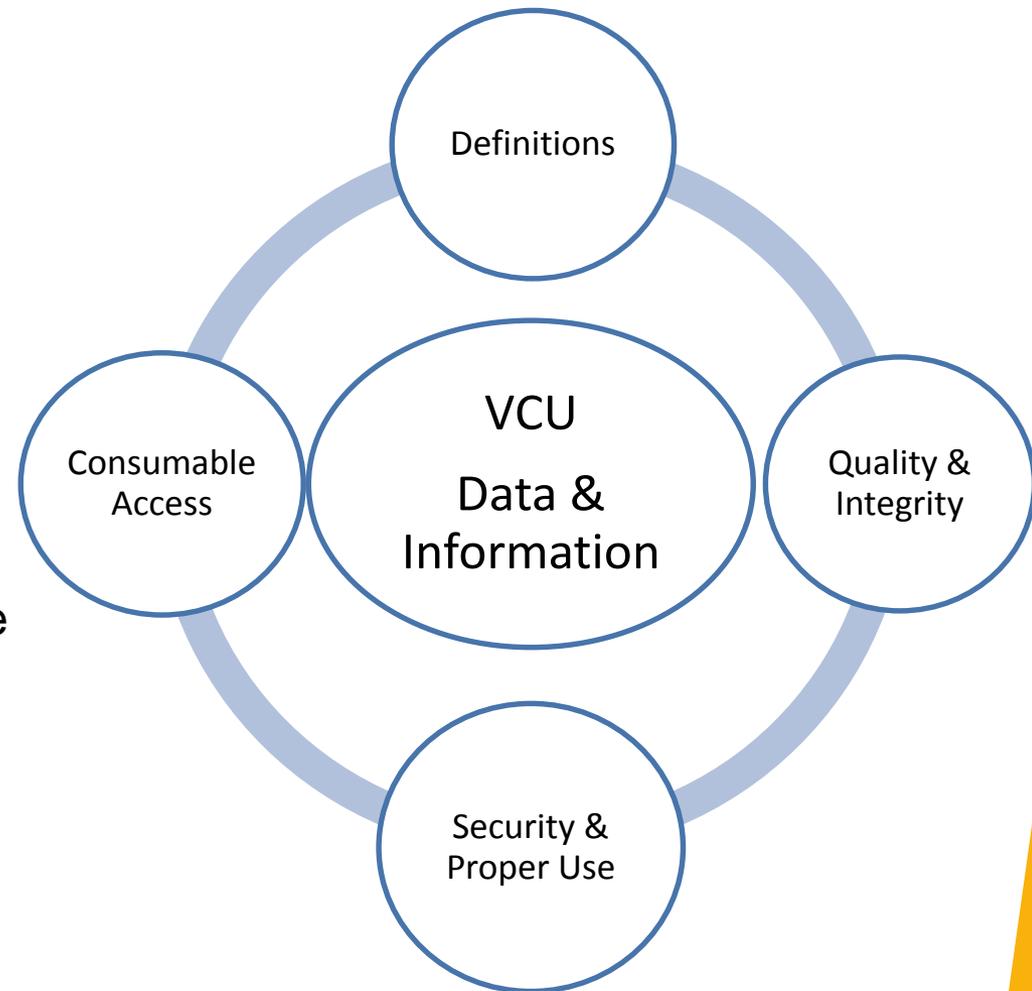
Monal Patel
Alex Henson



What is DIMC

In other words, what is data governance?

- Data governance is a business program; it adds value to the organization.
- A holistic effort requiring enterprise attention
- The program results in business practices and policies aimed to manage data as an institutional asset
- The program transforms authoritative data into meaningful information



Why data governance at VCU?

- Higher education institutions disseminate knowledge. It is imperative that institutions build a program to ensure accurate dissemination of operational knowledge to support data driven decisions.
- Historically, domain experts were called upon to share information. Consumers are now used to having information readily available. The switch to an information on-demand environment created DIMC with the following charge:
 1. Establish data as a trusted institutional asset to further VCU's mission and to advance knowledge and student success.
 2. Institute and manage policies, processes, structures and definitions that support effective decision-support, university-wide collaboration and operational efficiency.
 3. Improve the security, integration, accessibility, quality, transparency, and consistency of data across the institution.

DIMC beginnings

Charge

- December 4, 2015
- Authority to make decisions
- Form a structure, task forces, necessary committees
- Protect our data asset

Foundation

- 2016-2017
- Developed initial data stewardship framework
- First draft of institutional data map
- Banner System Revitalization project

Building

- 2017-2018
- Preliminary data management strategy
- Progress with dashboards
- Dean's New Budget Model dashboard and first comprehensive enrollment dashboards

2019 Key Milestones

Revision of Charter

Goals

- To reduce overhead from a 40+ member committee
- Create well defined operating procedures for clarity

Results

- 12 member decision-making Steering Committee
- Tasks groups on demand

Approved Policy

Goals

- Necessity of a policy to enforce governance procedures
- Define DIMC's role and authority

Results

- Aligned Policy with revised Charter
- Approved policy as of November 2019

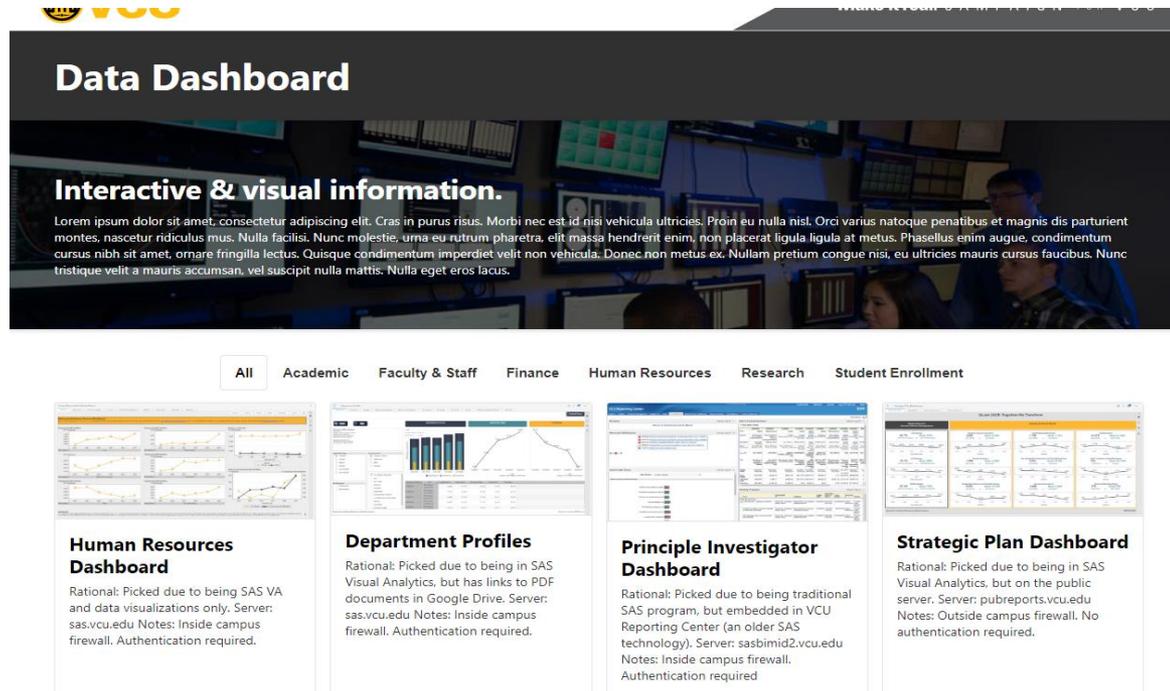
2019 Key Milestones

Creation of a Dashboard Portal – data.vcu.edu

Goals

- One stop for all authoritative information
- Identify and enforce gatekeeping criteria for dashboard entry into the portal
- Communicate often, encourage use of the portal to reduce shadow information sources

Results:



The screenshot displays the 'Data Dashboard' portal. At the top, there is a navigation bar with tabs for 'All', 'Academic', 'Faculty & Staff', 'Finance', 'Human Resources', 'Research', and 'Student Enrollment'. Below the navigation bar, there are four main dashboard sections, each with a title, a brief description, and a 'Rational' section explaining why it was selected. The sections are: 'Human Resources Dashboard', 'Department Profiles', 'Principle Investigator Dashboard', and 'Strategic Plan Dashboard'. Each section includes a small thumbnail image of the dashboard content.

Data Dashboard

Interactive & visual information.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras in purus risus. Morbi nec est id nisi vehicula ultricies. Proin eu nulla nisl. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Nulla facilisi. Nunc molestie, urna eu rutrum pharetra, elit massa hendrerit enim, non placerat ligula ligula at metus. Phasellus enim augue, condimentum cursus nibh sit amet, ornare fringilla lectus. Quisque condimentum imperdiet velit non vehicula. Donec non metus ex. Nullam pretium congue nisi, eu ultricies mauris cursus faucibus. Nunc tristique velit a mauris accumsan, vel suscipit nulla mattis. Nulla eget eros lacus.

Human Resources Dashboard

Rational: Picked due to being SAS VA and data visualizations only. Server: sas.vcu.edu Notes: Inside campus firewall. Authentication required.

Department Profiles

Rational: Picked due to being in SAS Visual Analytics, but has links to PDF documents in Google Drive. Server: sas.vcu.edu Notes: Inside campus firewall. Authentication required.

Principle Investigator Dashboard

Rational: Picked due to being traditional SAS program, but embedded in VCU Reporting Center (an older SAS technology). Server: sasbimid2.vcu.edu Notes: Inside campus firewall. Authentication required.

Strategic Plan Dashboard

Rational: Picked due to being in SAS Visual Analytics, but on the public server. Server: pubreports.vcu.edu Notes: Outside campus firewall. No authentication required.

2019 Key Milestones

Creation of a Data Steward Resource Site

Goals

- Establish a program to mitigate data/information security risks
- One stop for all data handling procedures, information security rules and regulations
- Provide training sessions often
- Coordinate data stewards across campus
- Integrate data stewards as a primary partner for DIMC

Results:

- Website has been created
- Ongoing efforts to task data stewards
- Ongoing efforts to establish data steward role in HR

DIMC 2020 and beyond

Critical evaluation of institutional definitions

Goals

- Position the campus on the same footing by declaring official definitions
- Vet the methodology
- Collaborative approach to consensus building

Results

- Possible first DIMC approved definition (online section, program, student)
- Formalized process for future declarations of official definitions
- Link dashboards to the official definition

Thoughts?

Creation of a dashboard portal and data steward toolkit are actionable outcomes from VCU's data governance program. Is an immediate outcomes based approach a viable strategy? What are the unintended consequences?

A data governance program is more about inserting additional processes to the existing way we do business. It can be invasive. In what ways can the program become non-invasive so that data governance is part of the culture?

Item 7a - External Quality Assessment

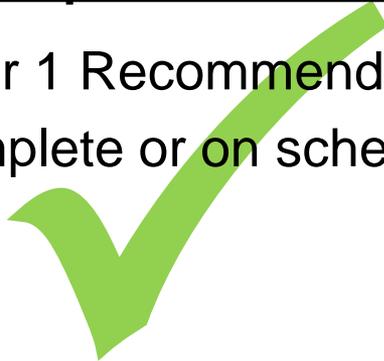


Item 7b - Effectiveness Response Plan

Item 7c - Audit Work Plan

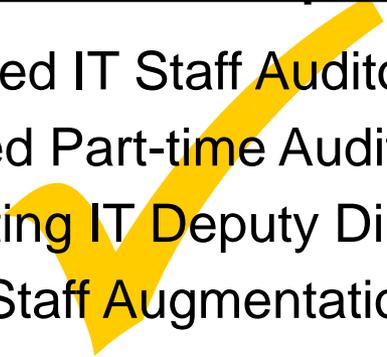
Effectiveness Report Response Plan

All Tier 1 Recommendations
complete or on schedule



Audit work plan

Hired IT Staff Auditor
Hired Part-time Auditor
Recruiting IT Deputy Director
IT Staff Augmentation



Closed Session

Item 8 - Closed Session Agenda

- a) University Counsel Update
- b) Audit Report for Information
- c) Audit Reports for Discussion

University Counsel Update



Annual Review of President's Discretionary Accounts

- Scope expanded to include leave reporting
- Review objectives met
- No issues

ACH Corrective Action - Status Update

- In March 2019 Committee informed:
 - Treasury and Finance modifying ACH controls
 - Internal audit to report at December 2019 committee meeting
- Treasury and Finance improvements are underway
 - ACH payee process “locked down” & all current payees validated (March 2019)
 - Treasury and Technology Services (IT Security & Administrative Systems) investigated available improvements to existing Wells Fargo system and found that Wells Fargo’s available solutions were insufficient (June 2019)
- Internal audit review is on hold
 - Banking services RFP issued in December 2019; award contract by May 2020
 - Audit ACH controls in FY21 approved audit work plan

ACH Corrective Action - Status Update

- Treasury has temporarily suspended the enrollment of new ACH payees and has validated all current ACH payees.
- New vendors are receiving checks, which are protected by positive pay.
- Bank services RFP has been issued, a primary requirement of which is validation and security of electronic payees.
- Industry best practices are to remove VCU employees from the process of entering or updating payees' bank account information, placing this risk solely between the payee and the bank.

Audit of Selected Employment Separation Processes



U.S. Citizenship and
Immigration Services

GEO did not report H1B employee separations in FY19

- Notify USCIS of separations
- Collaborate with HR to use software solution

Audit of Desktop Service Delivery



Improve Local Liaison Managed Workstations

Findings

- No listing of managed workstations
- Missing security compliance evidence
- Little security training and oversight

Recommendations

- Maintain workstation listing
- Monitor workstation patching and risks
- Provide security training
- Analyze cost/benefit/risk of local liaison model and consider removing this option

Executive Session