

Virginia State University

Cyber Security Review Consultation

Internal Audit Report

January 11, 2024

CONTENTS

Executive Summary..... 3

 Background 3

 Scope and Objectives 4

 Conclusion..... 4

Observations, Recommendations, and Responses 6 - 11

Appendix A - Risk Definition and Classifications 12

EXECUTIVE SUMMARY

BACKGROUND

Our review of the cybersecurity posture of Virginia State University (the University) focused on the five Core Functions of the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), which we define in detail below. The NIST CSF represents the gold standard for cybersecurity in the United States and the foundation for many new standards and regulations starting to emerge today. The Commonwealth's Security Standard (SEC-530) is based on NIST.

The Functions are the highest level of abstraction included in the Framework. They act as the backbone of the Framework Core that all other elements are organized around. These five Functions were selected because they represent the five primary pillars for a successful and holistic cybersecurity program. They aid organizations in easily expressing their management of cybersecurity risk at a high level and enabling risk management decisions.

The Core Functions are:

Identify:

The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect:

The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect:

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

Respond:

The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

EXECUTIVE SUMMARY

Recover:

The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

SCOPE AND OBJECTIVES

The Office of Internal Audit has completed its Cybersecurity Review consultation. This consulting engagement was included in the 2024 Audit Plan. This report provides an analysis of the current cybersecurity posture of Virginia State University and offers recommendations for improving security measures to mitigate potential vulnerabilities and threats. The review scope included an evaluation of the University's security infrastructure, policies, and procedures. The objectives were to test the adequacy and effectiveness of policies and procedures, controls and configurations, and compliance with applicable state and federal laws, regulations, standards, and industry best practices. The steps performed were intended to provide reasonable assurance that controls are working to protect the confidentiality, integrity, and availability of data that support the mission of Virginia State University.

We reviewed for compliance with the University Information Technology (IT) security policies and procedures, and the NIST CSF five core functions: Identify, Protect, Detect, Recover, and Respond. For reference we have also provided the Commonwealth's requirements in our observations and recommendations as they coincide with NIST and are the basis of the University's policies.

CONCLUSION

Overall, the University's cybersecurity posture is adequate, however, opportunities exist to strengthen and enhance our posture. This report outlines six recommendations, some of which the University mitigated or partially mitigated by the time of report publication, but are required to be disclosed

EXECUTIVE SUMMARY

as they existed as of the date of field work. Included in the table below is a summary of the observations ranked by internal audit’s risk definition and classification. See Appendix A for risk rating classifications and definitions.

| | | | | |
|-------------------------|---------------------|-----------------------|--------------------|----------------------|
| Priority (1) | High (2) | Medium (1) | Low (2) | Total (6) |
|-------------------------|---------------------|-----------------------|--------------------|----------------------|


As this was a consulting engagement, and not an audit, we present the observations and recommendations solely for management’s consideration. However, management has plans to address the issues identified in the report and in some cases has already implemented corrective actions. These responses, along with the detailed observations and recommendations, are in the Observations, Recommendations, and Responses section of this report. We present them in order of risk classification.

In conclusion, we have identified areas for improvement within Virginia State University’s cybersecurity posture. By implementing the recommendations outlined in this report, the University can enhance its overall security resilience and reduce the risk of cyber threats. We should note that some of the areas where we observed deficiencies during this review were also found in 2022 and 2023, during the audits completed by the Virginia Information Technology Agency (VITA) and the Auditor of Public Accounts (APA). Those areas include Disaster Recovery Testing, Access Reviews and Controls, and Role-Based Security Awareness Training.


OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

| Observation | Recommendation | Management Response |
|--|---|--|
| <p>Risk Rating: Priority ●</p> <p><i>Requirement - Access permissions are managed, incorporating the principles of least privilege and separation of duties. (Function: Detect)</i></p> <p>1. Conduct regular periodic access reviews of systems</p> <p>The University does not currently conduct regular periodic access reviews of its systems. The Commonwealth’s Security Standard section AC-2 Account Management and the University’s Logical Access Control and Account Management Policy require that the system administrator will review existing accounts periodically for validity (at least annually) and obtain department approval/sign-off. Failure to not perform access reviews can lead to unauthorized access and the risk of a data breach.</p> | <p>We recommend that the University perform access reviews on an annual basis. By performing access reviews, the University can ensure that all granted user access rights giving access to the University’s information system are appropriate and legitimate. In so doing, the University will decrease cybersecurity risk and lessen the potential for data breaches or unauthorized access.</p> | <p>Technology Services is implementing a solution called “Okta”. Okta will allow for the automation of regular periodic access reviews across all systems. Technology services held an entrance meeting with Okta on 1/10/2024 to discuss next steps with respect to implementation, which should take approximately 90 days once procurement of the solution is complete.</p> <p>Okta is an enterprise-grade, identity management service, built for the cloud, but compatible with many on-premises applications. With Okta, IT can manage any employee's access to any application or device. Okta runs in the cloud, on a secure, reliable, extensively audited platform, which integrates deeply with on-premises applications, directories, and identity management systems.</p> <p>Okta’s Identity Governance is a SaaS-delivered, converged, and intuitive Identity and Access management platform. It is used to simplify and manage identity and access lifecycles across multiple systems and improve the overall security. With OIG, Access Certification campaigns can support one or two levels of reviews. This functionality supports not only an additional review layer but also enhances the notifications supported.</p> |


OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

| Observation | Recommendation | Management Response |
|--|---|--|
| <p>Risk Rating: High </p> <p><i>Requirement - Audit/Log records are determined, documented, implemented, and reviewed in accordance with policy. (Function: Protect)</i></p> <p>2. Review System Audit Logs Timely</p> <p>The University does not currently review audit logs in a timely manner. The University’s IT Audit and Accountability Policy requires that that the University reviews and analyzes information system audit records at least once a week for indications of inappropriate or unusual activity. The Commonwealth’s Security Standard SEC 530 section AU-6 Audit Record Review, Analysis, and Reporting, requires that audit logs be reviewed at least once every 30 days. Failing to review audit logs can result in attacker activities going unnoticed and evidence of whether the attack led to a breach can be inconclusive.</p> | <p>We recommend:</p> <ol style="list-style-type: none"> 1. The University system owners review audit logs as required by policy and standard. By doing so, it will allow for tracking of user activity, and investigation of anomalous activities. 2. The University should consider revising their IT Audit and Accountability Policy from weekly audit log review to monthly review to match the Commonwealth’s less restrictive requirement. | <p>See response to Observation #1 above. Technology Services is planning to implement Okta. This solution will allow Technology Services the capability to automate exporting the logs to system owners for monthly reviews as required by the standard.</p> <p>The Okta System Log records events of interest in the organization that may be of interest for purposes such as audit, troubleshooting, and security analysis. These events are made available in the organization through several interfaces, including the Okta Admin Console, the System Log API, Log Streaming, and third-party integrations from cloud services providers such as Splunk and LogRhythm. System Log events are retained in Okta for a period of 90 days.</p> |


OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

| Observation | Recommendation | Management Response |
|--|---|--|
| <p>Risk Rating: High </p> <p><i>Requirement - Detection activities comply with all applicable requirements. (Function: Detect)</i></p> <p>3. Conduct Incident Response Testing and Document Results of Tests</p> <p>The University has not conducted an incident response test and has not document the test results. The Commonwealth Security Standard section IR-3 Incident Response Testing and Exercises and the University’s Threat Management policy require that at least once per year the Cybersecurity Incident Response Team will hold a formal tabletop exercise to incorporate simulated events to facilitate response by personnel in crisis situations. Failure of not performing incident response tests can result in not effectively being able to respond to various incidents which could potentially lead to data breaches.</p> | <p>We recommend that the University conduct annual incident response tests and document the results of the tests. Performing incident response tests can assist the University in potentially reducing losses, restoring business processes and services, and quickly mitigating exploited vulnerabilities.</p> | <p>Technology Services will hold a tabletop exercise for Incidence Response testing during our next departmental meeting. The Deputy Chief Information Officer is meeting with the IT Business Manager during the week of January 15 to finalize the date/location with Thompson hospitality. This table top exercise will incorporate a scenario-based presentation, the Incident Response Plan, lessons learned, and training verification roster.</p> |

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

| Observation | Recommendation | Management Response |
|--|---|--|
| <p>Risk Rating: Medium </p> <p><i>Requirement - Senior executives understand roles and responsibilities. (a) Specific role-based training is assigned based on cybersecurity roles and responsibilities. (Function: Protect)</i></p> <p>4. Administer Cybersecurity Awareness Role-Based Training</p> <p>The University does not administer role-based training based on cybersecurity roles and responsibilities. The Commonwealth’s Security Awareness Training Standard SEC 527 section 4.1 Cybersecurity Curriculum Outline and the University’s Security Awareness and Training Policy require that system owners, system administrators and data owners complete annual role-based training (or more frequently based upon enterprise needs) and maintain records of training. Failure to provide role-based training can potentially result in data breaches, malware infections, phishing attempts, and malicious activities.</p> <p>NOTE: The VSU CISO has stated that the University did conduct role-based training during 2023, and has provided a power point presentation of that training. However, both the University’s policy and the Commonwealth’s standard require that training records be maintained. As of the date of this report, no records have been provided.</p> | <p>We recommend that the University administer role-based training for users that have cybersecurity roles and responsibilities. By providing role-based training the University can further secure and protect their data from breaches and other malicious attacks.</p> | <p>Senior Executive leadership role-based security awareness training has been created, and was sent to users on 1/11/2024 at 8:00 AM.</p> <p>The cybersecurity role-based training for system owners, data owners, data custodians, and system administrators will be performed by the Department of Human Resource Management’s Commonwealth of Virginia Learning Center (COVLC) for the newly approved system security roles.</p> <p>This training will be conducted before the end of January 2024, and will include acknowledgement forms and an annual acknowledgement of the User Access Agreement and Policy.</p> <p>Technology Services will send a list of those individuals with security roles and responsibilities that are required to take the training to Human Resources to update their Employee Work Profile’s to reflect their responsibilities for these roles.</p> |

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

| Observation | Recommendation | Management Response |
|---|---|--|
| <p>Risk Rating: Low </p> <p><i>Requirement - A baseline of network operations and expected data flows for users and systems is established and managed. (Function: Detect)</i></p> <p>5. Develop and Maintain a Data Flow Diagram to Include the Direction(s) the Data Flow Between Systems</p> <p>The University does not currently have a data flow diagram in place. The Commonwealth’s Security Standard section CA-3 Information exchange and the University’s Systems Security Plan and Systems Operability Agreement Policy requires that for University-owned sensitive IT systems, the University shall require that the system owners or the University service provider specify and document all IT systems with which data is shared. This documentation, in form of written agreement, shall include the direction(s) of data flow. Failure to have a documented data flow diagram can result in the inability to understand processes or system operations to discover potential problems, improve efficiency, and develop better processes.</p> <p>NOTE: We would like to note that Technology Services did provide a network diagram that does include some data flows. However, that diagram did not clearly include the documented flow of information between the systems.</p> | <p>We recommend that the University develop a data flow diagram for its systems. By having a documented data flow diagram, it will help the University to understand the functions and limits of a system, help visualize contents, and provide a detailed and well-defined diagram of system components. This will provide a straightforward, efficient way for the University to understand, perfect, and implement new process or systems.</p> | <p>Technology Services has provided the overall data flow diagram. We will be breaking them out into single system diagrams to ensure the data flow can be managed/viewed more efficiently. This will be completed prior to the end of February.</p> |

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

| Observation | Recommendation | Response |
|--|--|---|
| <p>Risk Rating: Low ●</p> <p><i>Requirement - Response Plans incorporate lessons learned, Response Strategies are updated (Function: Respond)</i></p> <p><i>Requirement - Recovery Plans incorporate lessons learned, Recovery Strategies are updated. (Function: Recover)</i></p> <p>6. Perform and Document Annual Disaster Recovery Plan Testing</p> <p>As of the date of this report, this deficiency was corrected. Auditing standards require that we report the condition as of the date of the fieldwork. See further information below.</p> <p>The University has not performed and documented annual disaster recovery plan testing. The Commonwealth’s Security Standard section CP-4 Contingency Plan Testing and the University’s Contingency Planning Policy and Business Impact Analysis Policy requires that University Executives and Senior Management periodically review, reassess, test, and revise the University’s Continuity of Operations Plan (COOP) and IT Disaster Recovery Plan to reflect changes in essential business functions, services, IT system hardware and software and personnel. Failure to complete a disaster recovery plan test can result in extended downtime, inefficient recovery efforts and failure to meet regulatory and compliance requirements.</p> <p>NOTE: After the date of fieldwork, this finding was corrected. The University has now conducted and documented the annual disaster recovery plan testing and provided evidence of such, as well as documented lessons learned.</p> | <p>We recommend that the University establish a cadence in which they perform disaster recovery plan testing to help ensure that the University can recover data, restore business critical applications, and continue operations after an interruption in service. We also recommend that the University document result of the tests and lessons learned, so the recovery and response strategies are updated as required.</p> | <p>Not Applicable – no further action by management is necessary. Technology Services has corrected the deficiency.</p> |

APPENDIX A - RISK DEFINITION AND CLASSIFICATIONS

The chart below represents a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our audit. The chart provides information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

| Risk Definition: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. | Degree of Risk and Priority of Action | |
|---|---------------------------------------|--|
| | Priority | An issue identified by Internal Audit that, if not addressed immediately, has a high probability to directly impact achievement of a strategic or important operational objective of a VSU business unit or the University as a whole. |
| | High | An issue identified by Internal Audit that we consider to have a high probability of adverse effects to the University or to a significant college/school/business unit. As such, we recommend that management act to address the noted concern and reduce risk to the organization. |
| | Medium | An issue identified by Internal Audit that we consider to have a medium probability of adverse effects to the University or to a college/school/business unit. As such, we recommend that management consider action to address the noted concern and reduce the risk to a more desirable level. |
| | Low | An issue identified by Internal Audit that we consider to have minimal probability of adverse effects to the University or to a college/school/business unit. As such, we recommend management consider whether to act to reduce the risk, or accept the risk as being within the University's risk appetite. Cost-benefit analysis may be useful. |

We use considerable professional judgment in determining the overall ratings presented on the previous pages of this report. Accordingly, others could evaluate the results differently and draw different conclusions. This report provides management with information about the condition of risks and internal controls at one point in time; future changes in environmental factors and actions by personnel may significantly impact these risks and controls in ways that this report did not and cannot anticipate.