#### MS_WordReportCover_fadeVALines

#### 2018 Commonwealth of Virginia Information Security Report

Prepared and Published by:

**Virginia Information Technologies Agency**

*VITA - Powering the commowealth’s digital government*

Comments on the

*2018 Commonwealth of Virginia Information Security Report*

are welcome

Suggestions may be conveyed electronically to CommonwealthSecurity@vita.virginia.gov

 Please submit written correspondence to:

Chief Information Officer of the Commonwealth

Virginia Information Technologies Agency

Commonwealth Enterprise Solutions Center

11751 Meadowville Lane

Chester, VA 23836

cio@vita.virginia.gov



**Contents**

[Executive Summary 4](#_Toc14262267)

[2018 Annual Information Security Report 8](#_Toc14262268)

[Commonwealth Threat Management Program 8](#_Toc14262269)

[Commonwealth Cyber Threat and Attack Analysis 8](#_Toc14262270)

[Incident trends by category 12](#_Toc14262271)

[Cyber Intelligence from Commonwealth Partners 15](#_Toc14262272)

[Security investigations by category 16](#_Toc14262273)

[CSRM Security Services Center 17](#_Toc14262274)

[Centralized IT security audit services 17](#_Toc14262275)

[ISO services 18](#_Toc14262276)

[Web Application Vulnerability Scanning Program 20](#_Toc14262277)

[Commonwealth Information Security Governance Program 21](#_Toc14262278)

[Statute requires compliance monitoring 21](#_Toc14262279)

[Audit compliance report card 21](#_Toc14262280)

[Key commonwealth security audit compliance metrics and analysis 22](#_Toc14262281)

[Commonwealth Information Security Officers Advisory Group 24](#_Toc14262282)

[Cybersecurity strategy development and monitoring 24](#_Toc14262283)

[Commonwealth Information Security (IS) Council 25](#_Toc14262284)

[Commonwealth IT Risk Management Program 25](#_Toc14262285)

[Risk compliance report card 25](#_Toc14262286)

[IT Risk Management Program Monitoring 25](#_Toc14262287)

[Nationwide Cyber Security Review 28](#_Toc14262288)

[Appendix I –Agency compliance report card 33](#_Toc14262289)

[Appendix II - Agency information security data points 35](#_Toc14262290)

[Appendix III – Cybersecurity framework results – Detail 41](#_Toc14262291)

# Executive Summary

**This 2018 Commonwealth of Virginia (COV) Information Security Report is the 11th annual report by the chief information officer (CIO) of the commonwealth to the governor and the General Assembly. As directed by § 2.2-2009(B)(1) of the *Code of Virginia,* the CIO is required to identify annually those agencies that have not implemented acceptable policies, procedures and standards to control unauthorized uses, intrusions or other security threats. In accordance with § 2.2-2009(B)(1), the scope of this report is limited to the six independent and 72 executive branch agencies, including two Level I institutions of higher education. This report does not address compliance for Level II and Level III institutions statutorily exempted from compliance with commonwealth policies and standards.**

**The CIO has established a commonwealth security and risk management (CSRM) directorate within the Virginia Information Technologies Agency (VITA) to fulfill his information security duties under §2.2-2009. CSRM is led by the commonwealth’s chief information security officer (CISO).**

This report has been prepared by CSRM on behalf of the CIO. It follows a baseline created by CSRM in 2008 to assess the strength of agency information technology (IT) security programs that have been established to protect commonwealth data and systems. A detailed listing of the agencies that were assessed and their security compliance and cybersecurity framework assessment metrics are found in the appendices of this document.

**There were significant personnel changes in information security officers throughout the commonwealth.** In 2018, commonwealth agencies appointed 13 new information security officers (ISOs), which represented 17% of all the ISOs in the commonwealth. This turnover is unusually high for the commonwealth and will result in knowledge loss within the information security community. There will be a period of time where ISOs will need to be trained on how to work within the agency and how to manage a commonwealth information security program. CSRM has been actively working with new ISOs as they are coming on board and will work to get them trained up as soon as possible.

**There were significant changes to infrastructure services in the commonwealth**. The commonwealth moved from a single provider infrastructure environment to a multisourcing service integrator (MSI) model with multiple supplier providing services to the commonwealth, including managed security services, server storage and data center, voice and data network, mainframe, messaging, end-user support and managed print services. As with any transition of services there is an increase in risk to services not functioning as expected or lack of understanding of risk introduced during change. CSRM is monitoring for the introduction of new risks as well as the looking for improvements in managing risks and operations. This monitoring occurs in several ways, including the managing the information technology risk within the program, implementation of system security plans, ensuring audits of supplier IT systems, and reviewing adequacy of the remediation plans for supplier IT security audit findings. CSRM is in the process of developing the necessary risk management and security program monitoring to ensure the environment is maintaining an adequate risk posture with functioning security controls.

**Security standards have been updated to address the changing threats to information security**. Standards are important to improve the security of information technology systems, networks and critical infrastructure. CSRM has made changes to the SEC501 and SEC525 standards to further clarify requirements for agencies and supplier. These standards now require that the agency ISO report to the agency head. In addition, updates to the SEC502 IT Security Audit Standard require that all IT security audits be conducted using a recognized auditing framework.

**Agencies using VITA centralized ISO and audit services had improved audit and risk metrics**. These services assist agencies in improving the effectiveness of their IT security program and in complying with commonwealth IT security requirements. There are 32 signed clients in 2018 for the audit services, an increase of five clients from the prior year. For the agencies using this service, the percentage of sensitive systems audited over the last three years increased to 92% from last year’s 54%. We anticipate nearly all audits of sensitive systems for these agencies to be completed by 2020. There are 33 agencies participating in the centralized ISO service. This is an increase of two additional agencies over the prior year. For these agencies, the percentage of risk assessments completed for sensitive systems has increased by 24% from last year. We anticipate nearly all of the risk assessments for agencies using the shared ISO service to be complete by 2020. Lastly, the vulnerability scanning service assisted 77 agencies and performed more than 1,300 vulnerability scans each quarter of public-facing websites in 2018. CSRM worked with agencies to reduce their footprint by decommissioning legacy applications and moving sites behind the secure perimeter. The centralized security services complement each other to identify risks to commonwealth information and develop action plans to further safeguard the commonwealth’s information assets. Agencies participating in the centralized services should continue their work with CSRM personnel to continue to bolster the agencies’ information security programs.

**Incident response playbook has adjusted with new VITA service model.** The “VITA Incident Response” playbook is a comprehensive document that details the processes that the CSRM computer security incident response team (CSIRT) will utilize to identify, contain, repair and recover from an incident. The playbook is written from the perspective of the managed security service (MSS) and incorporates standard incident scenarios. As new supplier are incorporated into the environment, the CSIRT reviews existing incident response plans, adjusts processes and modifies incident response playbooks so that they work efficiently with the other supplier and VITA. This coordination effort will promote response preparedness, consistency and overall effectiveness of the incident response program. CSRM will use the CSIRT’s incident response playbook in our evaluation of agency incident response programs.

**Virginia colleges and universities continue to be targets of cyberattacks**. According to analysis from the Multi-State Information Sharing & Analysis Center (MS-ISAC), higher education entities continue to experience a large number of cyberattacks, suffer from the most software vulnerabilities on internet-facing systems, and face a significant number of account compromises and malware infections. Based on the continuing issues facing these public institutions higher education in Virginia, we continue to recommend that additional governance be established for these institutions to promote effective information security at the commonwealth’s colleges and universities.

**Agency audit program compliance metrics continue to improve.**Audit program compliance, which includes audit plan submissions, completed audits and corrective action plan updates, was 44% for 2018. While overall compliance in the commonwealth is still less than half of the agencies, this was an improvement of 11% from the prior year. CSRM will continue to work with agencies to ensure that they have submitted their audit plans, completed audits, and corrective action plans to address the findings from the audits. In addition, as VITA’s centralized audit services continues to mature, we anticipate agency audit programs to improve. Audit program compliance is important to ensure that sensitive systems are independently assessed and that corrective action plans have been developed to address any issues.

**Risk management program results improve.** In 2018, agencies made progress on their business impact analyses, risk assessment plans and risk assessments than in the prior year. Overall, 51% of agencies were compliant with the risk management program. This represents an increase of 10% in compliance over the previous year. This increase is attributed to a continued emphasis on risk management, VITA’s centralized ISO services and additional funding provided for IT security services. CSRM determined that 86% of agencies with poor risk compliance metrics (grades of D or F) did not take advantage of the centralized ISO service offerings that could have supported their risk management efforts. Overall, CSRM anticipates that risk management program compliance metrics will continue to improve as agencies dedicate the necessary resources to address this issue.

**The commonwealth participated in the Nationwide Cyber Security Review (NCSR), a self-assessment survey aligned with in the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) to evaluate the commonwealth’s cybersecurity posture and compare with other states.** There were 65 agencies (84%) that completed the NCSR survey for 2018. The results are summarized by the core elements of the NIST cybersecurity framework, which are the following basic cybersecurity functions: identify, protect, detect, respond and recover. Survey results indicated that agencies on average have partially documented standards and/or procedures in all five cybersecurity functions. Agencies reported that their processes were least mature in the “recover” function, where agencies need to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity event. The “protect” function, related to agencies’ ability to limit or contain the impact of a potential cybersecurity event, is where agencies indicated their processes were the most mature. Agencies should use the survey results to prioritize their IT security efforts, as well as a benchmark to gauge progress in the maturity of their cybersecurity posture and assisting in cybersecurity investment decisions. Agencies should strive toward optimized maturity where each organization has policies, standards and/or procedures to achieve their objectives, and implementation is not only tested and verified but also regularly reviewed, improved and repeated to ensure continued effectiveness of their controls. The average score for each function improved in 2018 from the prior year. According to NCSR, the recommended minimum maturity level is set at a score of five and higher; agencies reported that they reached this level for nearly every function on average. Going forward CSRM will perform additional analysis on the NCSR ratings and ensure they are in line with the adequacy of an agency’s program.

**The commonwealth was a target of a sextortion email campaign**. During 2018, attackers found a new way to extort bitcoin from users. Instead of holding data for ransom, the attacker sends an email stating that they have “explicit videos” of the user that were obtained by using a remote access Trojan (RAT) that they installed on the user’s device. The attacker threatens that if the user’s doesn’t pay the extortion fee, the attacker will send the videos to everyone on the user’s contact list. In order to make this seem legitimate, the attacker includes an old password in the subject line that was harvested from a data breach. The threat goes on to state if the user pays the extortion fee, the attacker claims they will destroy all copies of the videos. These emails are intended to create fear and do not tie back to any actual activity however, without sufficient security awareness training, users will fall prey to these scams. CSRM issues advisories and recommended training for agencies to help combat these scams and others. CSRM will continue to refine training to help combat exploitation such as this campaign.

**New security controls for email access.** CSRM has worked with the messaging supplier to incorporate two-step and two-factor authentication. As expected implementing this change has reduced direct email attacks significantly this year. Attackers are constantly changing the methods they use so CSRM will monitor for a shift in attack tactics. As new attack types are discovered the CSRM incident management team works with the security and messaging suppliers to find ways to block the attacks.

**Vulnerability scanning results continue to show progress.** The scanning program continues to provide valuable insight into the existing web application vulnerabilities as well as the remediation efforts required to reduce risk to the commonwealth. CSRM assesses all public-facing sites and are adding all private sites containing sensitive data. Scan results indicate that agencies are addressing the vulnerabilities identified in the scans further securing commonwealth data. CSRM currently scans private sensitive sites with operating system level scans and will be adding application level scanning for all sensitive applications to build on the successes of the scanning program.

**New identity and access management is part of the new services offered to commonwealth agencies.** Identity management is also known as identity and access management (IAM). IAM refers to a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. Identity and access management systems not only identify, authenticate and authorize individuals who will be utilizing IT resources, but also the hardware and applications employees need to access. CSRM anticipates that these new tools will allow agencies to better manage and control access to their environments, further securing the commonwealth’s information. As part of the new offering CSRM will be developing additional policies and standards to help with standard implementation within the commonwealth.

# 2018 Annual Information Security Report

The 2018 Annual Security Report for the Commonwealth of Virginia report includes an analysis of the commonwealth threat management program, new services offered, the commonwealth information security governance program and the commonwealth risk management program.

# Commonwealth threat management program

The threat management program monitors and manages potential malicious IT attacks against commonwealth agencies and information. CSRM collects information from within the VITA IT infrastructure program, as well as agencies falling outside the scope of the IT infrastructure program to evaluate the commonwealth's threat posture overall. This information is analyzed to identify threats affecting the commonwealth, to identify widespread vulnerabilities and to respond appropriately. Some of the key components of the program are highlighted in this report.

## Commonwealth cyber threat and attack analysis

The *Code of Virginia*, *§2.2-603(F)*, requires all executive branch agency directors to report IT security incidents to the CIO within 24 hours of discovery in accordance with security standard SEC501. The CSIRT then categorizes each security incident based on the type of activity.

During 2018, the Commonwealth of Virginia continued to be a target for cyberattack.

The commonwealth experienced 33 million attack attempts on the network and more than 489,000 pieces of malware. Despite many layers of protection, the commonwealth still experienced 151 successful IT security incidents. Threat data for 2018 was limited due to the supplier transition and loss of some of our standard reporting sources.

**Insider threat was the largest attack vector during 2018.**

The commonwealth uses a defense in-depth approach that includes implementation of the Center for Internet Security (CIS) top 20 controls to harden systems. This approach has limited the number of systems being compromised by attack. During 2018, the greatest exposure was due to insider threat. Insider threat is identified as actions, whether intentional or unintentional, carried out by commonwealth employees or agents resulting in harm to commonwealth data or infrastructure. With the large number of employees turned over supporting the infrastructure combined with the unusually high loss of information security personnel across the commonwealth likely resulted in less effective monitoring of the environment. While it will be difficult to tell with certainty if any issues were a result of these changes CSRM will attempt to review the environment for areas of concern. Once a review is complete CSRM will investigate options to help reduce the chance of a similar situation occurring in the future.

In addition to the personnel aspect of the insider threat, there were a large number of assets reported lost or stolen. In preparation for transitioning to the new suppliers, VITA and the agencies worked together to verify the asset inventory. Many discrepancies were identified which is believed to be a result of the refresh process where an old device was replaced with a new one. The old device was to be picked up from the agency, have the data wiped and then sent off to disposal. After disposal, the asset inventory was to be updated with a status of disposed. The records for the pickup, wiping and disposal were not consistently provided to the agencies or VITA. As a result, it was not possible to determine whether the asset had been lost, stolen or sent to disposal. To resolve this discrepancy, the assets that could not be located were submitted as “lost” equipment. These inventory discrepancies accounted for 7% of incidents for 2018.

In addition to asset inventory discrepancies, commonwealth employees were targets for the theft of laptops and cell phones. These incidents of physical theft or loss accounted for 23 percent of incidents in 2018.

**Information disclosure was the second largest category of incidents for 2018.**

In 2018 we saw a shift in this type of incident from being triggered by phishing messages to being triggered by user error. During the first quarter, agencies were migrated to a new email system. As part of this migration, VITA implemented both two-step and two-factor authentication for email access. The new system with these additional controls reduced the number of phishing messages being delivered to mailboxes and protected email accounts from being used by attackers who have acquired credentials. However, the new email system presented challenges for employees. Data leakage incidents increased due to users sending sensitive data to the wrong recipient and including sensitive data in emails without using encryption. Providing additional security awareness training will help to protect both commonwealth employees and data. Information disclosure incidents accounted for 30% of all incidents experienced during 2018.

**Malware, also known as malicious software, continues to be a serious threat to commonwealth systems.**

As the third largest category of incidents, malware is a constant threat to commonwealth devices and data. Malware programs are designed to infect legitimate users’ computers to damage systems or provide unauthorized access to sensitive data. Malware will normally exploit a known vulnerability to gain access to the system. Once an application has been declared to be end-of-life, the manufacturer no longer provides updates for known vulnerabilities. As a result, both unpatched and end-of-life software are vulnerable to attack. During 2018, 35% of high priority incidents were due to attackers exploiting these vulnerabilities. The attacks could have been thwarted by upgrading end-of-life software to supported versions and by applying patches to vulnerable systems, reaffirming the need to apply system patches in a timely manner.

**Security awareness training is critical to protecting COV employees, systems and data from cyberattacks.**

As the attack landscape is constantly changing, the primary point of defense remains the same – the employee. While technical controls can be put in place to protect the environment, the only effective approach is employee training. The COV IT Security Standard requires all employees to take security awareness training annually. This allows a large amount of time between training for attackers to develop new techniques and employees to forget what they have learned. In order to supplement this yearly training, CSRM has developed a free service where agencies can request simulated phishing campaigns to reinforce the security awareness training and to allow users to practice their skills in a safe environment.

During 2018, CSRM modified their simulated phishing environment to work with the enterprise email environment. After the system was updated for the change, CSRM provided simulated phishing campaigns to agencies. The campaigns targeted 529 COV employees, of whom 384 opened the phishing message, 41 clicked on the link and 10 employees submitted their credentials. The chart below shows a comparison of the results from 2017 to 2018.

While the sample size is smaller than in previous years, it validates the continued need for phishing training to be included in agency security awareness programs. The CSIRT intends to increase the number of simulated phishing campaigns provided to agencies next year.

**Cybersecurity incident trends continue to be monitored.** CSRM has been working diligently to protect commonwealth systems from cyber threats. As best practices are implemented and additional layers of protection are added, attackers develop new tactics to compromise systems. CSRM is continually investigating new security controls to protect the environment from compromise.

Despite these efforts, the commonwealth experienced a spike in incidents during the last quarter of 2018. At the beginning of November, Adobe released a critical patch for Cold Fusion. Within two weeks of the patch being release, all COV Cold Fusion servers were attacked. While some agencies had applied the patch, others were still in the process of testing and deploying the patches. As a result of this missing patch, five servers were compromised. These attacks demonstrate the need to patch systems as soon as possible after appropriate testing has been completed.

**The origins of the attacks on the commonwealth’s network are monitored and tracked.** CSRM receives threat intelligence information from multiple sources. This information is incorporated into the security monitoring systems that protect the commonwealth’s data from attack. In correlating this information with our intelligences partners we are able to proactively block origins of attack before systems are compromised. During the past year, this information indicated that the top five countries where attacks against the commonwealth originated were the United States, Brazil, China, Egypt and Germany. According to the Worldwide Threat Assessment report, Russia has the ability to conduct cyberattacks from within the United States. Iranian threat actors are targeting government officials and organizations to position themselves for future cyber operations. As the source of an attack is identified by geo-location, it makes the United States appear to be the number one source of attack. As long as the data housed in the commonwealth’s IT assets continues to be a valuable resource in the global marketplace, we expect to see these threat actors look for new and innovate ways to gain access to COV systems and data. CSRM will continue to monitor the origins of these attacks and respond promptly to attacks on our networks, regardless of their origin.

****

**Attack attempts**

During 2018, over 33 million attack attempts were detected against commonwealth systems. This is a rate of one attack every 1.07 seconds. The spikes in attack attempts are indicative of new types of attack traffic being observed. When an alert is triggered, the traffic is examined to determine whether it is malicious or authorized. Systems are adjusted to prevent the malicious attack attempts from penetrating the COV network. Alerts for known authorized traffic are tuned out to reduce false positives. The drop in attack attempts following a spike is due to the tuning of the systems.

## Incident trends by category

Reported security incidents are analyzed and grouped into one of the following categories described below:

* Denial of service - Loss of availability of a COV service due to malicious activity
* Inappropriate usage - Misuse of COV resources
* Information disclosure – COV data was exposed to recipients that didn’t have a need to know this data. COV systems were not accessed as part of the disclosure.
* Malware - Execution of malicious code such as viruses, Trojans, ransomware, spyware and key loggers
* Phishing - Theft or attempted theft of user information, such as account credentials
* Physical loss - Loss or theft of any COV resource that contains COV data
* Unauthorized access - Unauthorized access to COV data

During 2018, information disclosure and physical loss tied for the top category for security incidents. The addition of two-step and two-factor authentication prevented attackers from being able to utilized stolen credentials. The migration to enterprise email caused some information disclosure incidents where users inadvertently sent emails to the wrong recipient or sent sensitive data without using encryption. In addition, COV employees were a target of theft of both laptops and cell phones. These issues can be addressed through cybersecurity awareness training which includes physical security of devices.

Malware dropped to third, with unauthorized access moving to fourth. Security awareness training, implementation of two-step and multifactor authentication, and full disk encryption are controls VITA has implemented to limit the impact of those incident categories. Teaching users to protect their passwords and to utilize unique passwords for each account sign-on instance help reduce the likelihood of such incidents. Full disk encryption is leveraged to mitigate data loss in hardware thefts; however, as this issue is also attributed to user behavior, theft prevention is also included in security awareness training.

**Malware blocked**

During phase two of the email migration project, a new web gateway product was introduced into the COV environment. This product protects COV systems from receiving malware via the internet. The new web gateway has been configured to scan all files while they are being downloaded to prevent malware from being delivered to the end user. If a file is determined to be malicious, it will not allow the user to receive the file. While the new gateway blocked 99.99% of malware, the commonwealth still experienced 35 successful malware infections. Of these successful malware infections, 37% targeted the Microsoft Office suite by overwriting memory causing buffer overflows or malware being delivered through a malicious word attachment.

**Malware Blocked**

**2016 - 2018**

**Vulnerability tracking**

As part of tracking threats to the commonwealth, CSRM monitors commonwealth systems for newly discovered vulnerabilities and incorporates them into a weekly advisory. This advisory is distributed to localities, state agencies and higher education. In 2018 the advisory identified 4,287 vulnerabilities that could affect commonwealth systems. ISOs can use this information to ensure that systems are being patched in compliance with security standards.

**Critical exploits in the wild increased by 19% from the previous year**

Zero day vulnerabilities are newly discovered vulnerabilities that do not have patches available. These vulnerabilities are prime targets for attackers. Attackers develop exploit code using these vulnerabilities to install malware on a device before the manufacturer can provide an update or patches can be applied. As attackers publish the exploit code in the wild, these zero day vulnerabilities pose an increased risk to the environment.

During 2018, the total number of critical exploits tracked by CSRM rose from 125 to 149, a 19% increase. In order to address the increased risk to the environment, CSRM implemented a series of new security controls. The chart below shows the effect that these new controls had on incidents. While the risk of being compromised by a critical exploit increased, the new controls allowed the number of incidents to remain steady. In order to continue to protect the environment from these risks it is important that critical exploits are patched as soon as possible after appropriate testing.

## Cyber intelligence from commonwealth partners

The information received from commonwealth partners includes data involving state and local governments, higher education and public schools systems. The majority of the data is reported by MS-ISAC as potential events that they have monitored on the internet. CSRM disseminates the alerts to the affected entities and tracks them as investigations, since the results of the alert are unknown. In 2018, the commonwealth completed 400 investigations for the 2,925 alerts that were received. This was a 65% increase from 2017. The following chart shows the percentage of investigations by type of entity.

**Cyberattacks against Virginia’s educational system has expanded to include public schools systems.**

During 2018, we saw an increase in the number of public school systems targeted by cyber criminals. As public schools introduce information technology into the classroom, their threat landscape expands. The most significant change was in the exposure of public education credentials harvested by hackers. The number of exposed credentials increased from 23 in 2017 to 311 in 2018. Since public education is so heavily targeted, we recommend that public school systems implement an information security program that not only incorporates cybersecurity awareness training, but also includes security controls to protect sensitive data from attack.

During 2018 Virginia colleges and universities continued to be at a significant risk for attack. Last year these entities lead in the number of cyberattacks launched against them, number of software vulnerabilities on internet-facing systems and took second place for the number of accounts compromised and the number of malware infections detected. While the raw number for compromised accounts and malware infections decreased in 2018, there was an increase in the number of reported cyberattacks and software vulnerabilities. When an internet-facing system has known software vulnerabilities, attackers look for ways to exploit these vulnerabilities to do damage to systems. Some of the methods are to deface a web page, while others look at gaining and maintaining access to those systems so they can steal valuable data. As the number of software vulnerabilities has increased, it appears that higher education may be experiencing issues with keeping software up-to-date and resolving these vulnerabilities on their system. In light of this, we continue to recommend additional guidance for these institutions. It is important to ensure that appropriate governance is established, a centralized reporting effort is developed and effective information security programs are implemented in higher education.

The below table summarizes the data we received from MS-ISAC during 2018. MS-ISAC is an organization that is comprised of state government, local government, tribal territories, elections agencies, fusion centers and institutions of education. They monitor the intelligence community and the internet for attacks against their members. As this data only contained alerts that were identified by the MS-ISAC, the potential of additional data loss is possible.

## Security investigations by category

|  | Higher education | Local government | Public school systems | COV agencies |
| --- | --- | --- | --- | --- |
| Accounts compromised | 39% | 3% | 56% | 2% |
| Malware infections | 37% | 1% | 1% | 61% |
| Cyberattacks | 67% | 7% | 13% | 13% |
| Software vulnerabilities  | 38% | 12% | 23% | 27% |
| \*Potential loss associated with records exposed | $186,086 | $38,038 | $93,790 | $57,365 |

\*Potential loss associated with records exposed assumes records were exposed and was calculated using the per capita cost by industry of a data breach from the Ponemon Institute’s 2018 Cost of a Data Breach Study: Global Analysis report and the number of security investigations.

**The CSIRT and CSRM are adjusting the cyber incident response playbooks and other security analysis tools to reflect the new multisupplier service platform environment.**

The VITA incident response playbook is a comprehensive document that details the processes that CSIRT will utilize to identify, contain, repair and recover from an incident. The playbook is written from the perspective of the managed security service (MSS) and incorporates standard incident scenarios experienced in the past. These scenarios include the steps required to process an incident and define which service tower supplier (STS) will be responsible for each step. The actions taken to handle an investigation and/or incident will be recorded in Archer, CSRM’s system of record for IT security incidents.

CSIRT has been meeting with the MSI and the MSS on a weekly basis to ensure that the incident response teams have an intimate understanding of how the incident process will work in the multisourcing environment. During these meetings, any process or procedure questions that arise are discussed to determine the most effective course of operation to facilitate resolving incidents in a timely manner.

As new supplier are incorporated into the environment, CSIRT reviews the incident response plans and provides guidance on their role in the process and how to develop their incident response playbooks to work with the other STSs, the MSS, the MSI and VITA. This coordination effort will promote response preparedness, consistency and overall effectiveness of the incident response program. CSRM will use the CSIRT’s incident response playbook to integrate with agency incident response programs.

**CSIRT provided support for the mid-term elections.** In line with the declaration of election systems as critical infrastructure CSRM provided assistance to the Department of Elections in preparing for mid-term elections. CSRM performed a comprehensive security review to ensure the different systems and infrastructure supporting the elections secure. CSRM worked with the Department of Elections to have their systems scanned for vulnerabilities, conducted a simulated phishing campaign with local registrars and participated in the command center that was set up to handle any issues occurring on Election Day. CSRM is also working to develop standard election readiness protocols in line with trending election threats.

# CSRM Security Services Center

The Security Services Center, also called centralized services, includes centralized IT security audit services, ISO services, and web application vulnerability scanning programs. These services are designed to supplement agency IT security programs and support of the overall information security in the Commonwealth of Virginia.

## Centralized IT security audit services

This program provides IT security audit services for 32 agencies, including providing assistance to develop agency IT security audit plans, conduct IT security audits, and support agency efforts to create corrective action plans to address the issues found in the audits. In 2018, audit services completed 32 IT security audit plans and audits of 50 IT security systems at 11 agencies in the commonwealth.

IT security audit plans for agencies using the IT security audit services improved by 11% from the previous year.

Agencies are required to audit their sensitive systems at least once every three years. In 2017, these audit services agencies compliance averaged 54 percent. In 2018, agencies participating in the centralized audit services were able to show auditing compliance of 92%.

After audits are completed, centralized IT audit services continues to work with the agencies to advise them on corrective action plans and scheduling of future audits.

Agencies using the centralized IT audit service have shown a marked improvement in the percentage of sensitive systems that are audited. Based on the audits that are currently scheduled, agencies that are served by VITA IT security audit services are projected to improve their IT security audit compliance metrics and should have fully compliant audit programs by 2020. This will provide further assurance that agencies are aware of any IT security issues related to their sensitive systems and are able to develop corrective action plans to address any security concerns identified.

IT audit services also works closely with the ISO service, maintaining professional segregation of information gathered, but sharing knowledge and insight of client applications, environments\ and challenges to further promote the security of the commonwealth’s information.

## ISO services

Centralized ISO services now supports 33 customer agencies, which is a slight increase from 2017. These agencies have made improvements in the number of business impact analyses (BIAs) performed, completing risk assessment plans and conducting IT system risk assessments since last year.

BIA metrics have increased. In 2018, the average ISO services BIA completion percentage improved from 75% to 97%.

There was a 29% increase in the completion of risk assessment plans for the ISO services customer agencies.

The number of IT risk assessments developed for sensitive systems increased for significantly for agencies using the centralized ISO services.

These agencies are all in various stages of their project plan, with some having been working with division staff on multiple levels of support. The past year focus has been to update and report on agency-specific business processes (business impact analysis), documenting IT system risk assessments, responding to IT security audits, and developing agency-specific policies audits have been completed at 11 agencies. After an audit has been completed, we continue to work with the primary contact to advise them on corrective action plans and scheduling of future audits.

ISO services anticipates a significant improvement in the area of risk assessments. Risk assessments, required by COV standards, help agencies identify, evaluate and prioritize risks and vulnerabilities in commonwealth systems. Agencies then develop risk treatment plans to address these concerns. Based on scheduled risk assessments, ISO services will complete nearly 100% of risk assessments for all ISO centralized service agency sensitive systems by 2020.

## Web application vulnerability scanning program

The scanning program continues to provide valuable insight into the existing web application vulnerabilities as well as the remediation efforts required to reduce risk to the commonwealth. CSRM continues to assess all public-facing sites and are adding all private sites containing sensitive data. Additionally, CSRM scans the private sensitive sites with operating system level scans and are in the process of integrating application level scanning for all sensitive applications. Over 300 alert groups were consolidated into eight common categories for analysis and ease of discussion.

|  |
| --- |
| * Client attacks
 |
| * Content management system (CMS)-lacking security updates
 |
| * Data loss and compromise
 |
| * Information leakage
 |
| * Lacking security updates
 |
| * Least privilege missing
 |
| * Secure data transmission
 |
| * Security misconfiguration
 |

This category consolidation provided a more efficient analysis of data for reporting to stakeholders. The overall risk rating of the assessed applications continues to improve with two notable exceptions. Analysis indicates an increase in the use of CMSs that contain known security issues as well as the continued use of end-of-life data encryption mechanisms. These security issues must be remediated by the individual agencies deploying the CMS instances and the deprecated transport layer security protocols. Any delay in remediating the security vulnerabilities will expose the agency and the commonwealth to a level of risk relative to the classification of the data housed within the system.

The detection rate for new alerts has not decreased in an appreciable manner over the last year indicating that remediation efforts may have plateaued. In addition, incident response analysis indicates that security incidents resulting in compromised web applications are related to application software lacking security updates. The average number of days for high and medium alerts remaining open is beyond the standard requirements for remediation.

Based on the analysis of historical data as well as software development life cycle best practices it is recommended that all web applications undergo web application scanning and certification prior to deployment. Web application scanning should also be implemented in the development and test environments to ensure that any vulnerability is uncovered at the earliest possible point during website development. The commonwealth would benefit from deploying a simple, secure, content delivery and content management mechanism as a service to agencies.

# Commonwealth information security governance program

The commonwealth’s information security governance program is responsible for monitoring performance and compliance against IT security policies and standards, setting security strategy for the commonwealth, supporting agencies in their efforts to foster secure IT security environments, and promoting information security training and awareness.

## Statute requires compliance monitoring

As directed by §2.2-2009 (B.1) of the Code of Virginia, the CIO is required to report the “results of security audits, the extent to which security policy, standards, and guidelines have been adopted by executive branch and independent agencies, and a list of those executive branch agencies and independent agencies that have not implemented acceptable security and risk management regulations, policies, standards, and guidelines to control unauthorized uses, intrusions, or other security threats.” CSRM accomplished this task by monitoring agencies’ overall compliance with IT audit program and information security risk program standards and policies. In addition CSRM started transitioning toward a maturity model which provides additional insight into agency programs. This insight will help show where the commonwealth can direct efforts to further the security program.

## Audit compliance report card

The compliance report card summarizes agency compliance with the commonwealth’s IT security standards, specifically the standards related to IT security audit and risk management. The report card measures each agency’s compliance with a letter grade of A, B, C, D or F to provide a more gradated measurement of agency compliance and more insight into changes in compliance over time.

Overall agency audit programs compliance has improved with the percentage of agencies with grades of A and B increasing from the prior year. CSRM anticipates that compliance will continue to improve that as agencies use the funds afforded them in the biennial budget for IT security, including centralized audit services.

## Key commonwealth security audit compliance metrics and analysis

Metrics are summarized below to illustrate the results of IT audit program compliance, security trends, and emerging issues as reported by state agencies.

**Agency audit programs mature in 2018.** Agencies are required to develop an IT security audit plan annually, conduct an IT security audit on sensitive systems and carry out corrective action plans for findings noted during the audits. Audit program compliance has improved from the prior year, with 44% of agencies having implemented a comprehensive audit program in 2018, compared to 33% of agencies with a complete audit program last year. Improvements can be attributed to additional audits completed with funding designated for these programs, as well as the continued growth of the VITA IT security audit services program that supports over 40% of agency IT security audit programs.

**Audit program compliance improved by 11 percent**

**Agencies generally submit IT security audit plans in accordance with requirements.**  IT security audit plans are important measure because they demonstrate the agencies’ intentions to complete the required audits of their sensitive information systems within the required timeframes. In 2018, 90% of agencies submitted an IT security audit plan. These results were consistent with last year’s metrics which were driven by VITA audit services that completed over 40% of agency IT security audit plans. This indicates that agencies are aware of this requirement and generally comply. CSRM will continue to work with the agencies that have not met this requirement and determine what additional resources are needed for these agencies to comply.

**IT security audit plans submitted**

**remained the same**

**Agency three-year audit obligation metrics improve.** Of the agencies that have established an audit plan, 36% have fulfilled their obligation to have every sensitive system audited at least once every three years, up from 28% last year. This moderate increase is attributed to agencies using funds provided for security services to conduct audits and the utilization of VITA IT audit services to conduct audits for many agencies that had not been conducting them in the past. CSRM anticipates that this metric will progress.

**Three-year audit obligation completions increased by 8%**

**Quarterly updates for corrective action plans have improved from last year.** The percentage of quarterly updates, which includes audit and risk updates, received improved 4%from the prior year. VITA ISO services agencies assisted agencies in preparing corrective action plans after agency IT security audits were completed and CSRM reminded agencies to submit their quarterly updates to confirm that issues identified during audits were addressed. CSRM anticipates agencies will continue to make progress in this metric.

**Quarterly updates received increased by 4%**

## Commonwealth Information Security Officers Advisory Group

The Information Security Officers Advisory Group (ISOAG) is a dynamic group of information security professionals, open to all state and local government personnel. The group’s goal is to exchange IT security knowledge to improve the security posture of the commonwealth. In 2018, CSRM provided knowledgeable speakers from government and private sector organizations to share their information security expertise with the group at no cost to attendees.

In addition, the members are able to earn continuing professional education credits (CPE), a requirement necessary for security professionals to maintain their security certifications and memberships in global security organizations, share best practices, provide feedback on proposed policy changes and are notified of local training opportunities. Members can attend the meetings in person or via webinar. Meeting presentation materials are posted to the VITA website as an additional resource to the group.

## Cybersecurity strategy development and monitoring

CSRM has established a cybersecurity strategy to address the security needs for the commonwealth. While the objectives of the strategy have not changed, the tactics to implement the strategy will change to adjust to the multisupplier environment.

As a part of the cybersecurity strategy, CSRM will continue to be an integral part of the IT strategic planning process to ensure security needs are addressed when considering investing in new technologies.

Governance also plays a role in cybersecurity strategy. The commonwealth’s IT security governance program is formally documented in one policy and five standards designed to assist agencies in building and documenting their individual security programs. The policy sets the commonwealth’s overall direction and establishes a framework that agency heads must follow in implementing IT security programs. In addition, templates are also available to help agencies develop their own policies.

In 2018, CSRM updated SEC-501 ”IT Information Security Standard” and SEC-525 “Hosted Environment Security Standard.” Changes were related to penetration testing, data center minimum requirements and refining the existing guidance. A more extensive update will be done in the upcoming year.

## Commonwealth Information Security (IS) Council

The Commonwealth IS Council is comprised of members from various state agencies who provide input for the direction of the commonwealth-wide information security program and raise information security awareness within the commonwealth. In 2018, the council was temporarily used as a risk advisory committee primarily focused on identifying and mitigating risks to the environment identified by the CSRM risk management program

# Commonwealth IT risk management program

The commonwealth IT risk management program provides oversight of the agencies’ risk management programs, including submission of their BIA, risk assessments and intrusion detection reporting. In addition, CSRM collected sets of data from agencies’ existing BIAs, risk assessments and data on vulnerabilities and threats. These data are used to develop the commonwealth’s overall risk program score, which indicates that more than half of the agencies have an insufficient risk management program.

## Risk compliance report card

Overall risk compliance has improved. The percentage of agencies with grades of A and B also increased from the prior year. CSRM anticipates the risk program compliance will continue to increase with agencies using the centralized ISO service and dedicating IT resources toward their risk management programs.

## IT risk management program monitoring

**Risk management program compliance improved.** Risk management program compliance increased 10% from last year due to agencies implementing a comprehensive risk management program, including business impact analysis, risk assessment plans and risk assessments. CSRM dedicated additional resources to monitor agency management. Agencies used additional IT security funding to complete perform risk management functions, including engaging VITA ISO services. CSRM recommends that agencies continue to support risk management efforts by dedicating the necessary resources to their IT risk management programs.

**Overall risk program compliance increased by 10%**

**Most agencies complete their risk assessment plans.** Agencies are required to submit a risk assessment plan on annual basis that summarizes how they plan to complete risk assessments for each of their sensitive systems. Risk assessment plan submissions improved from 77% to 85% of agencies completing their annual risk assessment plan. This was driven by ISO services agencies completing nearly 100% of their agencies risk assessment plans. CSRM recommends agencies that are unable to complete the required risk assessment plans seek assistance from VITA centralized services to ensure their risk assessment plans are developed and implemented.

**Risk assessment plan**

**submissions increased by 8%**

**Three-year risk assessment obligation compliance has improved; however, most agencies still have not met this obligation.** Agencies are required by SEC520to review their risk assessment plans for the IT systems for which they are the data owner on an annual basis. The risk assessment is the process of identifying vulnerabilities, threats, likelihood of occurrence and potential loss or impact. There were 26 agencies (34%) that provided complete risk assessment information. Of the 77 agencies, 51 agencies (66%) did not fully complete the required risk assessment information.

**Three-year risk assessment obligation increased by 11%**

**The percentage of certified ISO personnel working at the agencies has improved.**

Certification is one way to provide assurance that agency IT personnel are trained and equipped to manage agency IT security programs. The commonwealth ISO certification demonstrates that personnel have received annual information security training and have some knowledge of commonwealth information security practices. Upcoming changes to policy will also require ISO’s to report directly to the agency head reinforcing ISO independence and the critical nature of information security at the agencies. Agencies that do not have a certified ISO have an average IT security audit compliance grade of F and an average risk management grade of F. The following agencies do not have certified ISOs at the conclusion of 2018:

* Tobacco Region Revitalization Commission
* Southwest Virginia Higher Education Center
* Virginia Commission for the Arts
* Virginia Foundation for Healthy Youth

CSRM strongly recommends that these agencies participate in the ISO services or consider recruiting and hiring capable and certified ISO staff to improve their agencies IT security posture.

**The % of ISO’s that are certified increased by 7 percent**

**BIA metrics have improved from last year.** Agency BIA metrics have improved form 69% of agencies having a completed BIA to 82% of agencies having a completed a BIA, an increase of 19%from the prior year. This improvement can be attributed to agencies’ increased attention on IT security and support from VITA ISO services to complete BIAs for agencies that have not completed them in the past.

**BIA completion improved by 19%**

# Nationwide Cyber Security Review

**Commonwealth agencies participate again in the “Nationwide Cyber Security Review” (NCSR).** The NCSR questions are built on the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) core and serve as cyber network security assessment designed to measure security gaps and capabilities. The assessment provides a point-in-time analysis based on the agency’s self-assessment of their controls, policies and procedures and allows comparison between states. The five main functions of the NCSR are: identify, protect, detect, respond and recover. Each function is subdivided into categories and then further into subcategories. The number of agencies who participated in the survey increased from 39 agencies to 65 agencies, an increase of 34%. Agencies are asked to evaluate the maturity level of their processes and controls using the scoring described in the table below from the Nationwide Cyber Security Review.



**Commonwealth results are consistent with the prior year and exceed the recommended maturity levels.** For the agencies that participated, the “protect” function is the most mature function and “recover” is the least mature function in 2018, consistent with the results of prior year. As noted in the table above, the recommended minimum maturity level is a score of five or higher and agency results meet this minimum criterion for every function in the CSF. This indicates that agencies believe that that they have adequately documented their policies, standards and procedures and are in the process of implementing them for all of the functions in the framework.

**Commonwealth agencies compared favorably with their peers in other states**.

The results demonstrate that the commonwealth agencies reported maturity levels significantly higher than the maturity level of peer state agencies that took part in the survey in 2017 for every function in the framework. The most significant difference is found in the identify function, where commonwealth agencies reported they were 20% more mature than their peer agencies on average.

**Cybersecurity Framework- analysis by function**

**Identify**

This function includes asset management (AM), business environment (BE), governance (GV), risk assessment (RA) risk management (RM) and supply chain (SC). In 2018, agencies reported that the commonwealth is most mature in the RA category.

**Protect**

This function includes access control (AC), awareness and training (AT), data security (DS), information protection processes and procedures (IP), maintenance (MA) and protective technology (PT). Agencies report they were strongest in the AC category and the weakest in the IP category. CSRM will continue to support agencies as they develop in that area.

**Detect**

This function includes categories for anomalies and events (AE), security continuous monitoring (CM) and detection processes (DP). Agencies reported that the CM category was the most mature and the AE was the least mature part of this function, indicating that agencies were less confident that anomalies would be identified timely. New enterprise partners and updated security tools should result in further improvement in this area.

**Respond**

The categories for respond (RS) are response planning (RP), communications (CO), analysis (AN), mitigations (MI) and improvements (IM). The agencies reported that they are strongest on average in the MI category and indicated that the IM category was the least mature category in the function. CSRM will continue to support agencies as they progress in this area.

**Recover**

This function includes recovery planning (RP), improvements (IM) and communications (CO). The results were very similar for all of the categories, with the RP category being slightly more mature and IM being slightly less mature than the other categories. The overall recover function needs improvement to reach the desired level for the commonwealth.

# Appendix I –Agency compliance report card

|  | **Agency Secretariat** | **Audit or ISO Services?** | **Agency Acronym** | **Audit Compliance Grade** | **Risk Compliance Grade** |
| --- | --- | --- | --- | --- | --- |
| \*\* | Administration | Audit, ISO | CB | D | A |
|  | Administration |   | DGS | A | A |
| \*\* | Administration | Audit, ISO | DHRM | C | A |
| \* | Administration | ISO | ELECT | D | A |
| \*\* | Administration | ISO | VITA | A | A |
| \*\* | Agriculture & Forestry | Audit, ISO | DOF | D | A |
|  | Agriculture & Forestry |   | VDACS | A | A |
| \*\* | Agriculture & Forestry | Audit, ISO | VRC | D | A |
| \*\* | Commerce and Trade | Audit, ISO | BOA | D | A |
| \* | Commerce and Trade | Audit | DHCD | B | B |
| \*\* | Commerce and Trade | Audit, ISO | DMME | A | A |
| \*\* | Commerce and Trade | Audit, ISO | DOLI | B | A |
|  | Commerce and Trade |   | DPOR | A | A |
|  | Commerce and Trade |   | IEIA | A | B |
| \*\* | Commerce and Trade | Audit, ISO | SBSD | A | A |
|  | Commerce and Trade |   | TIC | D | F |
|  | Commerce and Trade |   | VEC | A | A |
|  | Commerce and Trade |   | VEDP | F | F |
| \* | Education | Audit | DOE | B | A |
| \* | Education | ISO | FCMV | D | A |
| \* | Education | ISO | GH | A | A |
| \*\* | Education | Audit, ISO | JYF | D | B |
|  | Education |   | LVA | F | A |
| \*\* | Education | Audit, ISO | NSU | D | F |
|  | Education |   | RBC | F | D |
| \*\* | Education | Audit, ISO | SCHEV | C | C |
| \* | Education | ISO | SMV | C | B |
| \* | Education | ISO | SVHEC | A | B |
|  | Education |   | SWVHEC | F | F |
|  | Education |   | VCA | F | F |
| \* | Education | Audit | VMFA | F | B |
|  | Education |   | VSDB | D | B |
| \*\* | Education | Audit, ISO | VSU | A | A |
| \* | Executive | ISO | GOV | D | A |
|  | Executive |   | OAG | F | F |
|  | Executive |   | OSIG | A | A |
| \* | Finance | Audit | DOA | A | A |
| \*\* | Finance | Audit, ISO | DPB | A | A |
|  | Finance |   | TAX | A | F |
|  | Finance |   | TD | B | A |
|  | Finance |   | VRA | F | F |
|  | Health and Human Resources | Audit | CSA | F | C |
|  | Health and Human Resources |   | DARS | A | B |
|  | Health and Human Resources |   | DBHDS | D | B |
| \* | Health and Human Resources | Audit | DDHH | A | A |
|  | Health and Human Resources | Audit, ISO | DHP | A | A |
|  | Health and Human Resources |   | DMAS | D | C |
|  | Health and Human Resources |   | DSS | F | D |
|  | Health and Human Resources |   | VDH | B | A |
|  | Health and Human Resources |   | VFHY | F | F |
| \*\* | Independent | Audit, ISO | IDC | D | A |
|  | Independent |   | SCC | A | C |
|  | Independent |   | SLD | C | F |
|  | Independent |   | VCSP | A | B |
|  | Independent |   | VRS | A | C |
| \* | Independent | Audit | VWC | A | B |
| \* | Natural Resources | ISO | DCR | A | A |
| \*\* | Natural Resources | Audit, ISO | DEQ | A | A |
| \* | Natural Resources | ISO | DGIF | C | C |
| \*\* | Natural Resources | Audit, ISO | DHR | D | A |
| \* | Natural Resources | Audit | MRC | A | A |
| \*\* | Natural Resources | Audit, ISO | VMNH | A | A |
|  | Public Safety |   | ABC | B | B |
|  | Public Safety |   | CASC | A | A |
| \*\* | Public Safety | Audit, ISO | DCJS | D | B |
|  | Public Safety |   | DFP | F | B |
| \*\* | Public Safety | Audit, ISO | DFS | A | A |
| \* | Public Safety | ISO | DJJ | A | A |
|  | Public Safety |   | DOC | B | A |
|  | Public Safety |   | VDEM | F | F |
| \*\* | Public Safety | Audit, ISO | VSP | D | C |
|  | Transportation |   | DMV | F | B |
|  | Transportation |   | DOAV | A | A |
| \* | Transportation | Audit | DRPT | A | A |
| \*\* | Transportation | Audit, ISO | MVDB | A | B |
|  | Transportation |   | VDOT | B | C |
|  | Veterans and Defense Affairs |   | DMA | F | F |
|  | Veterans and Defense Affairs |   | DVS | A | A |

# Appendix II - Agency information security data points

**Agency information security data points detail - Legend**

**Audit and/or ISO shared services**

Audit -Participated in VITA IT security audit service

ISO -Participated in VITA ISO program

Audit, ISO -Agency used both IT Security and audit services

**Audit plan status**

Pass - Documents received as scheduled

N/C - Missing audit plan

**Current year percentage of audit reports received**

X% - The percentage of due audit reports received based on the security audit plan

N/A - Not applicable as the agency had no audits due

N/C - The agency head has not submitted a complete IT security audit plan

**Current year percentage of quarterly updates received**

X% - The percentage of due corrective action plans and quarterly updates received

N/A - Not applicable as the agency had no quarterly updates due

**Three year audit obligation**

X% - The percentage of audit work completed as measured against the agency’s security audit plans over the past three years

N/A - Not applicable as the agency had no audits due

N/C - The agency head has not submitted a security audit plan

**Risk assessment plan status**

Pass - Documents received as scheduled

N/C - Missing risk assessment plan

**Three year risk assessment obligation completed**

X% - The percentage of risk assessment work completed as measured against the agency’s sensitive systems over the past three years

N/A - Not applicable as the agency had no risk assessments due

N/C - The agency head has not submitted an audit plan

**2018 business impact analysis status**

Pass - All documentation received as requested

Incomplete - Documentation received, but incomplete

N/C - Documentation was not submitted

**IDS quarterly reports**

Pass - Documents received as scheduled

N/C - Reports were not received

**Data set inventory**

Compliant - Data set information was provided

Non-Compliant- Data set information was not provided fully

**ISO certification status**

Pass - The primary ISO is certified

Incomplete - The ISO met all other requirements but did not attend the mandatory ISOAG meeting

N/C - The primary ISO is NOT certified

| Agency Secretariat | Agency Acronym | Agency Name | Vita ISO Services Agency | Vita Audit Services Agency | ISO Certification Status | Audit Plan Status | Current Year Percentage Of Audit Reports Received | Current Year Percentage Of Quarterly Updates Received | 3 Year Audit Obligation | Audit Program Compliance | Risk Program Compliance | Risk Assessment Plan Status | 3 Year Risk Assessment Obligation | BIA Status |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Administration | CB | Compensation Board | Yes | Yes | Pass | Pass | N/A | 100% | 0% | 66% | 100% | Pass | 100% | 100% |
| Administration | DGS | Department of General Services | No | No | Pass | Pass | 100% | 100% | 88% | 96% | 98% | Pass | 88% | 100% |
| Administration | DHRM | Department of Human Resource Management | Yes | Yes | Pass | Pass | N/A | 100% | 28% | 75% | 100% | Pass | 100% | 100% |
| Administration | ELECT | Department of Elections | Yes | No | Pass | Pass | N/A | 100% | 0% | 66% | 100% | Pass | 100% | 100% |
| Administration | VITA | Virginia Information Technologies Agency | Yes | No | Pass | Pass | 100% | 100% | 100% | 100% | 97% | Pass | 82% | 100% |
| Agriculture & Forestry | DOF | Department of Forestry | Yes | Yes | Pass | Pass | 100% | 11% | 78% | 62% | 97% | Pass | 81% | 100% |
| Agriculture & Forestry | VDACS | Virginia Department of Agriculture and Consumer Services | No | No | Pass | Pass | 100% | 100% | 100% | 100% | 100% | Pass | 100% | 100% |
| Agriculture & Forestry | VRC | Virginia Racing Commission | Yes | Yes | Pass | Pass | 100% | 100% | 100% | 100% | 92% | Pass | 100% | 100% |
| Commerce and Trade | BOA | Board of Accountancy | Yes | Yes | Pass | Pass | N/A | 100% | 0% | 66% | 100% | Pass | 100% | 100% |
| Commerce and Trade | DHCD | Department of Housing and Community Development | No | Yes | Pass | Pass | N/A | 50% | 100% | 83% | 83% | Pass | 0% | 100% |
| Commerce and Trade | DMME | Department of Mines, Minerals and Energy | Yes | Yes | Pass | Pass | 100% | N/A | 100% | 100% | 100% | Pass | 100% | 100% |
| Commerce and Trade | DOLI | Department of Labor and Industry | Yes | Yes | Pass | Pass | 0% | 100% | 57% | 81% | 100% | Pass | 100% | 100% |
| Commerce and Trade | DPOR | Department of Professional and Occupational Regulation | No | No | Pass | Pass | N/A | 100% | 100% | 100% | 100% | Pass | 100% | 100% |
| Commerce and Trade | IEIA | Center for Innovative Technologies | No | No | Pass | Pass | N/A | N/A | 100% | 100% | 85% | Pass | 10% | 100% |
| Commerce and Trade | SBSD | Department of Small Business and Supplier Diversity | Yes | Yes | Pass | Pass | N/A | 100% | 100% | 100% | 100% | Pass | 100% | 100% |
| Commerce and Trade | TIC | Tobacco Region Revitalization Commission | No | No | N/C | Pass | 0% | N/A | 0% | 61% | 38% | N/C | N/C | 25% |
| Commerce and Trade | VEC | Virginia Employment Commission | No | No | Pass | Pass | 88% | 100% | 74% | 91% | 92% | Pass | 52% | 100% |
| Commerce and Trade | VEDP | Virginia Economic Development Partnership | No | No | Pass | N/C | N/C | N/A | N/C | 34% | 25% | N/C | N/C | N/C |
| Education | DOE | Department of Education | No | Yes | Pass | Pass | 100% | 100% | 59% | 86% | 92% | Pass | 100% | 100% |
| Education | FCMV | Frontier Culture Museum of Virginia | Yes | No | Pass | Pass | N/A | N/A | 0% | 66% | 100% | Pass | 100% | 100% |
| Education | GH | Gunston Hall | Yes | No | Pass | Pass | N/A | N/A | N/A | 100% | 100% | Pass | 100% | 100% |
| Education | JYF | Jamestown-Yorktown Foundation | Yes | Yes | Pass | Pass | N/A | N/A | 0% | 66% | 89% | Pass | 83% | 100% |
| Education | LVA | Library of Virginia | No | No | Pass | Pass | N/A | 0% | 0% | 32% | 100% | Pass | 100% | 100% |
| Education | NSU | Norfolk State University | Yes | Yes | Pass | Pass | 0% | N/A | 0% | 61% | 33% | N/C | N/C | N/C |
| Education | RBC | Richard Bland College | No | No | Pass | Pass | 50% | 0% | 73% | 54% | 67% | N/C | N/C | 100% |
| Education | SCHEV | State Council of Higher Education for Virginia | Yes | Yes | Pass | Pass | N/A | 25% | 100% | 74% | 75% | Pass | 0% | 100% |
| Education | SMV | Science Museum of Virginia | Yes | No | Pass | Pass | N/A | N/A | 14% | 71% | 83% | Pass | 0% | 100% |
| Education | SVHEC | Southern Virginia Higher Education Center | Yes | No | Pass | Pass | N/A | N/A | N/A | 100% | 83% | Pass | N/A | 100% |
| Education | SWVHEC | Southwest Virginia Higher Education Center | No | No | N/C | N/C | N/C | N/A | N/C | 34% | 0% | N/C | N/C | N/C |
| Education | VCA | Virginia Commission for the Arts | No | No | N/C | N/C | N/C | N/A | N/C | 34% | 33% | N/C | N/C | 0% |
| Education | VMFA | Virginia Museum of Fine Arts | No | Yes | Pass | Pass | N/A | 0% | 0% | 32% | 83% | Pass | N/C | 100% |
| Education | VSDB | Virginia School for the Deaf and Blind | No | No | Pass | Pass | N/A | N/A | 0% | 66% | 83% | Pass | 0% | 100% |
| Education | VSU | Virginia State University | Yes | Yes | Pass | Pass | 100% | 100% | 100% | 100% | 99% | Pass | 92% | 100% |
| Executive | GOV | Office of the Governor | Yes | No | Pass | Pass | N/A | N/A | 0% | 66% | 100% | Pass | 100% | 100% |
| Executive | OAG | Office of Attorney General | No | No | Pass | N/C | N/C | 0% | N/C | 0% | 33% | N/C | N/C | N/C |
| Executive | OSIG | Office of State Inspector General | No | No | Pass | Pass | 100% | N/A | 100% | 100% | 98% | Pass | 100% | 89% |
| Finance | DOA | Department of Accounts | No | Yes | Pass | Pass | 100% | 100% | 100% | 100% | 100% | Pass | 100% | 100% |
| Finance | DPB | Department of Planning and Budget | Yes | Yes | Pass | Pass | 100% | 100% | 100% | 100% | 100% | Pass | 100% | 100% |
| Finance | TAX | Department of Taxation | No | No | Pass | Pass | 100% | 100% | 96% | 99% | 42% | N/C | N/C | N/C |
| Finance | TD | Department of Treasury | No | No | Pass | Pass | 100% | 73% | 95% | 89% | 99% | Pass | 95% | 100% |
| Finance | VRA | Virginia Resources Authority | No | No | Pass | N/C | N/C | N/A | N/C | 34% | 50% | N/C | N/C | N/C |
| Health and Human Resources | CSA | Office for Children's Services | No | Yes | Pass | Pass | N/C | 0% | N/C | 27% | 79% | Pass | 60% | 14% |
| Health and Human Resources | DARS | Department for Aging and Rehabilitative Services | No | No | Pass | Pass | 100% | 100% | 100% | 100% | 87% | Pass | 22% | 100% |
| Health and Human Resources | DBHDS | Department of Behavioral Health and Development Services | No | No | Pass | Pass | 50% | 56% | 57% | 68% | 83% | Pass | 81% | 14% |
| Health and Human Resources | DDHH | Department for the Deaf and Hard of Hearing | No | Yes | Pass | Pass | 100% | N/A | 100% | 100% | 100% | Pass | 100% | 100% |
| Health and Human Resources | DHP | Department of Health Professions | Yes | Yes | Pass | Pass | N/A | 100% | 80% | 93% | 100% | Pass | 100% | 100% |
| Health and Human Resources | DMAS | Department of Medical Assistance Services | No | No | Pass | Pass | 100% | 71% | 24% | 64% | 75% | Pass | 0% | 100% |
| Health and Human Resources | DSS | Department of Social Services | No | No | Pass | Pass | N/A | 0% | 77% | 58% | 67% | Pass | 50% | N/C |
| Health and Human Resources | VDH | Virginia Department of Health | No | No | Pass | Pass | 100% | 77% | 66% | 81% | 100% | Pass | 100% | 100% |
| Health and Human Resources | VFHY | Virginia Foundation for Healthy Youth | No | No | N/C | N/C | N/C | N/A | N/C | 34% | 50% | N/C | N/C | 100% |
| Independent | IDC | Indigent Defense Commission | Yes | Yes | Pass | Pass | N/A | N/A | 0% | 66% | 100% | Pass | 100% | 100% |
| Independent | SCC | State Corporation Commission | No | No | Pass | Pass | 100% | 100% | 87% | 96% | 75% | Pass | 0% | 100% |
| Independent | SLD | State Lottery Department | No | No | Pass | Pass | 67% | 100% | 38% | 77% | 58% | Pass | 0% | 100% |
| Independent | VCSP | Virginia College Savings Plan | No | No | Pass | Pass | 100% | 100% | 73% | 91% | 83% | Pass | 100% | 100% |
| Independent | VRS | Virginia Retirement System | No | No | Pass | Pass | 100% | 100% | 89% | 96% | 78% | Pass | 70% | 100% |
| Independent | VWC | Virginia Workers Compensation Commission | No | Yes | Pass | Pass | 100% | 100% | 100% | 100% | 83% | Pass | 100% | 100% |
| Natural Resources | DCR | Department of Conservation and Recreation | Yes | No | Pass | Pass | N/A | 100% | 100% | 100% | 100% | Pass | 100% | 100% |
| Natural Resources | DEQ | Department of Environmental Quality | Yes | Yes | Pass | Pass | N/A | 100% | 91% | 97% | 100% | Pass | 100% | 100% |
| Natural Resources | DGIF | Department of Game and Inland Fisheries | Yes | No | Pass | Pass | 0% | N/A | 33% | 73% | 75% | Pass | 0% | 100% |
| Natural Resources | DHR | Department of Historic Resources | Yes | Yes | Pass | Pass | 0% | N/A | 0% | 61% | 100% | Pass | 100% | 100% |
| Natural Resources | MRC | Marine Resources Commission | No | Yes | Pass | Pass | N/A | N/A | 100% | 100% | 100% | Pass | 100% | 100% |
| Natural Resources | VMNH | Virginia Museum of Natural History | Yes | Yes | Pass | Pass | 100% | 100% | 100% | 100% | 100% | Pass | 100% | 100% |
| Public Safety | ABC | Alcoholic Beverage Control | No | No | Pass | Pass | 20% | 100% | 61% | 83% | 83% | Pass | 0% | 100% |
| Public Safety | CASC | Commonwealths Attorneys Services Council | No | No | Pass | Pass | N/A | N/A | N/A | 100% | 100% | Pass | N/A | 100% |
| Public Safety | DCJS | Department of Criminal Justice Services | Yes | Yes | Pass | Pass | N/A | 100% | 0% | 66% | 88% | Pass | 75% | 100% |
| Public Safety | DFP | Department of Fire Programs | No | No | Pass | Pass | 0% | 50% | 35% | 56% | 83% | Pass | N/C | 100% |
| Public Safety | DFS | Department of Forensic Science | Yes | Yes | Pass | Pass | 100% | N/A | 100% | 100% | 100% | Pass | 100% | 100% |
| Public Safety | DJJ | Department of Juvenile Justice | Yes | No | Pass | Pass | N/A | N/A | 100% | 100% | 100% | Pass | 100% | 100% |
| Public Safety | DOC | Department of Corrections | No | No | Pass | Pass | 33% | 100% | 79% | 90% | 100% | Pass | 100% | 100% |
| Public Safety | VDEM | Virginia Department of Emergency Management | No | No | Pass | N/C | N/C | N/A | N/C | 34% | 33% | N/C | N/C | N/C |
| Public Safety | VSP | Virginia State Police | Yes | Yes | Pass | Pass | 0% | 100% | 0% | 61% | 75% | Pass | N/C | 100% |
| Transportation | DMV | Department of Motor Vehicles | No | No | Pass | Pass | 80% | 0% | 62% | 52% | 89% | Pass | 31% | 100% |
| Transportation | DOAV | Department of Aviation | No | No | Pass | Pass | 100% | 100% | 100% | 100% | 100% | Pass | 100% | 100% |
| Transportation | DRPT | Department of Rail and Public Transportation | No | Yes | Pass | Pass | 100% | 100% | 100% | 100% | 100% | Pass | 100% | 100% |
| Transportation | MVDB | Motor Vehicle Dealer Board | Yes | Yes | Pass | Pass | N/A | 100% | 100% | 100% | 83% | Pass | 100% | 100% |
| Transportation | VDOT | Virginia Department of Transportation | No | No | Pass | Pass | 100% | 100% | 70% | 90% | 79% | Pass | 73% | 100% |
| Veterans and Defense Affairs | DMA | Department of Military Affairs | No | No | Pass | N/C | N/C | N/A | N/C | 34% | 42% | N/C | N/C | N/C |
| Veterans and Defense Affairs | DVS | Department of Veterans Services | No | No | Pass | Pass | 100% | N/A | 100% | 100% | 100% | Pass | 100% | 100% |

# Appendix III – Cybersecurity framework results – Detail

National Cyber Security Review (NCSR) Results

**Maturity Level Legend**

7 – Optimized

6 – Tested and Verified

5 – Implementation in Process

5 – Risk Formally Accepted

4 –Partially Documented Standards and/or Procedures

3 – Documented Policy

2- Informally Performed

1 - Not Performed

*0 -Agency did not complete the survey*

*\* Recommended maturity level is 5 or higher*

| **Agency** | **Detect** | **Identify** | **Protect** | **Recover** | **Respond** |
| --- | --- | --- | --- | --- | --- |
| Department of Criminal Justice Services | 2.33 | 2.06 | 2.26 | 1.67 | 1.68 |
| Department of Forestry | 5.07 | 1.63 | 2.91 | 1.67 | 1.12 |
| Alcoholic Beverage Control | 2.6 | 3.03 | 3.23 | 1.22 | 2.29 |
| Motor Vehicle Dealer Board | 2.28 | 3.95 | 3.94 | 1.83 | 1.96 |
| Virginia Department of Transportation | 2.4 | 3.78 | 4.01 | 3.33 | 2.52 |
| Department of Taxation | 3.91 | 3.55 | 3.66 | 3.67 | 3.66 |
| Department of Social Services | 3.93 | 2.94 | 3.64 | 5.33 | 5.48 |
| Richard Bland College  | 4.09 | 4.22 | 4.44 | 4.22 | 4.32 |
| Department of Corrections | 7 | 3.52 | 4.2 | 3 | 3 |
| Center for Innovative Technologies | 4.13 | 4.6 | 5.45 | 2.67 | 2.39 |
| Department of Juvenile Justice | 4.6 | 5.15 | 5.01 | 3.56 | 3.32 |
| Department of Professional and Occupational Regulation | 3.5 | 4.96 | 4.16 | 4.67 | 4.98 |
| Virginia State Police | 3.53 | 5.26 | 4.37 | 5.5 | 4.08 |
| Virginia Department of Health | 5.43 | 5.58 | 5.3 | 1 | 2.76 |
| Department of Housing and Community Development | 5.83 | 3.26 | 5.7 | 3 | 4.08 |
| Virginia Museum of Fine Arts | 6 | 2.65 | 4.86 | 4.67 | 6 |
| Department of Behavioral Health and Development Services | 5.12 | 5.14 | 5.53 | 2.33 | 3.8 |
| Virginia Department of Emergency Management | 5 | 5.2 | 5.06 | 5 | 5 |
| Jamestown-Yorktown Foundation | 5.85 | 5.01 | 5.1 | 5.33 | 4.12 |
| Office of Attorney General | 5.15 | 5.24 | 5.2 | 5.22 | 5.47 |
| Office for Children's Services | 5.22 | 4.12 | 6.44 | 5 | 4.83 |
| Department of Environmental Quality | 4.15 | 5 | 5.49 | 6 | 5.96 |
| Marine Resources Commission | 5.8 | 5.19 | 5.51 | 4.94 | 5.17 |
| Virginia Employment Commission | 5.17 | 5.6 | 5.78 | 4.33 | 4.28 |
| Department of Mines, Minerals and Energy | 4.87 | 5.18 | 5.77 | 5.67 | 5.12 |
| Department of Forensic Science | 5.08 | 5.91 | 5.47 | 4.33 | 5 |
| Department of Elections | 5.72 | 5.08 | 5.48 | 5.67 | 5.32 |
| Virginia Racing Commission | 5.45 | 5.42 | 5.63 | 5 | 5.33 |
| Indigent Defense Commission | 5.52 | 5.3 | 5.45 | 5.56 | 5.61 |
| Office of the Governor | 5.52 | 5.24 | 5.45 | 5.89 | 5.61 |
| Science Museum of Virginia | 5.52 | 5.31 | 5.45 | 5.56 | 5.61 |
| Southern Virginia Higher Education Center | 5.52 | 5.24 | 5.52 | 5.56 | 5.61 |
| Virginia Museum of Natural History | 5.52 | 5.24 | 5.52 | 5.56 | 5.61 |
| Compensation Board | 5.69 | 5.76 | 5.41 | 5 | 5.15 |
| Department of Game and Inland Fisheries | 5.87 | 5.8 | 5.38 | 5.78 | 4.67 |
| Department of Historic Resources | 5.93 | 5.8 | 5.5 | 4 | 5.15 |
| Department of Labor and Industry | 5.52 | 5.24 | 5.61 | 5.56 | 5.68 |
| Frontier Culture Museum of Virginia | 5.76 | 5.69 | 5.5 | 5.22 | 5.45 |
| Department of Education | 5.51 | 4.62 | 6.3 | 4.33 | 5.72 |
| Department of Aviation | 4.54 | 5.61 | 5.72 | 5.67 | 6.96 |
| Gunston Hall | 5.76 | 5.35 | 5.74 | 5.67 | 5.65 |
| Board of Accountancy | 5.69 | 5.76 | 5.66 | 5.44 | 5.29 |
| Department of Human Resource Management | 5.93 | 5.8 | 5.54 | 5.67 | 5.53 |
| Department of Health Professions | 5.76 | 5.94 | 5.87 | 5.33 | 5.68 |
| Department of Planning and Budget | 5.76 | 5.86 | 5.8 | 6 | 5.61 |
| Virginia Workers Compensation Commission | 5.45 | 6.1 | 6.22 | 5.44 | 5.42 |
| Library of Virginia | 6.03 | 5.82 | 6.34 | 5.33 | 5.32 |
| Department for Aging and Rehabilitative Services | 6 | 6 | 6 | 6 | 6 |
| Department for the Deaf and Hard of Hearing | 6 | 6 | 6 | 6 | 6 |
| Department of General Services | 5.87 | 6.12 | 6.29 | 6 | 5.92 |
| Department of Medical Assistance Services | 6.27 | 5.8 | 6.23 | 6.22 | 5.81 |
| Department of Treasury | 6.08 | 5.83 | 6.14 | 5.89 | 6 |
| Virginia Department of Agriculture and Consumer Services | 6.46 | 5.74 | 6.68 | 5.33 | 6.01 |
| Department of Fire Programs | 6.48 | 6.55 | 5.93 | 5.67 | 6.04 |
| Department of Motor Vehicles | 6.27 | 6.05 | 6.74 | 6.33 | 6.67 |
| Virginia Retirement System | 6.73 | 6.58 | 6.65 | 5.22 | 6.08 |
| Office of State Inspector General | 5.77 | 7 | 6.86 | 7 | 5.68 |
| Department of Veterans Services | 6.27 | 7 | 6.54 | 7 | 6.8 |
| Virginia Information Technologies Agency | 6.87 | 6.47 | 6.58 | 7 | 6.89 |
| Department of Accounts | 7 | 6.91 | 6.85 | 6.22 | 6.4 |
| Virginia State University | 6.87 | 6.87 | 6.75 | 7 | 6.44 |
| Department of Conservation and Recreation | 7 | 6.83 | 6.78 | 7 | 6.6 |
| Department of Small Business and Supplier Diversity | 7 | 6.97 | 6.99 | 7 | 7 |