AGENDA

1. CALL TO ORDER
   Pamela El, Vice Chair

2. APPROVAL OF AGENDA
   Pamela El, Vice Chair

3. APPROVAL OF MINUTES
   (December 13, 2019)
   Pamela El, Vice Chair

4. REVIEW OF DASHBOARD MEASURES
   Karen Helderman, Executive Director
   Audit and Compliance Services
   Alex Henson, Chief Information Officer

5. ERM UPDATE
   Thomas Briggs
   Assistant Vice President
   Safety and Risk Management

6. REPORT FROM THE EXECUTIVE DIRECTOR OF
   AUDIT AND COMPLIANCE SERVICES
   a. Status of Annual Interest Disclosure for VCU and
      Commonwealth of Virginia Conflicts of Interest
   b. Ethics and Compliance Effectiveness Report Update
   c. Audit Work Plan Status FY20
   Karen Helderman, Executive Director
   Audit and Compliance Services

7. DATA SECURITY UPDATE
   Alex Henson, Chief Information Officer
CLOSED SESSION
Freedom of Information Act Sections 2.2-3711(A)
(1) (7) (8) and (19), specifically:

8. **DATA SECURITY UPDATE - continued**
   - Alex Henson, Chief Information Officer

9. **AUDIT REPORT FOR INFORMATION**
   - Review of President’s Discretionary Funds
   - Karen Helderman, Executive Director
     Audit and Compliance Services

10. **AUDIT REPORTS FOR DISCUSSION**
    - ACH Corrective Action – Status Update
    - Selected Employment Separation Processes
    - Desktop Service Delivery
    - Facilities Management IT Systems
    - Karen Helderman, Executive Director
      Audit and Compliance Services

EXECUTIVE SESSION

RETURN TO OPEN SESSION AND CERTIFICATION
   - Pamela El, Vice Chair
     Approval of Committee action on matters discussed in closed session, if necessary

ADJOURNMENT
   - Pamela El, Vice Chair
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

There have been no significant security incidents since our last meeting. The most prevalent threat continues to be targeted phishing scams, most of which attempt to trick individual employees into buying gift cards. Through the expansion of simulated phishing emails, training, and actively marketing our Security Heroes program, we continue to be successful in responding quickly to these types of threats and minimizing compromised accounts. We are also working to decommission or isolate from the campus network any computers still running Microsoft Windows 7, which is now unsupported and therefore less secure. We have relatively few of these devices on the network and other mitigation strategies in place, but this does take resources and effort.

From the network security perspective, we continuously see scanning activities and exploitation attempts from various areas around the world, and we continuously monitor and assess our environment and address existing and newly developing vulnerabilities. Continuous improvements in our next generation firewall (installed over the summer) and an improved Security Information and Event Management (SIEM) system have enhanced our team’s ability to monitor for and address threats. There are currently no signs of compromise or activities specifically targeting VCU.

ERM PROGRAM

- Status of ERM mitigation plans
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

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. Compliance Services continues to address the needed infrastructure improvements as part of the response plan to the Ethisphere external review completed in Spring 2019.
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.**

<table>
<thead>
<tr>
<th>Tier</th>
<th>Program Element Recommendation</th>
<th>Response to Recommendation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Include the CECO in Cabinet level and senior staff meetings to provide program updates and coordinate with senior-most leaders.</td>
<td>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.</td>
<td><strong>Complete</strong></td>
</tr>
<tr>
<td><strong>1</strong></td>
<td>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.</td>
<td>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.</td>
<td><strong>On Schedule</strong></td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>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.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Implement an ambassador program for Ethics and Compliance</td>
<td>Delayed, resource issue. Low risk, high reward if properly supported and incented.</td>
<td></td>
</tr>
<tr>
<td>#</td>
<td>Recommendation</td>
<td>Status/Agreement</td>
<td>Completion Status</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>1</td>
<td>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.</td>
<td>Agreed. Formalization of E&amp;C function continues to support this recommendation – for example: inclusion of function in strategic university affairs; formal charter for the E&amp;C function and oversight committee supplying regular reports to senior leadership.</td>
<td>On Schedule</td>
</tr>
<tr>
<td>1</td>
<td>Consider whether smaller CAC groupings for specific topics (subcommittees) might further work.</td>
<td>Agreed. Active for both training curriculum and communications per other recommendations. Safety, Conflicts of Interest and Improper Foreign Influence are pending.</td>
<td>On Schedule</td>
</tr>
<tr>
<td></td>
<td><strong>Perceptions of Ethical Culture: 2 Recommendations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Enhance the presence of leadership in training courses.</td>
<td>Delayed. Leadership presence is included in some training courses with planned expansion as we create new curriculum.</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Expand demographics and enhance participation in future culture survey initiatives.</td>
<td>Agreed. Have commitments to partner and share results with HR, Inclusive Excellence and Institutional Research.</td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td><strong>Written Standards: 7 Recommendations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Make Code of Conduct readily available on VCU's website on the home page or &quot;Mission and History&quot; page.</td>
<td>Disagreed. The Code is placed on the faculty and staff homepage as this is the audience to whom it most relates.</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>Consider addressing additional risk areas.</td>
<td>Agreed. An Ethics and Compliance Dashboard Initiative is underway which will help identify risk. E&amp;C also has presence at ERM meetings to increase risk awareness.</td>
<td>On Schedule</td>
</tr>
<tr>
<td>-</td>
<td>Revise Code of Conduct to lower grade level and simplify language.</td>
<td>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.</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>Move the &quot;decoding our code&quot; page to the beginning. -----------------------------------------------------------------------------------</td>
<td>Completed.</td>
<td>Complete</td>
</tr>
<tr>
<td>-</td>
<td>Lower grade level of policies.</td>
<td>Disagreed. Readability statistics are provided to policy drafters during review phase, goal is 11th grade reading level. Some topics cause the readability score to rise.</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>Develop a Foreign Corrupt Practices Act or anti-bribery policy.</td>
<td>Agreed. In progress with Global Education Office.</td>
<td>On Schedule</td>
</tr>
<tr>
<td>1</td>
<td>Create a true Supplier Code of Conduct.</td>
<td>Agreed. In progress with Procurement Office.</td>
<td>On Schedule</td>
</tr>
<tr>
<td></td>
<td><strong>Training &amp; Communication: 9 Recommendations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Create a multi-year training plan/curriculum and schedule.</td>
<td>Agreed. In progress. Training needs survey responses returned and currently being assessed.</td>
<td>On Schedule</td>
</tr>
<tr>
<td></td>
<td>Keep learners engaged through mature training mechanisms such as progressive course difficulty, pre-tests and self-directed topics.</td>
<td>Delayed, resource issue. Some aspects of this are implemented however not systemically.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Review current systems to identify places where “just in time” training can be deployed.</td>
<td>Agreed. In progress with interdisciplinary group, subcommittee of CAC. On Schedule</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
<td>Delayed, resource issue.</td>
<td></td>
</tr>
<tr>
<td>1 to 2</td>
<td>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.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Establish a mentor program for experienced managers to mentor newer managers.</td>
<td>Delayed, due to low risk.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Deploy a two-year, cross-functional communications plan that incorporates training and communications strategies together.</td>
<td>Agreed. In progress with interdisciplinary group, subcommittees of CAC. Efforts needed before a coordinated plan can be finalized.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Leverage the relationship with other leaders to diversify the voices delivering the integrity message around VCU.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>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.</td>
<td>Delayed, due to low risk.</td>
<td></td>
</tr>
</tbody>
</table>

### Risk Assessment, Monitoring & Auditing: 8 Recommendations

|   | 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 |

February 2020 AICC Update
<table>
<thead>
<tr>
<th></th>
<th>Identify places where budget and risk appetite could be more closely aligned to bolster risk assessments.</th>
<th>Delayed, resource issue. Working with ERM and Internal Audit to increase understanding of high risk compliance areas.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Perform root cause analysis on all substantiated and unsubstantiated cases.</td>
<td>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.</td>
</tr>
<tr>
<td>1</td>
<td>Continue work to integrate case management systems so there is one system of record; if multiple systems are used, ensure rigorous coordination.</td>
<td>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.</td>
</tr>
<tr>
<td>1</td>
<td>Develop a unified investigation process.</td>
<td>Agreed. A policy setting unified and consistent minimum standards related to this work is in progress. The policy will include root cause analysis.</td>
</tr>
<tr>
<td>2</td>
<td>Ensure consistent root cause designation for all cases.</td>
<td>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.</td>
</tr>
<tr>
<td>1</td>
<td>Develop an online proxy report pathway for all managers.</td>
<td>Agreed. Pathway exists, however decisions need to be made regarding training and support and then roll out and a communication plan.</td>
</tr>
<tr>
<td>1</td>
<td>Continue implementation of new processes around individual and institutional conflicts of interest monitoring.</td>
<td>Agreed. Currently in pilot phase. E&amp;C Annual Training provided in Fall 2019 will be on identification and disclosure of conflicts of interest.</td>
</tr>
</tbody>
</table>

**Enforcement, Discipline & Incentives: 2 Recommendations**

<table>
<thead>
<tr>
<th></th>
<th>Provide all managers with standalone manager-specific training on retaliation.</th>
<th>Agreed. Scheduled for delivery Spring/Summer 2020. Fall 2019 training will focus on Conflicts of Interest for all employees.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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.</td>
<td>Agreed. Completed for investigations conducted by ICS and working with other functional and operations areas to monitor and share information this with ICS.</td>
</tr>
</tbody>
</table>

February 2020 AICC Update
Audit and Management Services
Status of Fiscal Year 2019-2020 Audit Work Plan
January 31, 2019

<table>
<thead>
<tr>
<th>Risk-based Audits</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior Workplan: Network Management and Security</td>
<td>Completed</td>
</tr>
<tr>
<td>Prior Workplan: School of Medicine – Cardiology - Consolidated</td>
<td>Completed</td>
</tr>
<tr>
<td>Prior Workplan: Student Fees</td>
<td>Completed</td>
</tr>
<tr>
<td>Prior Workplan: Technology Services Desktop Services Operations and Systems</td>
<td>Completed</td>
</tr>
<tr>
<td>Prior Workplan: Human Resources – Separations</td>
<td>Completed</td>
</tr>
<tr>
<td>IT Facilities Management Department Systems</td>
<td>Completed</td>
</tr>
<tr>
<td>Budget and Resource Analysis</td>
<td>In Progress</td>
</tr>
<tr>
<td>Division of Inclusive Excellence</td>
<td>In Progress</td>
</tr>
<tr>
<td>Engineering and Utilities</td>
<td>Not Started</td>
</tr>
<tr>
<td>Degree Conference and Award</td>
<td>In Progress</td>
</tr>
<tr>
<td>VCU Card Office</td>
<td>Not Started</td>
</tr>
<tr>
<td>Office of Research and Innovation – Integrity and Compliance</td>
<td>Not Started</td>
</tr>
<tr>
<td>School of Dentistry</td>
<td>In Progress</td>
</tr>
<tr>
<td>Auxiliary Operations Forecasting</td>
<td>In Progress</td>
</tr>
<tr>
<td>Siegel Center Operations and Athletics Fiscal Processes</td>
<td>Not Started</td>
</tr>
<tr>
<td>IT Authentication Systems Management</td>
<td>Not Started</td>
</tr>
<tr>
<td>IT Office of Research and Innovation Technology</td>
<td>In Progress</td>
</tr>
<tr>
<td>IT Human Subjects Research Information Security</td>
<td>Proposed</td>
</tr>
<tr>
<td>IT Integrated Systems/ERP Management and Security</td>
<td>Postponed</td>
</tr>
<tr>
<td>Office of Strategic Enrollment Management</td>
<td>Postponed</td>
</tr>
</tbody>
</table>
## Audit and Management Services
### Status of Fiscal Year 2019-2020 Audit Work Plan
#### January 31, 2019

### Annual Engagements and Activities

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

### Special Project

<table>
<thead>
<tr>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Employees Fraud, Waste, and Abuse Hotline</td>
<td>In Progress – 0; Closed – 2</td>
</tr>
</tbody>
</table>

### Continuing Projects

<table>
<thead>
<tr>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Aid Work Study</td>
<td>Completed</td>
</tr>
<tr>
<td>Department of Psychology Purchase Card</td>
<td>Completed</td>
</tr>
<tr>
<td>College of Engineering Lab Usage</td>
<td>Completed</td>
</tr>
<tr>
<td>Purchase Card PayPal and Amazon Analysis</td>
<td>Completed</td>
</tr>
<tr>
<td>Authentication of Vendor Information</td>
<td>In Progress</td>
</tr>
<tr>
<td>Web Services and Application Security – Special Project</td>
<td>In Progress</td>
</tr>
<tr>
<td>University Internet of Things (IoT) – Special Project</td>
<td>Cancelled</td>
</tr>
</tbody>
</table>
Agenda

1. Call to Order
2. Approval of Agenda
3. Approval of Minutes (December 13, 2019)
4. Review of Dashboard Measures
5. ERM Update
6. Report from Executive Director ACS
7. Data Security Update
Approval of Agenda

• Audit, Integrity and Compliance Committee Meeting February 28, 2020

• Motion to approve the agenda
Approval of Minutes

• Audit, Integrity and Compliance Committee Meeting held on December 13, 2019

• Motion to approve the minutes
Committee Dashboard Measures

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

Risks reviewed on October, December and February include the following:

• Police and Emergency Preparedness (VP Administration)
• Academic Funding (Provost and SVP Finance and Budget)
• Strategic Plan Change Management (Provost)
• Improper Activities and Relationships Due to Foreign Influence (VP Research)
ERM Update

Risks that were revised and approved:
• Police and Emergency Preparedness (VP Administration)
• Improper Activities and Relationships Due to Foreign Influence (VP of Research)

Risks that are under review by Risk Owners for revision of controls:
• Academic Funding (Provost and SVP Finance and Budget)
• Strategic Plan Change Management (Provost)
ERM Update

Next Steps:

• Review and revise remaining risks, then present to Cabinet
• Begin new workshops with Risk Owners and Process Owners in April
• Initial audits of mitigation plans will be presented to ERM Steering Committee
Conflicts of Interest Update

- State Required Disclosure – **100% compliant**
- University Required Training & Disclosure

<table>
<thead>
<tr>
<th>VCU Training</th>
<th>VCU Disclosures</th>
<th>Research Training</th>
<th>Research Disclosures</th>
</tr>
</thead>
<tbody>
<tr>
<td>n=7759</td>
<td>n=647</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall – 89%</td>
<td>Overall – 94%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Position of Trust - 96%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(n=647)</td>
<td>Senior Leadership - 93%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(n=72)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Effectiveness Response Plan and Audit Work Plan

**Effectiveness Report**
Response Plan
All Tier 1 Recommendations complete or on schedule

**Audit Work Plan**
Recruiting IT Deputy Director
VCU’s Approach to Information Security: An Overview

VCU Board of Visitors
AICC Committee
February 28, 2020
Information Security Team

- Chief Information Security Officer
  - Deputy Director, Information Security
    - Security Operations Team Lead
      - Information Security Analyst
      - Risk Management Analyst
      - Student Workers (3)
    - System Security Architect
    - Security Engineering Team Lead
      - Senior Identity and Access Management Analyst
      - Identity and Access Management Analyst
      - Endpoint Security Analyst
What Makes Higher Education a Prime Target?

• Wide variety of valuable data
  • Student and employee data
  • Research data
• Openness
• Decentralization
• Organizational vulnerabilities
• Widespread use of personal devices
• Publicly available directories and large population
Higher Ed IT Environment

• Technology Environment
  • Distributed computing and wide range of hardware and software from outdated to state-of-the-art
  • Increased demands for distributed computing, global collaboration, and mobile/wireless capabilities which create unique security challenges

• Organizational Environment
  • Decentralized
  • Often reactive rather than proactive

• Academic Culture
  • Belief that security & academic freedom are antithetical
  • Experimentation and anonymity highly valued
Threat Actors

• Script Kiddies:
  • Generate noise in the environment, uses easily detectable and open source tools to attempt cyber attacks; usually motivated by perceived fame or monetary reasons.

• Organized Crime:
  • Use mainly phishing based social engineering attacks and attacks against web applications, goes after targets of opportunity; motivated by monetary gains

• Hacktivists:
  • Use a variety of tactics, mostly targeting web applications and use denial of service techniques; motivated by a common cause

• Nation-state:
  • Use advanced techniques that targets individuals, very stealthy and targets an extremely limited number of individuals; motivated by intellectual property or the possible gain of human assets
Examples of Vulnerabilities

- Networks – wired and wireless
- Operating systems – especially Windows
- Unpatched servers and systems
- Malicious code and viruses
- Improperly shared data in cloud applications or websites
- People not taking proper care with systems, devices, or data
Risk-Based Approach to Information Security

VCU Information Security Standard:
• Three-tiered information classification system
• Classification of information drives the protection of IT systems and processes
• Protections include:
  • Administrative
  • Physical
  • Technical

- Category I: High Sensitivity regulated and controlled information
- Category II: Moderate Sensitivity non-public information
- Category III: Low sensitivity public information
VCU Security Management Architecture Overview

- Security Frameworks / Models
- Industry / Legal Regulations

- Risk Tolerance

- Existing Processes / Capabilities

- Customized Security Framework

- Policies / Standards / Procedures / Operational Baselines

- Administrative Security Controls
- Technical Security Controls
- Physical Security Controls
Top Risk Mitigation Strategies in use at VCU

• Multifactor authentication
• Security training
• Scheduled vulnerability assessment and remediation
• Automated patching of servers
• Security reviews/audits of third parties
• IT governance/procurement safeguards
• Data governance
• Endpoint management – virus protection/patching
• Network security measures – segregation of higher risk traffic
Questions?
Closed Session
VCU Threat Intelligence Monitoring Architecture

External threat monitoring services (HIBP, Cyber Risk Analytics, Mention, PassiveTotal, Shodan)

External threat intel (RENSAC, VRT, VITA, FBI, Palo Alto, CrowdStrike, X-Force)

External Security Researchers (ZDI, ProjectZero, US-CERT)

Information Security Operations

VCU Internal Security Monitoring platform (IBM QRADAR SIEM)

VCU Internal Threat Intel

Authentication systems logs (CAS, DUO)

Firewall logs (Palo Alto, Cisco)

System Logs

Network data (flows, metadata, packet captures)

VCUHS Security

Procurement & Export Control

Antivirus & EDR logs (Micsorof Scep & Crowdstrike)

IT Staff

Network data (flows, metadata, packet captures)


VCU Community
Security Performance Metrics

FY19 (July 2018 – June 2019)

• Detected security events: 52,268
• Blocked external threats sources: 14,252
• Reported phishing scams: 165
• Confirmed compromised accounts: 6
• Total emails sent to VCU email addresses: 600.9 Million
• Total emails deemed clean and delivered: 65.2 Million
• Percentage of emails quarantined due to threat: 89.1%
• Percentage of high sensitivity security events triaged within 24 hours: 82.9%; within 72 hours: 99.7%
Questions?
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

• Treasury and Finance improvements are underway
  – ACH payee process “locked down”, current payees validated and new vendors are receiving checks, which are protected by positive pay (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)
  – Banking services RFP issued December 2019 - A primary requirement is validation and security of electronic payees as 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 (anticipated contract award May 2020)
Audit of Selected Employment Separation Processes

Ensure US Citizenship and Immigration Services Notification of H1B Nonimmigrant Employment Separations

- GEO did not report H1B employee separations in FY19
- Recommend GEO notify USCIS and collaborate with HR to use software solution
Audit of Desktop Service Delivery

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
Facilities Management IT Systems

Diagram of Common Building Automation Systems

- Internet Service Provider
- Server
- Router
- Remote Access
- Central Workstation
- HVAC
- Fire Alarm
- Lighting
- Energy Management
Facilities Management IT Systems

Audit Focus

• Support Servers
• Internet of Things (smart) devices
• Emergency Ops Center and MCV Steam Plant
Finding: Central Works Pro fire alarm server does not meet VCU’s information security baseline

- No patching
- Server support ends Jan 2020
- No password changes since 2013
- Outdated operational procedures
- No application updates installed

- Fire alarm system gap analysis underway (March, 2020)
- Move alarm monitoring & response coordination to VCU Police (in progress)
- Server hosted at UCC with continuous OS security monitoring & application support from software vendor (December, 2020)
Facilities Management IT Systems

Finding: Key internet of things (smart) devices (HVAC and Fire Alarms) had critical security concerns

- Remotely accessed 22 of 35 devices tested
- Use of default or weak passwords
- Use of well known default accounts
- Outdated firmware

- Exploring interim security processes with Technology Services
- All devices added to IT Network Security database (November 2020)
- Replacing end of life IoT devices; user accounts limited to key personnel & all admin accounts disabled (December 2020)
- Old servers decommissioned; server apps use VCU credentials. All servers require two factor authentication (March 2021)
Facilities Management IT Systems

Finding: Steam Plant needs physical security improvement plan

• Vulnerable to vehicles & pedestrians
• Lacks barriers to protect natural gas lines and fuel reservoirs
• No cameras, motion detection lighting, locked gate, fuel reservoir locks, inadequate fencing
• Pedestrian doors propped open
• No IT control room door lock, system placed in unlocked cabinet, control room has flooded in the past
Facilities Management IT Systems

Finding: Steam Plant needs physical security improvement plan

- Door card readers installed; Gates locked 7pm to 7am weekdays and all-day weekends; Exterior doors secured & Delta-V upgrade complete
- Secure server cabinet installed, equipment on upper shelves or second floor to reduce water damage (July, 2020)
- Expert evaluates physical security; VCU implements improvements (October, 2020)
- Vehicular access restrictions occur after Emergency Ops relocates adjacent to the Steam Plant (December, 2021)
Executive Session
University Counsel Update