OFFICE OF THE STATE INSPECTOR GENERAL

The Commonwealth of Virginia's Cybersecurity Program

Performance Audit

June 2018

Michael C. Westfall, CPA
State Inspector General

Report No. 2018-PA-003

COMMONWEALTH OF VIRGINIA
Office of the State Inspector General

Michael C. Westfall
State Inspector General

Post Office Box 1151
Richmond, Virginia 23218

Telephone (804) 625-3255
Fax (804) 786-2341
www.osig.virginia.gov

June 29, 2018

Governor Ralph Northam
P.O. Box 1475
Richmond, VA 23219

Dear Governor Northam:

The Office of the State Inspector General (OSIG) recently completed an audit of the Commonwealth of Virginia's Cybersecurity Program. The final report, which outlines five findings and recommendations for improvement, is attached for your review and information.

OSIG would like to thank Virginia Information Technologies Agency Chief Information Officer of the Commonwealth Nelson Moe and Department of Planning and Budget Director Daniel Timberlake and their staffs for their cooperation and assistance during this audit.

Sincerely,

Michael C. Westfall, CPA
State Inspector General

cc: Clark Mercer, Chief of Staff to Governor Northam
Suzette P. Denslow, Deputy Chief of Staff to Governor Northam
Dr. Keyanna Conner, Secretary of Administration
Aubrey Layne, Secretary of Finance
The Honorable Thomas K. Norment, Jr., Co-Chairman, Finance Committee
The Honorable Emmet W. Hanger, Jr., Co-Chairman, Finance Committee
The Honorable S. Chris Jones, Chairman, Appropriations Committee
The Honorable Frank M. Ruff, Chairman, General Laws and Technology Committee
The Honorable Roxann L. Robinson, Chair, Science and Technology Committee
Nelson Moe, Chief Information Officer of the Commonwealth, Virginia Information Technologies Agency
Daniel Timberlake, Director of the Department of Planning and Budget

Cybersecurity

What OSIG Found

Security Risk Management Not Cost-Effective

While VITA has adopted the National Institute of Standards and Technology's (NIST) security controls outlined in Special Publication 800-53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations, they have not adopted NIST Special Publication 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems. NIST 800-37 would allow agencies to assess system controls in a more cost-effective manner while still ensuring the independence and quality of the review.

Security Audits of Systems Not Accomplished

Executive branch agencies are not consistently complying with Information Technology Resource Management (ITRM) Standard SEC502-02.3. Of the 18 agencies evaluated for compliance, 11 had not performed all of their required sensitive system security audits over the past three years. Reasons included lack of available funding or positions within the agency, conscience decisions to address known security risks rather than conduct audits and reliance on VITA's Security Audit Service that was not fully operational.

Funding for Security Audits

Insufficient resources were often cited by agencies as a reason for not completing the security audits during the three-year audit period. Additional funds from the General Assembly were provided in the last year of the audit period to general fund agencies.

Commendable

Virginia Information Technologies Agency (VITA) has developed and documented policies and procedures to guide executive branch agencies in their cybersecurity management activities and established system audit services to conduct periodic audits of sensitive executive branch agency systems. With leadership from the Department of Planning and Budget (DPB), VITA secured needed additional funding for cybersecurity.

June 2018

HIGHLIGHTS

Why OSIG Did This Audit

- The Office of State Inspector General (OSIG) conducted this performance audit to determine if ITRM SEC501-09.1 and SEC502-02.3 were effectively reducing the risk of cyberattack on the Commonwealth. OSIG hired Cotton & Company LLP to conduct a performance audit of the Commonwealth's Cybersecurity program.

What OSIG Recommends

- Instead of conducting an audit on each sensitive system in accordance with the Institute of Internal Auditors' International Professional Practices Framework (IPPF – Red Book) or Generally Accepted Government Auditing Standards (GAGAS – Yellow Book), VITA should require such an audit be conducted on an agency information security program as a whole.

- The Commonwealth's budget should provide for continued, additional funding based on DPB and VITA recommendations. For non-general fund agencies, this may require redirection of existing resources as well as additional revenue to support the costs.

- Agencies or institutions should notify VITA when they realize security audits cannot be completed.

- VITA should continue expansion of its Centralized IT Security Audit Services to provide an efficient means of conducting IT security audits.

For more information, please contact OSIG at (804) 625-3255 or www.osig.virginia.gov

TABLE OF CONTENTS

BACKGROUND

With an increased reliance on the Internet to deliver government services, the Commonwealth faces more risk that a cyberattack against its information technology could lead to an adverse effect on providing services to its citizens. Section 2.2-2009, Code of Virginia, requires that the Commonwealth's Chief Information Officer (CIO) direct the development of policies, standards, and guidelines for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information.

In response to § 2.2-2009, the Virginia Information Technologies Agency (VITA) developed the Information Technology Resource Management (ITRM) Information Security Standard. Referenced as SEC501-09.1 issued December 8, 2016, the Standard "is to establish a baseline for information security and risk management activities for agencies across the Commonwealth." The Standard defines the minimum acceptable level of information and security risk management activities. The Standard was created using the National Institute of Standards and Technology (NIST) Special Publication 800-53 rev. *4*, Recommended Security Controls for Federal Information Systems and Organizations, as a framework.

SEC501-09.1 defines the information security roles and responsibilities and requires agencies to perform a business impact analysis to identify functions essential to its mission and the resources needed to support those functions. The Standard also requires classification of Information Technology (IT) systems and data, the creation of a sensitive system inventory, a risk assessment of sensitive systems and the performance of IT security audits to assess whether IT security controls implemented to mitigate risks are adequate and effective. The IT security audit requirement, defined in ITRM Standard SEC502-02.3 issued December 8, 2016, is only applicable to executive branch and independent agencies as well as institutions of higher learning.

Certain executive branch and independent branch agencies as well as Tier II and III universities are not covered by SEC501-09.1 or SEC502-02.3, as they have adopted alternative IT Security Standards.

The Office of the State Inspector General (OSIG) conducted this performance audit to determine if SEC501-09.1 and SEC502-02.3 were effectively reducing the risk of cyberattack on the Commonwealth. OSIG hired Cotton & Company LLP to conduct a performance audit of the Cybersecurity program.

SCOPE

The audit scope covered information security activities of executive branch agencies and institutions of higher learning for FY 2015 through FY 2017.

OBJECTIVES

Objectives for this audit were to:

- Determine whether executive branch agencies have identified all sensitive systems and accurately reported that information to VITA.
- Determine whether non-sensitive systems exclude sensitive data as defined by the Commonwealth of Virginia Information Security Standard (ITRM Standard SEC 501-09.1, December 8, 2016 or preceding versions).
- Determine whether the reporting structure of information security officers (ISOs) in executive branch agencies provides for independence and adequate separation of duties.
- Determine whether executive branch agencies have sufficient funding to complete required security audits.
- Determine if executive branch agencies comply with the Commonwealth of Virginia Information Technology Security Audit Standard (ITRM Standard SEC 502-02.3, December 8, 2016 or preceding versions).
- Determine if goals set by VITA to measure completion rates are reasonable.

METHODOLOGY

OSIG conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that OSIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. OSIG believes that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

OSIG, through Cotton and Company LLP, applied various methodologies during the audit process to gather and analyze information pertinent to the audit scope and to assist with developing and testing the audit objectives. The methodologies included the following:

- Conducting interviews;
- Conducting observations/walk-throughs;
- Examining policies and procedures to gain an understanding of the review area;
- Examining and assessing processes for efficiency and effectiveness; and
- Collecting and analyzing relevant data.

FINDINGS

SECURITY AUDITS OF SYSTEMS NOT ACCOMPLISHED

ITRM Standard SEC502-02.3 requires each agency to establish an IT Security Audit Program that includes assessing risks related to the agency's IT systems and conducting IT security audits of those systems at a minimum of once every three years. These audits must follow either the Institute of Internal Auditors' International Professional Practices Framework (IPPF – Red Book) or Generally Accepted Government Auditing Standards (GAGAS – Yellow Book) and include the preparation of audit work papers as documentation of the work performed. The audits must also assess applicable requirements of ITRM Standard SEC501-09.1, which identifies sensitive data as any data where a compromise with respect to confidentiality, integrity and/or availability could have a material adverse effect on Commonwealth's interests, the conduct of agency programs or the privacy to which individuals are entitled.

Executive branch agencies are not consistently complying with ITRM Standard SEC502-02.3. Of the 18 agencies evaluated for compliance, 11 had not performed all of their required sensitive system security audits over the past three years.

In a number of cases where agencies did perform audits of sensitive systems, the audits were not completed in accordance with IPPF - Red Book or GAGAS - Yellow Book standards as required by ITRM Standard SEC502-02.3. Of the 18 agencies evaluated for compliance, six did not complete all audits in accordance with standards. However, VITA accepted reports from three of these agencies that either had minor discrepancies with the standards, such as the wording in the reports, or where audits were completed in accordance with other standards such as the Statements on Standards for Consulting Services established by the American Institute of Certified Public Accountants (AICPA).

The lack of completed audits (and/or of audits in accordance with IPPF – Red Book or GAGAS – Yellow Book standards) resulted from a combination of factors, including:

1. Lack of funding or positions available to conduct multiple audits at each agency.
2. Conscious decisions made by agency management to use funding or resources to address known security risks instead of conducting audits that would identify such risks.
3. Reliance on VITA's Security Audit Service that was not fully operational during the entire three-year period covered by this performance audit.
4. Audits that cited IPPF – Red Book were conducted by agencies without the existence of an internal audit department.

By not completing the audits as required, management at these agencies lacked knowledge of the potential risks to sensitive systems and data.

During OSIG's discussion of this finding with agency contacts at a joint meeting on December 14, 2017, those attending also identified the following factors:

1. Some agency heads do not fully comprehend the seriousness of cybersecurity.
2. The ability to integrate VITA test results affecting agency audits is difficult due to the size of the report. The agency auditor must physically go to VITA to view the report, but is not permitted to make copies of the working papers.

Recommendations:

As reasons for not conducting required audits were in many cases legitimate, VITA should revamp ITRM SEC502-02.3 to implement a more efficient and effective process as discussed in the next finding of this report titled, "Improve Security Risk Management and Audit Process."

In addition, the following items should be considered:

1. Provide security awareness training for agency heads, emphasizing their responsibility in cybersecurity.
2. Improve communication between VITA and agencies regarding security testing on centralized operating systems, including network security systems.

Management Response(s):

VITA Response:

As noted in the conditions observed and in the auditors' recommendation, there are a number of reasons that agencies have not completed all required audits, but the main reason is typically a lack of audit resources or funding for audit resources. With the help and guidance of the Department of Planning and Budget (DPB), VITA has implemented a Central Auditing Service to address this need. The service is new, growing and still not fully staffed. Even so, the service has been successful in providing auditing resources to agencies that previously did not have any. In addition, the service has made a significant and noticeable effect in identifying and reducing commonwealth risk.

VITA will follow the recommendation to update the IT Security Auditing Standard (SEC502) and will include additional requirements and guidance for completing IT security audits.

VITA will also address the following items per the recommendations:

1) Provide security awareness training for agency heads, emphasizing their responsibility in cybersecurity.

VITA concurs and will develop and implement additional cybersecurity training.

2) Improve communication between VITA and agencies regarding security testing on centralized operating systems, including network security systems.

VITA currently requires that its current infrastructure partner submit to an independent third-party service auditor report. As VITA transitions into a new service model utilizing multiple vendors, it is also requiring independent third-party audits and will improve processes for disseminating this information to agencies.

DPB Response:
The lack of completion of all system security audits was due, in part, to the fact that funding only became available in the final year of the three-year period covered in the audit.

SECURITY RISK MANAGEMENT NOT COST-EFFECTIVE

Testing system controls through separate IPPF - Red Book or GAGAS - Yellow Book audits on each sensitive system as currently required by VITA's ITRM Standard SEC502-02.3 is not effective or efficient.

While VITA has adopted the NIST security controls outlined in Special Publication 800-53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations*, it has not adopted NIST's guidance to the Risk Management Framework for selecting (step 2), implementing (step 3), assessing (step 4) and periodically monitoring (step 6) those controls. Guidance for applying the Risk Management Framework is provided in detail in NIST Special Publication 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*. Key activities in this process are shown below.

(From NIST SP 800-53 Rev 4, Chapter 2, pg. 8)

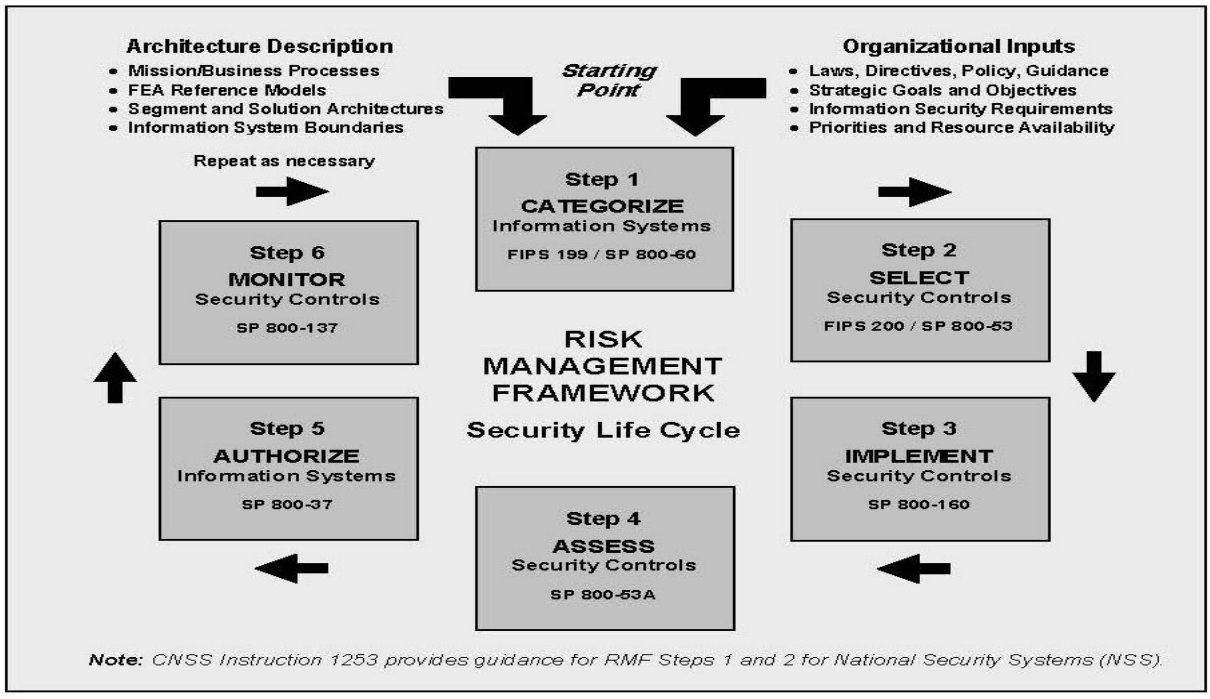

FIGURE 2: RISK MANAGEMENT FRAMEWORK

Rather than implementing the process outlined in NIST SP 800-37, VITA has developed, documented and implemented its own process for selecting, implementing and periodically testing controls. While this process does include a number of similar steps intended to manage risk to the Commonwealth's systems and information, it excludes or modifies key portions of the process that weaken VITA's overall security management program.

1. **Categorizing systems as low, moderate or high.** VITA identifies all systems as either sensitive or not sensitive. As a result, those systems identified as not sensitive have a minimum level of security controls identified, but are not periodically evaluated for effectiveness. Further, all systems identified as sensitive are treated equally, thus not allowing agency management the flexibility to prioritize allocation of their limited resources to those systems most critical to the Commonwealth.

2. **Comprehensive security assessment of in-place security controls**. While VITA's risk management process does include formal risk assessments and security audits for sensitive systems, these two processes do not have to be done in coordination, nor result in an assessment of all or most in-place security controls. Further, although risk assessments are done on non-sensitive systems, no verification of the effectiveness of the controls for those risks is in place.

3. **NIST security assessments are not required to be performed under IPPF - Red Book or GAGAS - Yellow Book audit standards.** The Commonwealth currently has more than 1,050 information systems identified as sensitive, which are therefore required to undergo an independent IPPF - Red Book or GAGAS - Yellow Book audit every three years. While NIST requires controls be assessed by management and results reported in a formal Security Assessment Report, NIST does not require these assessments be done under a formal audit standard, which generally adds cost and complexity to the assessment process.

Code of Virginia Section 2.2-2009, requires that the Commonwealth's Chief Information Officer (CIO) direct the development of policies, standards and guidelines for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. The Code does not specifically state that security audits of individual information systems must be performed. Although VITA interprets the code as requiring individual system audits based on the legal definitions of "electronic" and "information,"[1] paragraph A.1 of § 2.2-2009 regarding the frequency of security audits states, "periodic security audits of all executive branch agencies and independent agencies." Further, HB1221 as passed by both the House and the Senate in the 2018 General Assembly refers to security audit results reported by agency.

During OSIG's discussion of this finding with agency contacts at a joint meeting on December 14, 2017, concerns were raised regarding how to effectively shift resources and funding from the sensitive system security audits to individual audits of agencies with system testing performed as

[1] law.lis.virginia.gov/vacode/title64.2/chapter1/section64.2-116/

part of the risk assessment. The consensus was that additional study of how to implement this model would need to be performed.

Recommendation:

VITA should adopt NIST SP 800-37 to more thoroughly and economically assess risk and test controls. This would remove the need for a separate IPPF - Red Book or GAGAS - Yellow Book audit on each sensitive system. This would allow VITA to define the requirements of a technical security assessment of each sensitive system while also ensuring independent work and adequate documentation of test results. An audit in accordance with standards would then be conducted on an agency information security program instead of individual sensitive systems. This audit would verify that the technical security assessments were quality reviews, including independent testing and adequate documentation, thereby providing quality assurance of testing under NIST SP 800-37.

Management Response(s):

VITA Response:

VITA CSRM already encourages, and many agencies already do perform, an IT security audit of the agency's security program as a whole. We recommend that each agency conduct an audit of all common shared controls. This type of audit can be performed as a separate audit or in conjunction with an IT system security audit. The results of an audit of common controls can be relied on for subsequent system-specific control audits conducted during the three-year audit cycle. For audits of the system-specific controls for IT systems, VITA CSRM recommends that auditors focus on the CIS Critical Controls (formerly the SANS Top 20 Critical Controls).

There would also be numerous issues to address if we were to adopt NIST SP 800-37 in lieu of auditing:

- Although there may be other interpretations of the language in 2.2-2009, the phrase "performing security audits of government electronic information," has always been interpreted by VITA CSRM to mean performing audits of IT systems. To change our interpretation at this point, without any such changes to the language itself, may require guidance from the Office of Attorney General.

- In order to adopt NIST SP 800-37 and use IT risk assessments in place of IT security audits, VITA CSRM would need to assure assessor independence, as is currently in place for auditors. Both IPPF and GAGAS have independence requirements built into their existing frameworks, as well as controls, monitoring and quality assurance reviews to ensure it. NIST SP 800-37 provides recommendations for obtaining

assessor independence (typically outsourcing), but does not provide a framework to ensure that it occurs. VITA CSRM would need to create an additional oversight responsibility to monitor independence.

- Our current auditing model allows an auditor a great deal of flexibility in how they choose to scope, conduct and report the audit. Adoption of a new assessment standard will require assessors to adhere to a more structured format. That would require significant planning for us to implement and require a substantial training period for assessors to learn.

- The role of "assessor" to perform NIST SP 800-37 assessments does not currently exist at any commonwealth agency. The "assessor" position would be an additional role that would require new staff. In some agencies, the existing ISO or someone on the ISO staff could fill that role, but that would lead to an independence issue. No matter who fills these new roles, there would be significant training involved. It is also likely that a number of agencies will need to outsource for this service.

  Currently, about a third of our agencies have their own internal audit departments that conduct IT security audits. It is not certain at this time if all these existing internal audit departments will continue to be a resource for performing risk assessments as opposed to performing audits. If that happens, a larger number of assessments will need to be outsourced.

- There is no evidence in this report that risk assessments conducted using NIST SP 800-37 would be more thorough or economical than the existing process of audits conducted using IPPF or GAGAS. The change in process and personnel to perform the risk assessments could be significantly more expensive.

Because of the aforementioned issues as well as others, VITA CSRM would not be able to adopt NIST SP 800-37 in its entirety and in place of auditing at this time. However, we would consider forming a workgroup of commonwealth security and auditing professionals to study the proposal.

OSIG Response:

Although cost savings could take place by removing the overhead costs of IPPF or GAGAS audits on each system, OSIG recognizes the challenges described by VITA and is willing to participate in a workgroup to discuss adoption of NIST 800-37.

FUNDING FOR SECURITY AUDITS

ITRM Standard SEC501-09.1 requires agencies to identify information security requirements during business process planning. It also requires the allocation of resources needed to protect information systems and information system services. The sensitive system security audits required by ITRM Standard SEC502-02.3 should be a part of this planning and allocation process.

As noted in the "Security Audits of Systems Not Accomplished" finding, insufficient resources were often cited by agencies as a reason for sensitive system security audits not being completed between fiscal years 2014-15 and 2016-17. DPB recognized the need for additional funding and resources and began working with VITA. Based on the efforts of these two agencies, additional general funds were provided for sensitive system security audits in the Commonwealth's budget beginning in 2016-17. Through that funding, additional resources were provided in only the last year in OSIG's audit timeframe. As with any budget initiative, specific funding through the general fund was not provided to the non-general fund agencies, as each is expected to generate funding from non-general fund revenue streams.

The Commonwealth's budget for 2016-17 also provided for the establishment of VITA's Centralized IT Security Audit Services office. Each executive branch agency had an option of signing up for this service at that time. According to VITA, the Audit Services office can conduct the security audits at about $20,000 per system. This is more efficient than using private sector audit firms, potentially costing over $100,000.

DPB considered the need fully funded as it budgeted approximately $20,000 for each system needing an audit. VITA Audit Services office is fully staffed and funded to support the MOUs it has signed with agencies. Those agencies who have signed MOUs will receive the services needed and will have no further costs for the audits beyond what is required by the MOU. The MOU requires an agency to only pay what the funding model determines as the cost. If an agency decided not to have an agreement with VITA Audit Services, it made the decision to fund at a possible additional cost. Since the VITA Audit Services office is an Internal Service Fund, additional staff expansion is possible to meet the demand of the agencies seeking their services through authorized MOUs.

Without agencies either being able to complete audits on their own within the provided budget or entering into agreements with VITA Audit Services in the next budget cycle, those agency management teams risk not having a clear understanding of information security risks impacting their systems, data and operations. If agencies elect not to utilize the VITA Audit Services and they fail to complete the required audits, those agencies should be held responsible.

Recommendations:

Based on the importance of information security to the Commonwealth and individual citizens, and the potential risks associated with information security not being properly evaluated:

1. DPB and VITA should continue their current efforts to identify the needed funding during the budget cycle for the most efficient assessment and testing of sensitive-system security, either through the current system audit process or the NIST processes discussed previously in this report.

2. When an agency or institution identifies a deficiency in the proper assessment of sensitive-system security, the situation should be reported to VITA.

3. Continued expansion of VITA's Centralized IT Security Audit Services office is needed as additional agencies enter into agreements with the office to provide an efficient means of conducting IT security audits.

Management Response(s):

VITA Response:
Management elected not to provide a response.

DPB Response:
Management elected not to provide a response.

LACK OF SEPARATION OF DUTIES BETWEEN OPERATIONS AND SECURITY

ITRM Standard SEC501-09.1, Section 2.4, states that the ISO should report directly to the agency head where practical and should not report to the CIO.[2]

Executive branch agency ISOs are not consistently reporting to personnel within their agency to allow for independence and adequate separation of duties. Of 20 executive branch agencies and institutions selected to test and determine whether their ISO reported to an individual or individuals that would allow them to independently and effectively carry out their roles and responsibilities, eight directed their ISO to report to the Chief Information Officer (CIO) or someone within the IT department. One of those eight did have a compensating control whereby the ISO had a direct line of communication to the agency head.

Outside of this audit, OSIG has encountered situations where ISOs are supervised by the chief audit executives (CAEs), creating independence conflicts for those auditors by making them responsible for management functions. Risk management programs at the Commonwealth and agency/institution levels are potentially less likely to be effectively carried out when the ISO is not independent. IT operational and security needs are often competing for the same limited resources within an organization. Where ISOs report directly to the CIO or other personnel within the IT department, the risk of security needs being minimized or made secondary to operational needs increases.

Recommendation:

ISOs should be independent of their corresponding CIO while also maintaining the independence of the CAE. ITRM SEC501-09.1 should be updated to require independence of the ISO and only allow exceptions on a limited basis with compensating controls and approval from the Commonwealth's Chief Information Security Officer (CISO).

Management Response(s):

VITA Response:

VITA concurs with the observation and the recommendation. An update to ITRM SEC501 will require the independence of an agency's ISO from an agency's CIO. Any exceptions will need to be approved by the Commonwealth's Chief Information Security Officer (CISO).

[2] Although this standard is not applicable to the two universities included in our sample, adequate separation of duties is desirable to reduce conflicts created between system operability and system security.

IDENTIFICATION OF SENSITIVE SYSTEMS

ITRM Standard SEC501-09.1 requires use of a Business Impact Analysis (BIA) as a primary input to sensitivity classification and requires a system to be classified as sensitive if sensitivity is considered high concerning confidentiality, integrity or availability.

Controls are not adequate to ensure executive branch agencies are effectively identifying and reporting all sensitive systems to VITA.

Based on a review of VITA's ARCHER system (the Commonwealth's information system inventory database) for the 18 agencies and institutions sampled, 386 agency systems categorized as not sensitive were identified as having existing sensitivity conflicts as of August 17, 2017. These conflicts represent systems agencies did not identify and include in their annual sensitive system audit plan, but were identified in their BIA as being tied to a sensitive business process or sensitive data. VITA identified these sensitivity conflicts in ARCHER and followed up with agency personnel to determine whether the system should be categorized as sensitive, and if not, why.

ARCHER also had 97 systems that were identified as potentially sensitive (by VITA), but not included in the agency's most recent sensitive system audit plan.

Additionally, 24 systems belonging to 18 agencies listed in ARCHER as not sensitive or not categorized were judgmentally selected to determine whether they were in fact non-sensitive systems. Six systems were determined to be sensitive.

Each agency is responsible for identifying which systems should be classified as sensitive. While VITA has developed and documented in ITRM SEC501-09.1 a process for agencies to follow when identifying sensitive systems, guidance provided is high level and does not include specific types of data or instances where information systems and data should be considered sensitive.

In addition, while VITA has implemented a compensating control that evaluates systems not included in the agency's annual sensitive system audit plan to the agency's BIA, this process does not include evaluating systems without a sensitivity conflict. Finally, while VITA's process has identified a number of systems they believe should be categorized as sensitive, the communication of these systems to the agency and resolution of this difference was not always timely.

Weak controls over the identification and tracking of sensitive systems increases the risk those sensitive systems and the data they process and store will not be adequately protected from unauthorized use, modification or disclosure.

Recommendations:

1. Systems identified as having conflicts or potential misclassification as a non-sensitive system should be reassessed by the responsible agency and properly classified.

2. ITRM Standard SEC501-09.1 should be updated to:

   A. Provide additional information for agencies to use when determining whether a system is sensitive. At a minimum, VITA should include examples of specific types of information or activities that would require a system to be classified as sensitive.

   B. Require agencies to identify formally, where sensitivity conflicts exist. If the agency believes a system is not sensitive, it should formally document this assessment and provide it to VITA for review.

   C. Document VITA's process for reviewing agency system submissions and follow up with agency personnel where sensitivity conflicts are identified or where VITA and the agency do not agree on a system's sensitivity classification. Further, this documented process should include reviewing all agency systems (not just systems with sensitivity conflicts) within ARCHER and required timeframes and procedures for identifying and resolving conflicts.

Management Response(s):

VITA Response:
VITA concurs with the recommendations and will make the required updates to SEC501.

COMMENDATION

OSIG found that VITA has developed and documented policies and procedures to guide executive branch agencies in their cybersecurity management activities. OSIG also commends VITA for its effort to establish a centralized audit service to conduct periodic audits of sensitive executive branch agency systems. Further, OSIG noted VITA has taken steps to improve the accuracy of Commonwealth's inventory of information systems, including identifying which systems are sensitive.

AUDIT RESULTS

This report presents the results of OSIG's audit of the Commonwealth's Cybersecurity program. The following audit testing was performed with immaterial, if any, discrepancies noted:[3]

- Interviewed agency management and verified an IT Security Audit Services program was in place.
- Interviewed agency management and reviewed supporting documentation to conclude that when an agency depended on an IT service provider for services, the agency IT security auditor was able to rely on that provider's applicable IT security audits.
- Reviewed documentation that demonstrates IT security auditors used appropriate criteria as defined in ITRM Standard SEC501-09.1.
- Verified IT security auditors' documented findings and submitted results to VITA for audits conducted.
- Evaluated goals set by VITA to measure completion rates and determined goals were reasonable.

Based on the results and findings of the audit test work conducted of the Cybersecurity program, OSIG concluded that internal controls were operating properly except as identified in the report finding.

[3] Summary of Results contained in Objective 5 Results workpaper