SysAudits | Systems Security Audit Professionals

OFFICE OF THE STATE INSPECTOR GENERAL
COMMONWEALTH OF VIRGINIA

FINAL AUDIT REPORT

Summary of the Cybersecurity Audit for Virginia Higher Education Institutions

Report No. 2025-PA-001

October 30, 2024

Prepared By:

SysAudits | Systems Security Audit Professionals

COMMONWEALTH OF VIRGINIA

Office of the State Inspector General

Michael C. Westfall, CPA State Inspector General	P.O. Box 1151 Richmond, Virginia 23218	Telephone (804) 625-3255 www.osig.virginia.gov

October 30, 2024

The Honorable Glenn Youngkin
Governor of Virginia
P.O. Box 1475
Richmond, VA 23219

Dear Governor Youngkin,

The Office of the State Inspector General (OSIG) completed cybersecurity audits of the Commonwealth's Higher Education Institutions. Each Higher Education Institution was issued a final audit report, with findings and recommendations. A summary report of the audit is attached.

OSIG would like to thank the presidents of the Higher Education Institutions and their staff for their cooperation and assistance during this audit.

Sincerely,

Michael C. Westfall, CPA
State Inspector General

cc: The Honorable John Littel, Chief of Staff to Governor Youngkin
Tiffany Robinson, Deputy Chief of Staff to Governor Youngkin
The Honorable Aimee Rogstad Guidera, Secretary of Education
Emily Anne Gullickson, Deputy Secretary of Education
Nicholas Kent, Deputy Secretary of Education
Tammy Babbs, Executive Assistant for the Secretary of Education
Senator Ghazala F. Hashmi, Chair of Education and Health Committee
Delegate Sam Rasoul, Chair of the Education Committee
Staci Henshaw, Auditor of Public Accounts
HEI Presidents

Executive Summary

SysAudits.com, LLC performed cybersecurity audits on behalf of the Office of the State Inspector General (OSIG) for the Commonwealth of Virginia (COV) from December 2023 through October 2024. The audits were conducted in accordance with the Government Accountability Office's *Generally Accepted Government Auditing Standards (Yellow Book)*. The audit methodology was guided by policies and procedures issued by the Commonwealth of Virginia (COV) Higher education Institutions (HEI) and the National Institute of Standards and Technology (NIST) 800-53, Security and Privacy Controls for Information Systems and Organization, Revision 5 as a basis for industry best practices.

Eighteen separate audit reports were issued representing each of the COV's HEI schools. This report includes a summary of the findings on cybersecurity processes and controls from the 18 audit reports issued. All the HEIs provided responses to the audit findings and recommendations and submitted a corrective action plan to implement the recommendations.

The audit included 18 of the Commonwealth of Virginia's public colleges and universities. The audit assessed four cybersecurity audit objectives which were:

1. Determine if HEIs can identify and respond to cyberattacks in a manner consistent with industry standards through penetration testing;
2. Determine if HEI's current cybersecurity monitoring and testing, to include internal penetration testing, is adequate to reasonably protect against cybersecurity threats;
3. Determine whether HEIs have established performance metrics in responding to or preventing cyberattacks that are consistent with industry standards; and
4. Determine whether security assessments in the form of management reviews or security audits are performed as required by state or institution policy.

The audit scope included holding discussions with HEI internal audit and IT operations and security staff in addition to the following:

- Public facing web presence (IPs) to perform penetration testing of the HEI's public facing web presence;
- System monitoring processes that include the HEI's establishment and monitoring of secure configuration baselines, vulnerability management (vulnerability and compliance scanning), audit and logging of systems (servers, databases, web applications, routers, and firewalls);
- Cyber incident handling and management metrics to respond to cyberattacks;

and,

- Audit risk management process for planning cyber audits, and IT operations risk assessment process to identify and adjust to cyber and IT risks.

Overall, we found that the HEIs implemented processes to support cybersecurity. Our audit resulted in 34 findings[1] and 203 audit recommendations designed to improve the HEI's cybersecurity processes and controls. HEIs agreed with 31of the 34 findings.[2] The HEIs agreed with 196 of the 203 audit recommendations. For the seven recommendations that the HEI did not agree with, the HEI submitted a corrective action plan that addressed the findings and recommendations. A majority of the HEIs implemented corrective action during the audit to address the issues identified in the findings which resulted in the closing of 73 audit recommendations (35.96%) prior to the issuance of the final audit reports to the individual HEI. For the rest of the recommendations, HEIs submitted corrective action plans that will address all findings and recommendations by October 15, 2027, with all but two of the recommendations addressed prior to December 31, 2025.

David Cole, CPA, CISA, CRISC
SysAudits.com LLC

[1] The audit findings were categorized into two areas, one for penetration testing and one for cybersecurity monitoring. Two HEI's did not have penetration testing findings.

[2] One HEI did not agree with the audit use of NIST as the cybersecurity control industry standard and instead noted that the HEI follows an ISO standard. Both NIST and ISO align to GLBA; therefore, no significant discrepancies were noted. One HEI did not agree with the findings (two) or recommendations (seven) but submitted a corrective action plan to address all seven recommendations.

Table of Contents

Background

OSIG engaged SysAudits.com LLC (SysAudits) to assess and determine the effectiveness of HEI cybersecurity controls, policies, and procedures to monitor, identify, and secure IT systems. This report summarizes the findings from our audit evaluations and testing of security controls.

The audit entrance conference was conducted on December 12, 2023, and December 13, 2023, and included all the COV's HEIs. To facilitate timely completion of the audit and promote transparency of the audit scope, SysAudits provided a Non-Disclosure Agreement (NDA) and Rules of Engagement (ROE) to each of the HEIs on January 3, 2024.

COV HEI Schools

The following represents the 18 COV schools that were included in the audit:

1	Christopher Newport University	**10**	University of Mary Washington
2	College of William and Mary in Virginia	**11**	University of Virginia Academic *
3	George Mason University	**12**	University of Virginia Medical Center
4	James Madison University	**13**	Virginia Commonwealth University
5	Longwood University	**14**	Virginia Community College System**
6	Norfolk State University	**15**	Virginia Institute of Marine Science
7	Old Dominion University	**16**	Virginia Tech
8	Radford University	**17**	Virginia State University
9	Richard Bland College	**18**	Virginia Military Institute

* University of Virginia at Wise was included as part of University of Virginia Academic audit.

** Virginia Community College System is composed of 23 separate colleges of which only the central IT services were audited and not the 23 separate colleges. The 23 separate colleges operate, for the most part, autonomous from central IT services.

Summary of Cyber Audit Objective 1 – Penetration Testing

Determine if HEIs can identify and respond to cyberattacks in a manner consistent with industry standards through penetration testing.

Audit Methodology:

To assess the HEI's ability to identify and respond to cyberattacks, the audit included performing network penetration testing of the HEI's Internet public facing websites. Each HEI can have a significant number of available public-fronting IPs for which the schools can establish a public facing website. We performed network penetration testing on up to 10 public facing websites for each HEI audited for an estimate of about 160-180 public facing websites.

Pentest Methodology:

The following methodology was performed for external Internet based penetration testing:

1. Host Discovery
   a. External testing – internet based
   b. Review results and identify potential risks
2. Vulnerability Discovery
   a. External testing – internet based
   b. Review results and identify potential risks
   c. Design/perform targeted potential exploitation tests
3. Analysis and Exploitation
   a. Review results and identify potential risks
   b. Design/perform potential exploitation tests
4. Document Analyses and Results
5. Draft Penetration Testing Findings

Vulnerability Rating:

Identified risks and vulnerabilities were categorized into four severity levels: low, medium, high, and critical. When assigning a criticality level, multiple dimensions (e.g., impact, likelihood, and effort to remediate) were considered to determine the overall risk a specific vulnerability presents in the context of the target website, system, or application. The following table summarizes these ratings; however, each vulnerability is assessed and rated individually based on the target environment.

Severity	Vulnerability Description
Critical	Can be exploited as an unauthenticated or unprivileged user and grants an attacker root-level access to servers, infrastructure, or sensitive data.
High	Exploitation requires specific circumstances or results in increased, but not unrestricted, access to servers, infrastructure, or data.
Medium	Successful exploitation provides limited access or is dependent on the existence of other vulnerabilities or weaknesses.
Low	Vulnerabilities that cannot be exploited directly but provide an attacker with additional knowledge or data that may lead to discovery of other vulnerabilities.

Penetration Testing Results:
From our Internet network penetration testing, we identified the following. A total of 131 audit recommendations were made as a result of the audit penetration testing. During the audit, penetration testing findings and recommendations were provided to the HEIs. The penetration testing recommendations and actions taken included updating the hosts for missing patches and/or disabling unnecessary services. Some HEIs addressed and mitigated identified risks prior to finalizing the overall audit. The following represents the penetration testing audit recommendations based on severity:

Penetration Testing Recommendations	Low	Med	High	Critical	Total
	89	23	19	0	131

In performing the penetration testing, the HEIs were not notified specifically when penetration testing was to commence. Some schools requested to be notified of the specific test dates for penetration testing so that they could monitor the testing. However, for the penetration testing the HEIs were instructed to monitor their respective networks as usual and if they identified unusual activities, they should respond according to their monitoring processes such as blocking the IP of suspicious probes or attacks. The HEIs were also instructed that if they did identify suspicious activities, they could contact SysAudits for confirmation if the suspicious activities identified were those from SysAudits penetration testing. During the penetration testing, only two HEIs identified and reported to SysAudits that they observed, based on their network monitoring, suspicious activities from the audit's penetration testing activities.

In addition, although the audit penetration testing did not identify vulnerabilities that resulted in an access compromise to a specific website or webserver, the audit did identify risks which resulted in recommendations to enhance the public facing websites and webservers. While the majority of penetration testing findings were deemed “Low” risk, it should be noted that industry best practices are to review all penetration testing risks because penetration risks are from a point in time, and low risks can escalate to a higher rating if exploitations are developed or created to exploit a risk. A single risk can be elevated when multiple risks are combined resulting in a high-risk vulnerability, known as threat vulnerability pairing.

The U.S. Department of Homeland Security (DHS) provides guidance on remediation of vulnerabilities for Internet-accessible systems. Internet-accessible information systems include any system that is globally accessible over the public internet. DHS advises that adversaries operating in cyberspace can make quick work of unpatched Internet-accessible systems. The time between an adversary’s discovery of a vulnerability and their exploitation of it (i.e., the ‘time to exploit’) is rapidly decreasing. Industry reports estimate that adversaries are now able to exploit a vulnerability within 15 days (on average) of discovery. After gaining entry into information systems and networks, these adversaries can cause significant harm. As organizations continue to expand their Internet presence through increased use and operation of interconnected and complex Internet accessible systems, it is more critical than ever to rapidly remediate vulnerabilities inherent to these systems. Failure to do so could allow malicious actors to compromise networks through exploitable, externally-facing systems. DHS also recommends that ransomware threats can be mitigated to some extent by ensuring systems are patched and updated, and that an incident response management program and periodic security assessments be performed.

Summary of Cyber Audit Objective 2 – Cybersecurity Monitoring

Determine if HEIs current cybersecurity monitoring and testing is adequate to reasonably protect against cybersecurity threats.

Audit Methodology:

To assess the HEI's system monitoring processes, the audit included assessing whether the HEIs established secure baselines and secure configuration processes to monitor and ensure systems/hosts are securely configured for: server operating systems, databases, web services such as Apache and IIS, network routers, and firewalls. The audit included assessing whether HEIs had processes to perform vulnerability management (vulnerability and compliance scanning[3]), audit and logging of systems (servers, databases, web applications, routers, and firewalls).

HEI Cybersecurity Monitoring Results:

The following are the audit testing recommendations.

Secure Baselines*	Vulnerability and Compliance Scanning	Security Logging into a Security Incident Event Management System (SIEM)
21	22	13

* Secure baseline settings at a minimum for: server operating systems, databases, IIS, Apache, core routers, and firewalls.

The audit identified instances where the HEIs had not:

- Adopted secure baselines for server operating systems, databases, IIS, Apache, router, and firewalls.
- Established monitoring and scanning that secure baseline settings are maintained for server operating systems, databases, IIS, Apache, router, and firewalls.
- Established security audit and logging into a central monitoring system such as SIEM, for server operating systems, databases, IIS, Apache, router, and firewalls.

Prior to the audit, some of the HEIs had adopted secure baselines, some HEIs had vulnerability and compliance scanning processes in place, and most HEIs had a SIEM but

[3] We sought to determine if HEIs were performing both vulnerability and compliance scanning. Vulnerability scanning involves performing automated scans to identify missing patches, updates, and unnecessary ports and services. Compliance scanning is an automated means to perform scans using an industry secure baseline of secure settings to identify security misconfiguration settings based on the industry security baseline. Both types of scanning support ensuring systems (server operating systems, databases, webservices, routers, and firewalls) are securely configured.

may not have been collecting logs from all system server operating systems, databases, IIS, Apache, router, and firewalls. As a result of the audit, the HEIs have begun researching and identifying solutions to enhance their system secure configurations, monitoring secure configurations, and enhancing their SIEM processes.

The audit used NIST 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations as the basis for industry standard cybersecurity controls. NIST 800-53 has been adopted by many government and commercial entities and is often considered an industry's best practice even when not required by statute. The Commonwealth of Virginia also used NIST 800-53 as its basis for developing the Commonwealth's Information Security Standard (SEC 530). We used NIST 800-53 Controls for our analysis included:

- CM – 6: Configuration Setting. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements.
    - Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization defined hardening standards. Common secure configurations (also known as security configuration checklists, lockdown and hardening guides, and security reference guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology products and platforms as well as instructions for configuring those products or platforms to meet operational requirements.
    - Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
- RA-5: Vulnerability Monitoring and Scanning. Share information obtained from the vulnerability monitoring process and control assessments with the appropriate organization-defined personnel to help eliminate similar vulnerabilities in other systems. Monitor and scan for vulnerabilities in the system and hosted applications. Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly.
- AU- 6: Audit Record Review, Analysis, and Reporting. Integrate analysis of audit records with analysis of vulnerability scanning information; performance data; and system monitoring information to further enhance the ability to identify inappropriate or unusual activity. Integrate analysis of audit records with analysis of

> vulnerability scanning information; performance data; and system monitoring information to further enhance the ability to identify inappropriate or unusual activity. Integrated analysis requires that the analysis of information generated by scanning, monitoring, or other data collection activities is integrated with the analysis of audit record information. Security Information and Event Management tools can facilitate audit record aggregation or consolidation from multiple system components as well as audit record correlation and analysis.

In addition, the DHS recommends that organizations establish a vulnerability management program that includes:

- Establishing secure configuration management that includes adopting secure baselines, establishing these secure baselines across all systems, and the monitoring of secure baseline implementation because secure settings can change over time; and
- Identifying security risk vulnerabilities by performing vulnerability and compliance scanning of server operating systems, databases, web services such as IIS and Apache, and router and firewalls to identify systems that may be vulnerable or secure settings that have changed.

Summary of Cyber Audit Objective 3 – Cyber Performance Metrics

Audit Methodology:
To assess whether the HEIs had established cyber incident handling and management metrics to respond to cyberattacks.

HEI Cybersecurity Monitoring Results:
The audit included reviewing HEI incident handling policies and holding meetings with HEI information security staff to determine if HEIs had established cyber incident handling metrics into their policies. Establishing HEI metrics sets the requirement to investigate and respond to suspicious network security events. Also, the audit evaluated whether HEIs were performing incident handling response tabletop exercises.

From our audit testing, we identified seven audit recommendations that ranged from formalizing into policies specific incident handling response metrics, to scheduling and performing incident handling tabletop exercises.

The audit used NIST 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations as the basis for industry standard cybersecurity controls. NIST controls were:

- IR 8: Incident Response Plan. It is important that organizations develop and implement a coordinated approach to incident response. Organizational mission and business functions determine the structure of incident response capabilities. Develop an incident response plan that provides metrics for measuring the incident response capability within the organization.
- IR-3: Incident Response Testing. Organizations test incident response capabilities to determine their effectiveness and identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, and simulations. Incident response testing can include a determination of the effects on organizational operations and assets and individuals due to incident response. To help incident response activities function as intended, organizations may use metrics and evaluation criteria to assess incident response programs as part of an effort to continually improve response performance. These efforts facilitate improvement in incident response efficacy and lessen the impact of incidents.

DHS recommends that organizations establish a cyber incident Handling Plan and that organizations perform exercises of the incident handling plan that include a communications plan with notification procedures for a ransomware incident.

Summary of Cyber Audit Objective 4 – Cybersecurity Risk Assessments

Audit Methodology:

To assess whether the HEI's had established an audit risk management process for planning cyber audits, and IT operations risk assessment process to identify and adjust to cyber and IT risks.

HEI Cybersecurity Monitoring Results:

The audit included reviewing HEI processes to perform periodic cybersecurity assessments. From interview meetings with HEI internal audit departments and IT information security offices, we identified that for the most part, some level of cybersecurity assessment was being performed at the HEIs either by the internal audit departments or by information security offices.

It was noted that some of the HEIs operate in a decentralized IT environment where there is a central IT services and there are also HEI schools or divisions that can operate their own IT systems. The decentralized offices do have the responsibility to ensure compliance with HEI's computer security policies. As a result of the audit, we found that HEIs did not have a process for providing oversight of these non-centralized IT environments to ensure that the offices were compliant with the HEI's computer security policies and practices. As a result, we made nine audit recommendations to improve oversight of non-centrally managed IT environments.

We used NIST 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations as the basis for industry standard cybersecurity controls. NIST 800-53 has been adopted by many government and commercial entities and is often considered an industry's best practice even when not required by statute. NIST recommends a risk assessment include a process that:

1. Identifies threats to and vulnerabilities in the system;
2. Determines the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information;
3. Determines the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; and
4. Integrates risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments.

Cyber Audit Summary

The COV HEI cybersecurity audit identified opportunities to enhance the COV HEI cybersecurity posture. The audit identified 203 audit recommendations of which 73 were closed prior to the issuance of the final audit reports. OSIG will perform follow-up of outstanding audit recommendations for each HEI school, as corrective action is implemented.

In summary, it should be noted that cybersecurity risks and vulnerabilities are always changing and expanding. The COV HEIs should perform some level of periodic independent evaluation of cybersecurity processes and practices. In particular, the following security controls should be a part of regular independent audits every 12-18 months to ensure that HEI controls are continuing to improve:

1. Adoption and monitoring of secure baselines;
2. Audit of vulnerability risk management practices to ensure identified risks are mitigated within specified timeframes;
3. Audit of best practices to mitigate the risk of ransomware;
4. Audit of best practices for vulnerability and compliance scanning;
5. Annual penetration testing of public facing websites.