VIRGINIA IT AGENCY

2019 COMMONWEALTH OF VIRGINIA INFORMATION SECURITY REPORT

Commonwealth Security and Risk Management

VIRGINIA IT AGENCY

Prepared and Published by:

Virginia Information Technologies Agency

VITA - Powering the commowealth's digital government

Comments on the
2019 Commonwealth of Virginia Information Security Report
are welcome and may be conveyed electronically to
CommonwealthSecurity@vita.virginia.gov

Any paper correspondence may be sent to:

Chief Information Officer of the Commonwealth
Virginia Information Technologies Agency
Commonwealth Enterprise Solutions Center
11751 Meadowville Lane
Chester, VA 23836

VIRGINIA IT AGENCY

Contents

Executive summary **4**

Commonwealth threat management program **8**

Commonwealth cyber threat and attack analysis 8

Incident trends by category 13

Cyber intelligence from Commonwealth partners 15

Security investigations by category 16

CSRM centralized services **17**

Centralized IT security audit services and ISO services 17

Web application vulnerability scanning program 17

Commonwealth information security governance program **19**

Statute requires compliance monitoring 19

Commonwealth Information Security Officers Advisory Group 19

Commonwealth Information Security (IS) Council 19

Risk Advisory Committee 19

Commonwealth IT audit program **20**

Audit compliance report card 20

Key Commonwealth security audit compliance metrics and analysis 20

Commonwealth IT risk management program **24**

Risk compliance report card 24

IT risk management program monitoring 24

Nationwide Cyber Security Review **27**

Appendix I –Agency compliance report card **37**

Appendix II - Agency information security data points **43**

Appendix III – Cybersecurity framework results – Detail **48**

Executive summary

This 2019 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 seven independent and 70 executive branch agencies, including two Level I institutions of higher education. This report does not address compliance for Level II and Level III institutions, which are statutorily exempted from compliance with Commonwealth information security 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 is 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 are 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.

CSRM is supporting agency risk management and third party governance efforts. As part of the VITA governance program, CSRM has developed and implemented methodologies for monitoring and managing risks associated with third party service providers. Within the multi-sourcing service integration model that VITA has adopted, CSRM plays an integral role in identifying, recommending remediation of, and tracking until resolution, cybersecurity risks and issues within the program. Additionally, VITA provides an enterprise cloud oversight service (ECOS) to evaluate and manage third party cloud service providers to ensure that cloud based service providers are able to meet the requirements of Commonwealth agencies to provide secure, dependable and resilient products to meet Commonwealth business needs. CSRM, in partnership with several customer agency information security officers, hosts monthly risk management committee meetings to discuss identified risks and issues in order to determine the potential impacts and mitigating controls. The committee documents these risks and reports risk alerts to escalate risks and issues that may have a significant impact on the enterprise or customer agencies, as necessary. As a result, VITA and the associated service providers have made significant progress in the mitigation of the potential threats and impacts of the risk and issues identified.

Operational risks are a type of business risk that results from breakdowns in internal procedures, people and systems. CSRM is currently tracking over 100 operational risks or issues (ORIs) for 37 different agencies. Sixty-two percent of the ORIs being tracked are attributed to an agency's use of end-of-life or "EOL" hardware or software. When a system is EOL, it can no longer be updated or maintained properly. This exposes the Commonwealth to a number of elevated risks: compromised data security, higher maintenance costs, problems with scalability and non-compliance. Another significant percentage (34%) of ORIs are attributed to agencies with inadequate IT auditing or IT risk management programs. IT auditing and IT risk management programs are critically important for agencies to be able to recognize threats, minimize vulnerabilities and assure that the proper corrective actions have been implemented and are working as intended.

CSRM also monitors findings or issues that are identified through IT audits and IT risk assessments. Each issue indicates a gap or deficiency in the current state of a required IT security control and the recommended implementation of the IT security control. Each IT control is categorized into one of 17 control groups. The control group that was most frequently identified with issues (19% of all reported issues) is the "access control" group. Poor access control creates an increased risk that agencies will be exposed to unauthorized

access of data, fraud or the shutdown of IT services. To address this issue, CSRM is recommending the implementation of an identity access management (IAM) solution for the Commonwealth. IAM will create an automated framework for policies and technologies to ensure that users are properly authorized and have appropriate access to technology resources.

CSRM has demonstrated success in the remediation of systemic issues and ORIs within the environment by requiring those items to be addressed in the agency IT strategic plans. While this had led to improved agency security compliance scores and has reduced the amount of EOL software and hardware within the environment, more work must be done in order to continue to improve our security posture, such as timely flaw and vulnerability remediation.

VITA continues to help agencies shift their information technology services to cloud-based platforms securely. CSRM is working to ensure that cloud services are implemented in a manner that continues to ensure the availability, security, and privacy of Commonwealth and citizen data. This requires ongoing oversight and management to ensure compliance through service level agreements and other means. The Governor issued Executive Order 19 directing agencies to move their applications to the cloud. CSRM has provided support for moving agency applications to the cloud securely. VITA will ensure that workloads are optimized for cloud consumption prior to migration to the cloud.

About half of agencies have implemented the requirement for information security officers to report to agency heads. Commonwealth security standards require agency information security officers (ISOs) to report to their agency heads. This reporting structure reflects necessity of an independent information security function separate from IT operations and the critical need to protect citizens' sensitive information. Our analysis reflects that 55% of agencies have implemented this requirement, leaving nearly half of the agencies (45%) that have not complied with this requirement. Agencies should take the necessary steps to implement this required change in their organizational structure so agency ISOs have the appropriate authority to enact necessary security protocols in the agencies. In the future ISOs that do not report to their agency head will not be certified, impacting their compliance grade.

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 70 agencies (90%) that completed the NCSR survey for 2019. 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 2019 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. CSRM will perform additional analysis on the NCSR ratings and ensure they are in line with the adequacy of an agency's program.

Cyberattacks continue to threaten Virginia colleges and universities. According to analysis from the Multi-State Information Sharing & Analysis Center (MS-ISAC), higher education entities continue to experience a

large number of account compromises, malware infections and exposed vulnerable devices with public internet addresses. Due to a data breach with the MyFitnessPal smartphone app, over 14,000 accounts at three Virginia universities were exposed. The second largest threat to college and universities is malware. Attackers can infect these websites with malware then use that malware to gain access to the research or other resources available through the colleges. These institutions are also vulnerable to other attacks, including: spoofing, which is the act of disguising a communication from an unknown source as being from a known, trusted source and password cracking, which is the process of recovering passwords from data that have been stored in or transmitted by a computer system. As a way to better understand the complexities of their environment and provide support, CSRM reviewed the NCSR survey results to determine which educational entities participated and found four entities completed the survey. CSRM will encourage all Virginia colleges and universities to complete the NCSR survey going forward to assess their security and risk posture and benchmark with other colleges and universities in the Commonwealth and around the country. CSRM will continue to reach out to Virginia colleges and universities in support of their efforts to protect Commonwealth information and combat cyberattacks.

Agencies have improved the timeliness of remediating audit and risk findings associated with critical controls. Critical controls, as defined by the Center for Internet Security (CIS), are an identified set of measures and tactics that when implemented effectively protect organizations from known cyberattack vectors. In 2018, it took agencies an average of 565 days to close findings associated with critical controls. In 2019, the average number of days to remediate critical controls reduced to 331 days, which is a reduction of 41%. Although far from ideal, this improvement shows that CSRM's directive and encouragement to agencies to remediate critical findings quickly has reduced the number of critical vulnerabilities that expose the Commonwealth's data and information. CSRM will continue to investigate new methods to report outstanding and overdue findings to further encourage agencies to remediate critical findings quickly. We recommend that agencies dedicate the appropriate resources to remediate their findings timely. Agencies should prioritize and remediate findings by criticality, first addressing the findings that area associated with critical controls.

Centralized services continue to address agency audit and risk management needs. VITA offers centralized services for audit services, risk management services (called ISO services) and vulnerability scanning. Agencies that used both audit services and ISO services achieved an average audit compliance grade of B, higher than the average agency audit grade of C for non-audit services agencies. Agencies that used both audit and ISO services reached an average risk compliance grade of A, compared to non-ISO service agencies that had an average compliance grade of C. Audit Services and ISO services have taken steps to assist agencies in meeting their compliance requirements. In addition, CSRM's vulnerability scanning service continues to provide vulnerability scanning and assists agencies to reduce the number and impact of vulnerabilities associated with Commonwealth applications to further secure Commonwealth data. We anticipate further improvements in compliance and security as agencies utilize the centralized services.

CSRM works with the service providers and agencies to conduct the first annual cyber tabletop exercise. In coordination with National Cyber Security Awareness Month, CSRM worked with the multi-service integrator (MSI) to plan a tabletop exercise for the service tower suppliers (STSs) and the agencies to exercise their incident response plans. The exercise started with a phishing attack that turned into a full-blown Commonwealth incident. As information was injected into the incident, agencies turned to their policies and procedures to determine how they should respond. Sometimes agencies found their incident response plans worked very well. Other times they discovered that their plans did not work the way they expected and would need to be changed to adequately address the incident. The event lasted for eight hours with a four hour lessons learned session following the end of the exercise. Practicing incident response policies and procedures before an actual incident occurs allows agencies to test, adjust and mature their incident response plans.

Overall agency audit and risk compliance metrics were consistent with the prior year. Audit compliance metrics show a slight decline of 2% in overall compliance, while risk metrics show an improvement of 3% over

the prior year. We anticipate that both programs will improve as agencies' IT security programs mature and the necessary resources are dedicated to addressing agency requirements for audit and risk activities. CSRM will encourage agencies to use centralized ISO and audit services to achieve compliance. In addition, agency ISOs may be required to attend additional training. CSRM also reviews audit and risk compliance as a part of the IT strategic planning process.

Ransomware attacks targeted the Commonwealth. During 2019, two public school systems were prey to ransomware attacks. One of the schools, attacked by the Ryuk ransomware variant, was able to recover in about 12 hours due to their use of cyber hygiene best practices, backups and network segmentation. The second school system was prey to a social engineering attack. The school was advised by one of their software vendors to remove their anti-virus software because it was causing problems with their application. Once the anti-virus software was removed, the school systems was compromised by Emotet and Trickbot malware, facilitating the installation of the ransomware to their systems.

The Commonwealth experienced one successful ransomware attack in 2019. Agency IT vendors had a private internet connection tied into an agency's network which was used for remote administration. Poor security practices, and circumventing VITA's IT security stack led to Phobos ransomware compromising a server exposed on the public internet. This server then acted as a gateway to a handful of other agency servers. Proper network segmentation contained the spread to a very small portion of the agencies systems. Proper cyber hygiene practices will help reduce the impact of a ransomware infection. CSRM is also working with the Commonwealth Information Security (IS) Council to study the Commonwealth's susceptibility, preparedness, and ability to respond to ransomware attacks. In addition, CSRM will develop guidelines, best practices and recommendations to prevent ransomware attacks.

CSRM develops a new quantitative cyber risk analysis model, with planned implementation in 2020. The CSRM risk management team is developing an accurate and defendable methodology to estimate costs associated with the detection, response, and recovery activities associated with cyber security incidents within the Commonwealth executive branch, independent agencies and institutions of higher education. As this model matures, CSRM anticipates that it will provide executive leadership an enhanced ability to make informed risk based decisions.

2019 Annual Information Security Report

The 2019 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

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 2019, the Commonwealth of Virginia continued to be a target for cyberattack. The Commonwealth experienced over 30 million attack attempts on the network and blocked more than 457,092 pieces of malware. Despite many layers of protection, the Commonwealth still experienced 200 successful IT security incidents. Threat data for 2019 was limited due to the supplier transitioning to new reporting tools. This activity has been completed and full data will be available for 2020.

30% percent of all incidents were the result of successful malware attacks. As the 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. Multiple attack vectors can be used to carry out cyberattacks. The two primary avenues of attack seen by the Commonwealth are phishing emails containing malicious links or attachments and infected website redirection.

Cybercriminals often develop malware to exploit known vulnerabilities in a system. Systems are most vulnerable to these types of attacks when they are running unpatched and/or end-of-life software. Once an application has been declared to be end-of-life, the vendor no longer provides security updates for known vulnerabilities. In order to protect systems from this attack vector, system must be patched and/or upgraded to a supported version of the software.

In May 2019, Microsoft discovered the BlueKeep vulnerability in their Remote Desktop Protocol. This vulnerability would allow an attacker to perform remote code execution on the system allowing them to perform tasks such as creating user accounts, manipulating data and installing additional programs on the system. Before Microsoft could patch it, attackers were incorporating the vulnerability in exploit kits. As patches were released, CSRM worked with their supplies to get systems patched as soon as possible. However, before all patches could be deployed, the Commonwealth experienced three incidents involving exploit kits and one ransomware infection.

Attackers often target the human factor. When attackers cannot gain access to systems and data by exploiting vulnerabilities, they attempt to compromise users. Most of these attacks are achieved through phishing or malicious spam (malspam) emails.

Phishing is a fraudulent attempt to obtain sensitive information through the act of sending an email to a user while falsely claiming to be an established legitimate enterprise. The email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security number or bank account numbers. The website, however, is bogus and will capture and steal any information the user enters on the page.

Malspam email may contain a malicious attachment but most times contains a link to a malicious website or file. The link may take the user to a phishing website that requests the user to provide some information or it

may take the user to a malicious website that automatically downloads a malicious file with or without the users knowledge. If the malspam message does not include a link, but includes an attachment instead, it will likely be malicious. While email can be scanned for malicious attachments and links, the indicators for types of activity change so rapidly that border protections have a hard time keeping up.

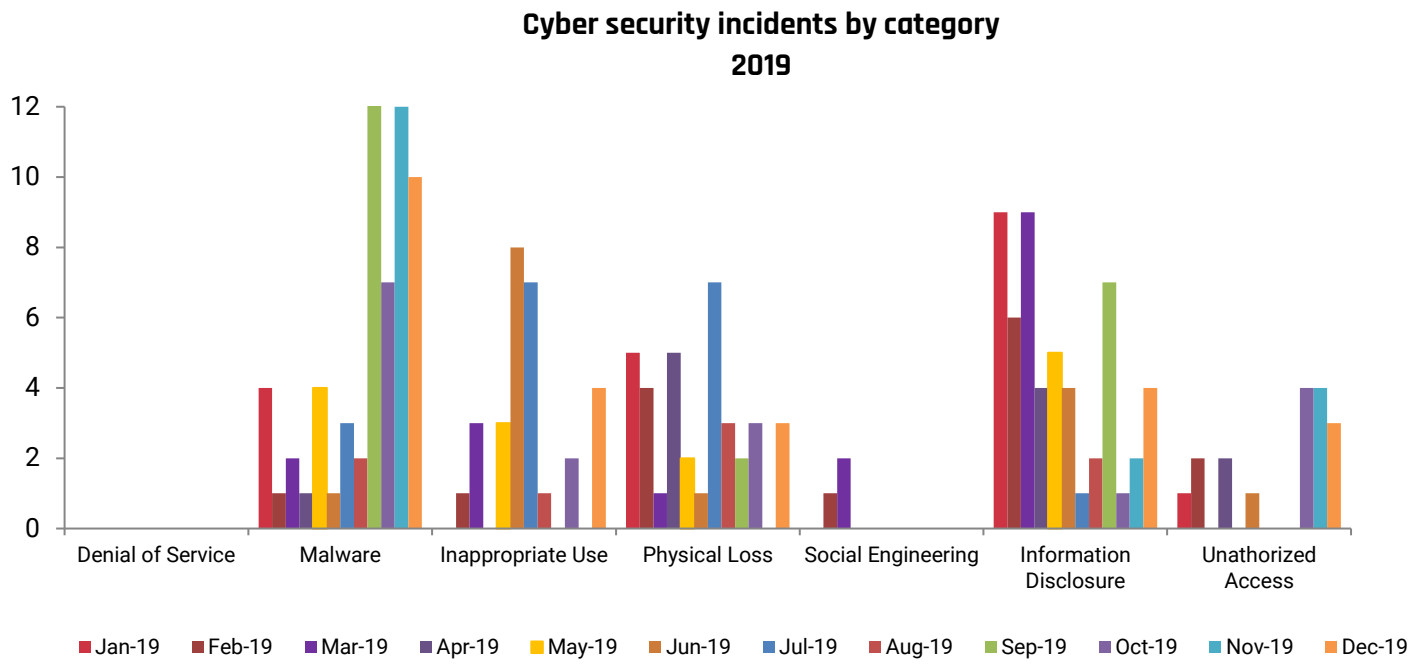
Most malware attacks are financially motivated. During 2019, the most prevalent types of malware across U.S. public entities were Trojans. Some of these Trojans were used to steal information while others were used as a mechanism to secure a ransom from the entity. Of the top 10 ten malware infections reported by MS-ISAC in 2019, six of these were banking Trojans. The Commonwealth only experienced three of the top 10, all of which were related to the banking industry. Emotet was most prevalent with 10 of the 62 infections. Emotet can be used to steal information or to install additional malware on a device. As more malware gets installed, more holes develop in the layers of protection around the device. Once a device is vulnerable, the attacker can install ransomware on the device in an attempt to encrypt the data and collect a fee.

Ransomware infects the machine then waits for commands from a command and control server. Once the handshake is established, the ransomware starts encrypting the data. Once the data has been encrypted, the ransomware displays a note on the screen requesting payment for the decryption key. This payment is normally requested in bitcoin so that the payment cannot be traced. If the entity pays the ransom, there is no guarantee that the key will be provided or that it will actually decrypt the data. The best protection from ransomware is to have a good clean backup of the data so that the device can be wiped and the data restored.

CSRM recommends best practices to combat malware. As Commonwealth Security has implemented many layers of protection to reduce the risk of malware infections, there are still a number of best practices that need to be followed:

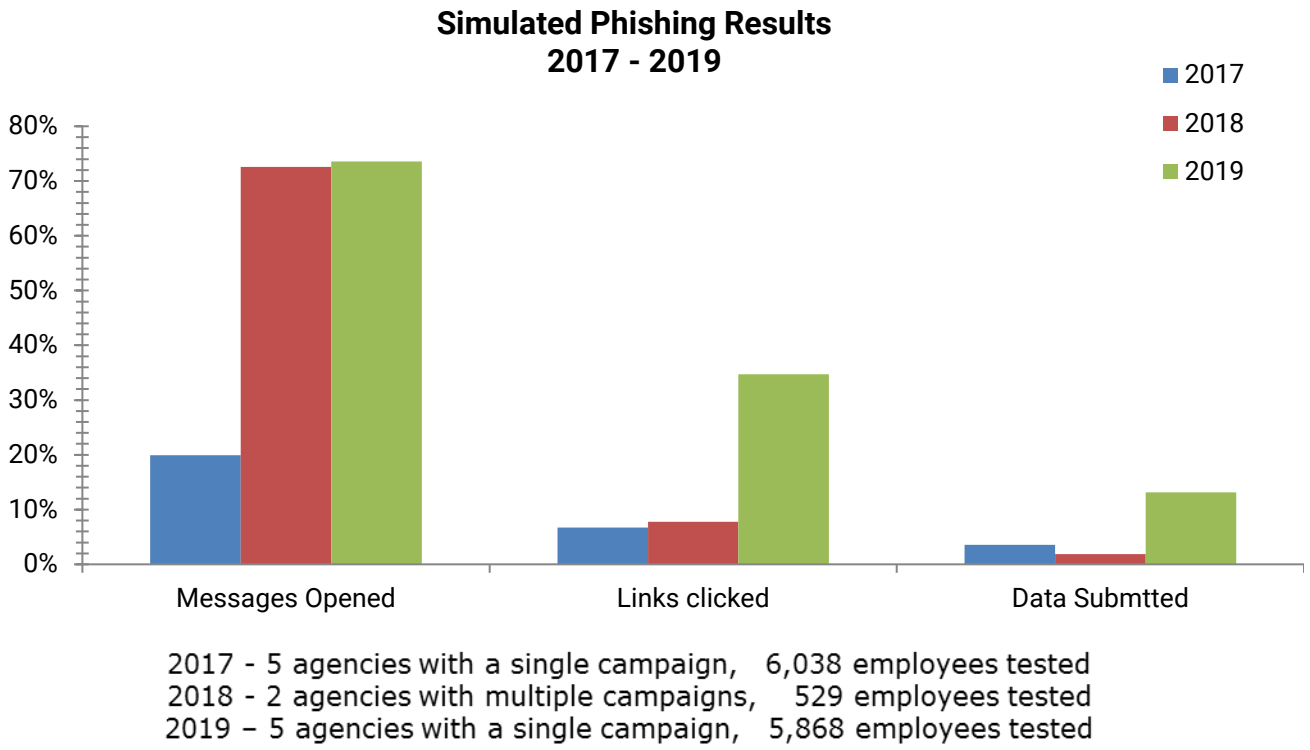
- all systems need to be patched and/or upgraded to supported versions of software
- controls need to be optimized to prevent successful cyberattacks
- users need to be given on-going security awareness training that includes:
    - Safe browsing habits
    - How to identify suspicious email messages
    - What to do if something appears suspicious
    - What not to do if something appears suspicious
    - How to report it

Information disclosure was the second largest category of incidents for 2019. Information disclosure incidents continued to be a threat. These incidents all revolve around the user. Unencrypted emails containing sensitive data, physical documents were misfiled and sensitive information was mailed to the wrong recipient. While the new multi-factor authentication protected exposed credentials from being utilized, it has not resolved the human error issues with data disclosure. Providing additional security awareness training will help to protect both Commonwealth employees and data. Information disclosure incidents accounted for 27% of all incidents experienced during 2019.



Security awareness training is critical to protecting COV employees, systems and data from cyberattacks. As the attack landscape is constantly changing, the last line 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 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.

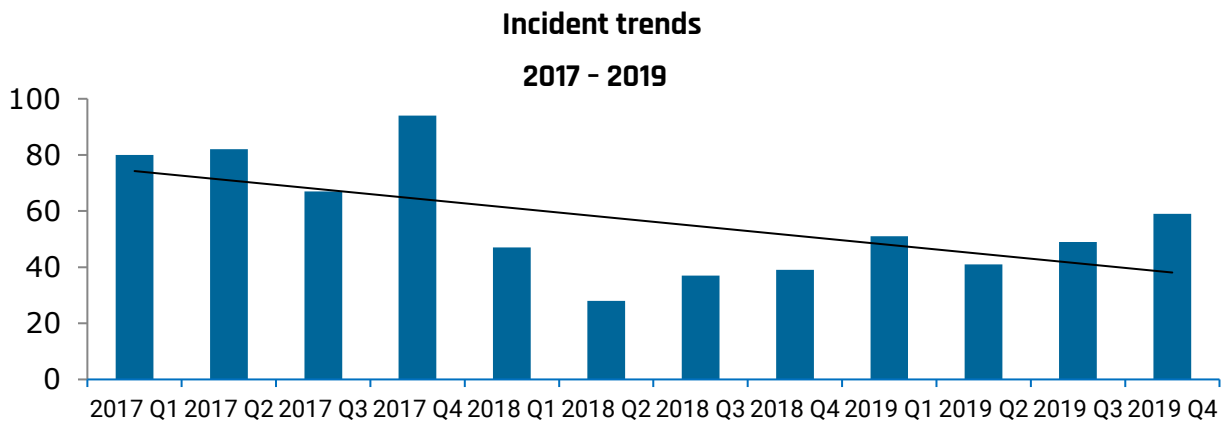
During 2019, CSRM provided simulated phishing training to 5,868 COV employees across several agencies. Of the employees targeted, 4,317 employees opened the phishing message, 2,037 clicked on the link and 770 employees submitted their credentials. The chart below shows a comparison of the results over the past three years (2017 to 2019).



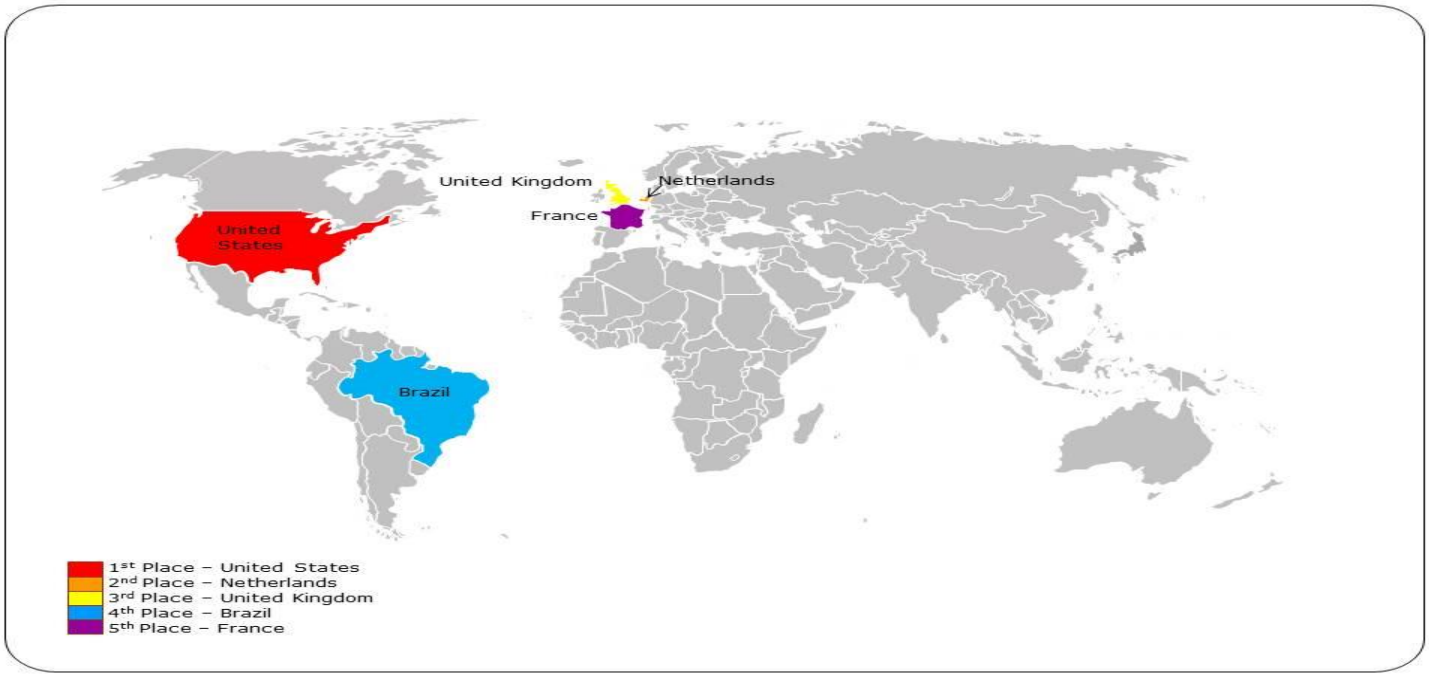
While the 2019 sample size is similar to 2017, the results show that 13% of users exposed their credentials in 2019, about a 10% increase over 2017. This re-emphasizes the need for continuous security awareness training to be included in agency security awareness programs. The CSIRT intends to increase the number of simulated phishing campaigns provided to agencies next year. In 2020, VITA will have additional authority in the Code of Virginia to establish minimum IT security awareness training requirements for all employees and contractors. VITA will develop a curriculum that include activities, case studies, hypothetical situations and other methods of instructions to improve and certify the effectiveness of IT security awareness particularly in areas related to phishing and ransomware attacks to meet this requirement.

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.

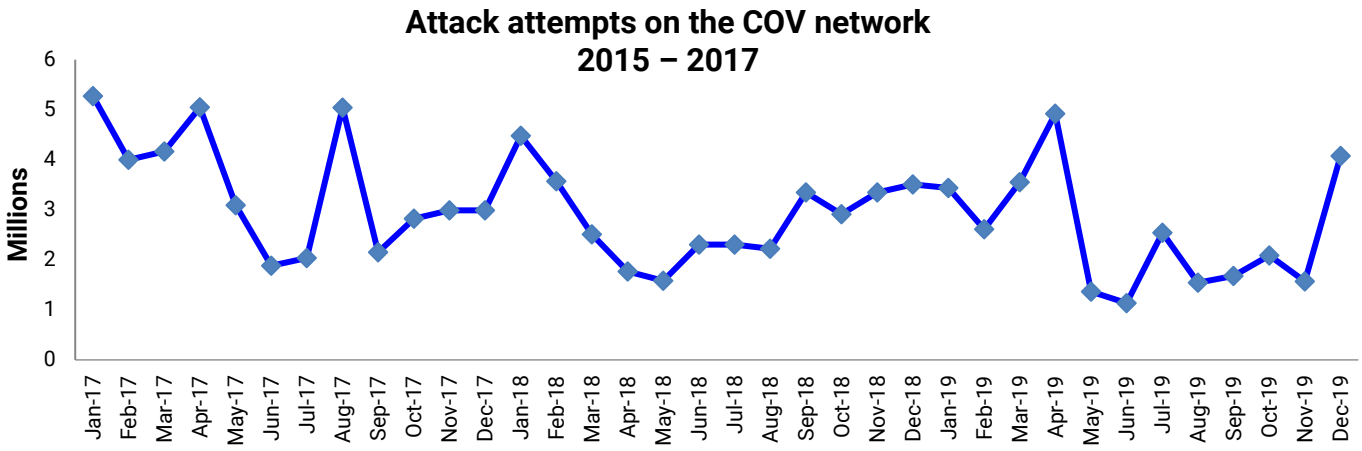
Despite these efforts, the Commonwealth experienced a spike in incidents during the last quarter of 2019 due to a malspam campaign. During the holiday season, it is not unusual for attackers to send spam messages, phishing messages and malicious attachments in an attempt to get users to respond to their attack. When deals are too good to be true, they should be ignored. However, users are not always thinking of it that way as they are trying to get everything done during the hurried holiday season. As a result, they are more vulnerable at that time of year. In order to prevent these attacks from impacting the Commonwealth, it is important that security awareness training is reinforced.



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 intelligence partners, we are able to proactively block origins of attack before systems are compromised. During 2019, this information indicated that the top five countries where attacks against the Commonwealth originated were the United States, Netherlands, United Kingdom, Brazil and France. It is important to remember that attack origination does not define attack attribution.



Attack attempts are persistent. During 2019, approximately 30,517,158 million attack attempts were detected against Commonwealth systems. This is a rate of one attack every 0.97 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.

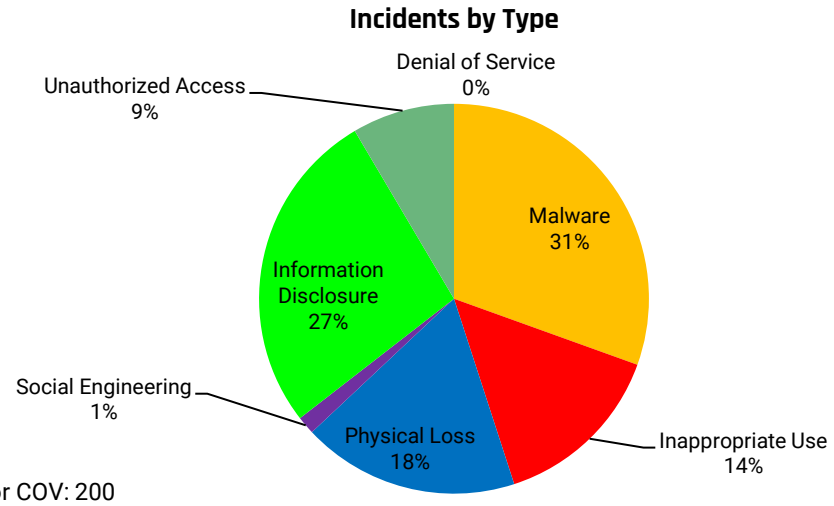


Incident trends by category

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

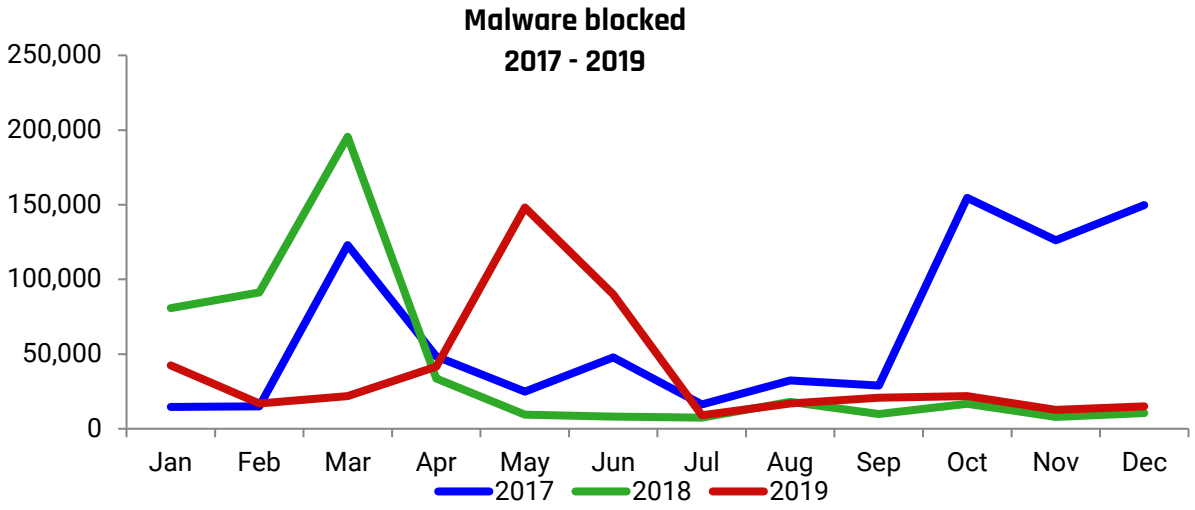
- Denial of service - Loss of availability of a COV service due to malicious activity
- Inappropriate usage - Misuse of COV resources
- Information disclosure – COV data was exposed to recipients that did not have a need to know this data. COV systems were not accessed as part of the disclosure.
- Malware - 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 2019, malware was the top category for security incidents. Information disclosure moved to second place followed by physical loss, inappropriate use, unauthorized access and social engineering. The COV environment did not experience any denial of service (DOS) attacks during 2019.

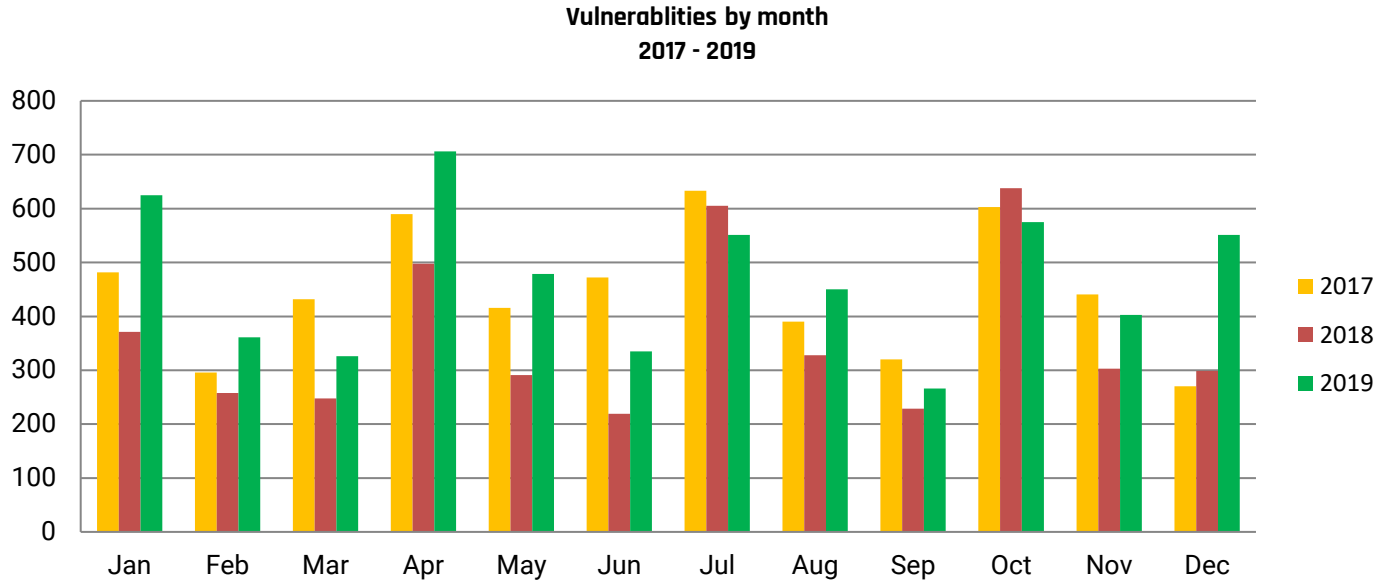


Total incidents for COV: 200
Estimated cleanup costs: $120,000

Malware is blocked. The Commonwealth has multiple layers of protection against malware infections occurring on COV devices. During 2019, these layers of protection blocked approximately 457,092 pieces of malware. Even with multiple layers of protection, the Commonwealth still experienced 61 successful malware infections.



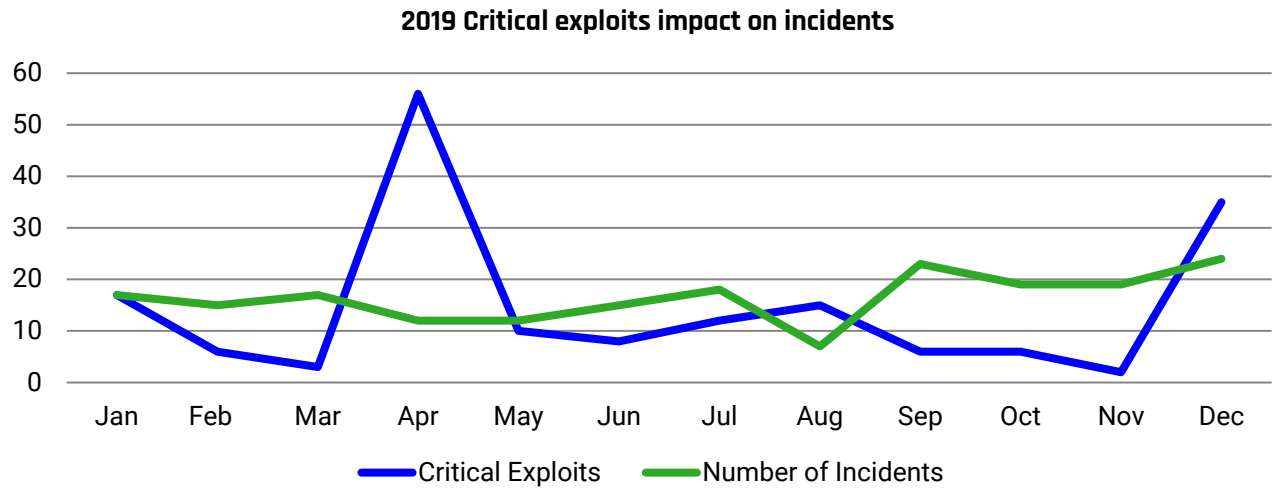
Vulnerability tracking is in place. As part of tracking threats to the Commonwealth, CSRM monitors Commonwealth systems for newly discovered vulnerabilities and incorporates them into a weekly advisory. This advisory is distributed to localities, state agencies and higher education institutions. In 2019, the advisory identified 5,628 vulnerabilities that could affect Commonwealth systems. This is a 131% increase over 2018. ISOs can use this information to ensure that systems are being patched in compliance with security standards.



Critical exploits in the wild increased by 4% 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.

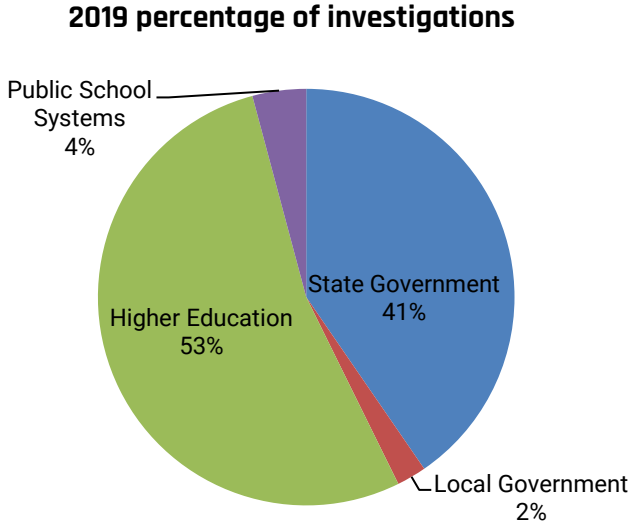
During 2019, the total number of critical exploits tracked by CSRM rose from 169 to 176, a 4% increase. As the chart below indicates, a spike in critical exploits is followed by an increase in the number of incidents. This is due to the attacker being able to compromise a system before patches were available or could be applied.

Each incident is analyzed to determine the root cause. This information is then used to strengthen protections to mitigate the risk of future attack. However, critical exploits still remain a risk. The best way to protect the Commonwealth from this is to patch 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 2019, the Commonwealth completed 463 investigations for 16,062 alerts that were received. This was a 16% increase in the number of investigations and a 449% increase in the number of alerts from 2018. The increase in alerts were due to the 2018 data breach with MyFitnessPal described below. The following chart shows the percentage of investigations by type of entity.



Cyberattacks against Virginia's higher education systems have targeted the user.
During 2019, we saw a new threat to higher education. As students, faculty and staff embrace technology, they are being targeted through these new information sharing mediums. Smartphones now come with many installed applications that may provide full access to the device if the software is compromised. In February 2018, the MyFitnessPal App was compromised. The attackers used the Smartphone app to harvest credentials for over 150 million users. The data from the breach was then released on the Dark Web in Feb. 2019. As a result of our partnership with the MS-ISAC, CSRM learned that over 14,000 users at 3 Virginia institutions of higher learning had been compromised. It was unknown whether the users had changed their credentials before the data was released. As a result, all the users had to be contacted and informed that they needed to change their passwords anywhere those credentials were used.

In addition to the credentials being harvested, the fact that the application was vulnerable needs to be addressed. Not all application vendors release security patches in a timely manner and not all users understand the process and/or the need to patch their devices. As a result, many of the vulnerabilities continue to exist. When the users store personal and/or sensitive data on their devices, the risk is increased. While there are technologies available that can be used to protect the data, it is unclear as to whether they are being implemented across all devices.

As we approach a more mobile and connected world, it is important to protect the users and the Commonwealth's data from exposure. 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 the Multi-State Information Sharing and Analysis Center (MS-ISAC) during 2019. MS-ISAC is an organization that is comprised of state government, local government and tribal territories. 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 (15,737)	95%	1%	2%	2%
Malware infections (237)	53%	0%	1%	46%
Cyberattacks (34)	21%	6%	3%	71%
Software vulnerabilities (54)	46%	6%	2%	46%
***Potential loss associated with records exposed**	$2,135,964	$17,238	$52,824	$33,306

*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 2019 Cost of a Data Breach Study: Global Analysis report and the number of security investigations.

CSRM provided information security support for elections in the Commonwealth. In line with the declaration of election systems as critical infrastructure, CSRM provided assistance to the Department of Elections in preparing for elections. CSRM performed a comprehensive security review to ensure the different systems and infrastructure supporting the elections were secure. CSRM worked with the Department of Elections to have their systems scanned for vulnerabilities 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 will also be supportive of Board of Elections efforts to develop to develop security regulations and standards and monitoring of local county and city security policies and procedures to promote the security and integrity of the Virginia voter registration systems. CSRM will continue to provide support for the primary elections and the upcoming presidential elections.

CSRM centralized services

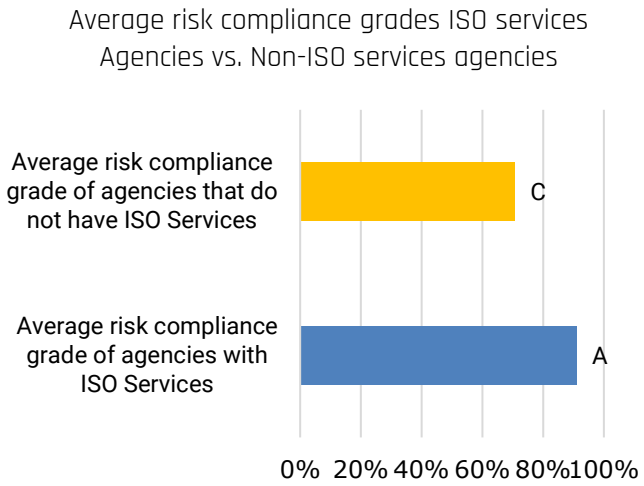
CSRM offers centralized services, also called the security services center, including IT security audit services, ISO services, and web application vulnerability scanning programs. Audit and ISO services are optional programs that agencies can acquire based on their particular needs. Web application vulnerability scanning is a mandatory program that identifies potential weaknesses in agency websites and recommends actions to address concerns identified in the scans. All these services supplement agency IT security programs and support information security in the Commonwealth.

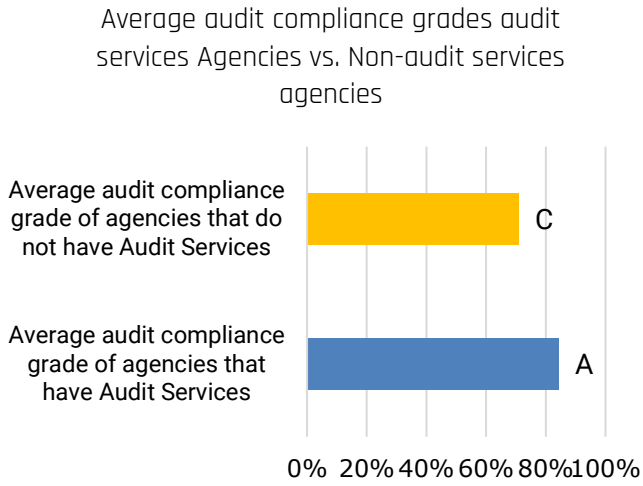
Centralized IT security audit services and ISO services

Centralized audit services assists agencies create their IT security audit plans, conducts IT security audits, and supports agency efforts to create and submit corrective action plans to address the issues found in the audits. Audit services customer agencies have an average audit compliance grade of A, which is 13 percentage points greater than those agencies that are not customers of the audit services.

Centralized audit services also works closely with the ISO service. Centralized ISO services supports 33 customer agencies. The centralized ISO services helps agencies maintain their key IT risk management tools, including Business Impact Analysis (BIAs), risk assessment plans and IT system risk assessments.

The average risk compliance score for agencies utilizing Centralized ISO services out performs the average risk compliance score for all Commonwealth agencies, indicating that ISO service agencies have supported Commonwealth efforts towards compliance. ISO services anticipates additional improvements in risk compliance as centralized services continues to help agencies complete risk assessments, update their BIAs, submit risk assessment plans, and address remediation for control weaknesses.





Web application vulnerability scanning program

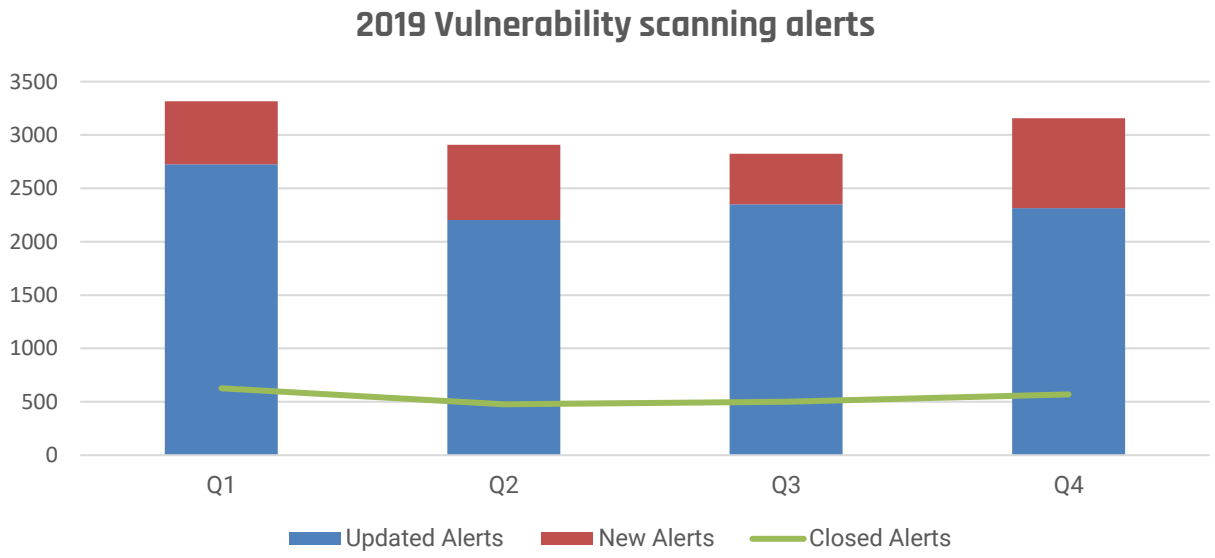
The scanning program continues to provide valuable insight into existing web application vulnerabilities and the respective remediation efforts required to reduce their risks to the Commonwealth. CSRM continually

assesses all public-facing websites and works on having all private sites containing sensitive data added to the program, which results in approximately 6,000 targets scanned annually. Additionally, CSRM scans private sensitive sites with operating system level scans and is in the process of integrating application level scanning for all sensitive applications. Over 300 unique 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
- Deficient security updates
- Least privilege missing
- Insecure 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 CMS's 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, nor has the rate of discovering updated alerts, alerts that were previously detected and repeated. These trends may indicate that remediation efforts 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.



New alerts– alerts that were never detected before
Updated alerts – repeat scan finding alerts
Closed alert – finding was not present in the following scan, so finding was closed

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 the website development cycle. 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.

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 2019, 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.

Commonwealth Information Security (IS) Council

The purpose of the Commonwealth IS Council is to promote information security awareness within the Commonwealth and provide input for the direction of the Commonwealth-wide information security program. The committee is comprised of stakeholders from a wide variety of state agencies. The council provides guidance on Commonwealth initiatives and policies, including IT security awareness training and addressing malware.

Risk Advisory Committee

The Risk Advisory Committee monitors the IT security risks facing the Commonwealth. The committee is comprised of VITA personnel and stakeholders from Commonwealth state agencies. The committee helps to

prioritize risk and issue alerts where necessary to ensure that critical risks are mitigated timely. The committee also recommends changes to standards, policies, and procedures to address the critical risks facing the Commonwealth.

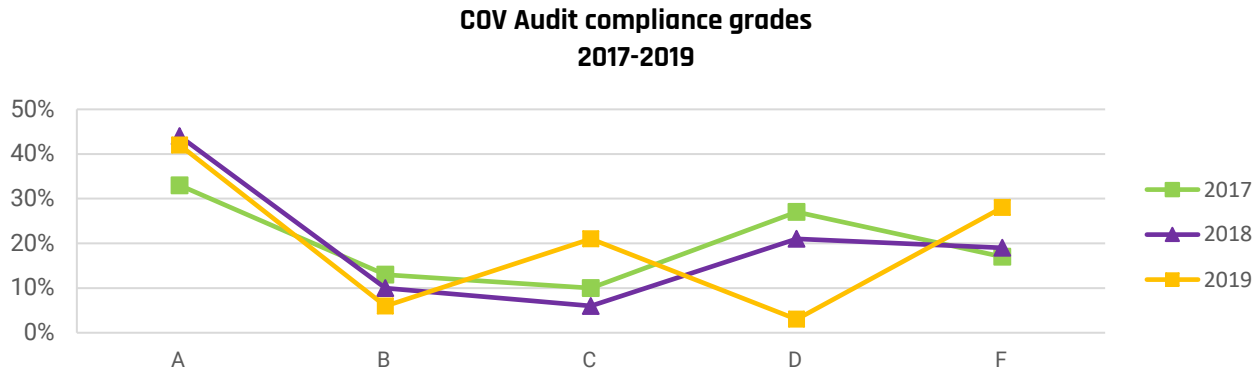
Commonwealth IT audit program

The Commonwealth IT audit program includes review and oversight of the agencies' IT auditing activities, including submission of audit plans, completed audits and corrective actions. The completion of these items are used to determine the agencies' overall audit program score.

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 audit compliance report card measures each agency's compliance with a letter grade of A, B, C, D or F. The audit compliance grade is based on an agency submitting an IT security audit plan, agency submission of quarterly updates to their IT security audit findings, and completion of required IT security audits for their sensitive systems within the required timeframes. The compliance grades provide a familiar measurement tool to reflect the degree to which agencies are completing their necessary IT security audit requirements. In addition, the compliance grades clearly identify agency IT audit strengths and opportunities for improvement.

Overall agency audit programs compliance has declined slightly from the prior year, with slightly fewer agencies earning compliance grades of an A or B. CSRM anticipates that audit compliance will continue to improve as agencies use the funds afforded them in the biennial budget for IT security, including centralized audit services.

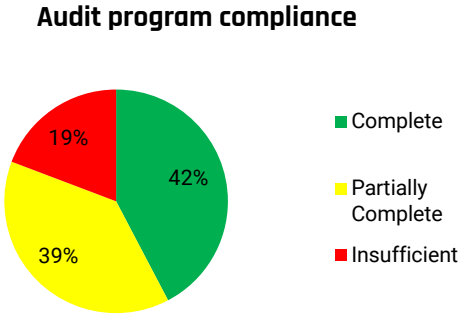


Key Commonwealth security audit compliance metrics and analysis

The following metrics provide additional information to explain IT security audit program compliance in the Commonwealth.

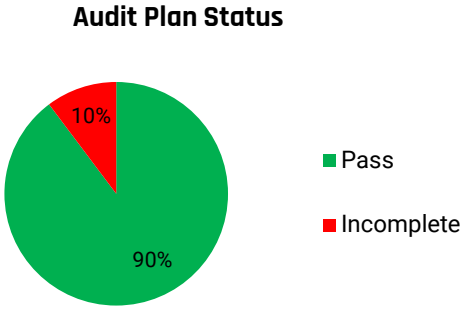
Agency IT security audit program compliance has not changed significantly.
IT security audits provide assurance that agencies have implemented the required IT controls to protect Commonwealth information. The agency audit requirements include: creating an annual IT security audit plan, performing IT security audits on sensitive systems triennially, and updating the status of corrective action plans for IT security findings discovered during the audits. Audit program compliance has declined slightly from the prior year, with 42% of agencies having implemented a comprehensive audit program in 2019. This is related to some declines in agencies completing their IT

security audits within the required timeframe. We anticipate audit program compliance will improve as agencies complete their IT security audits.



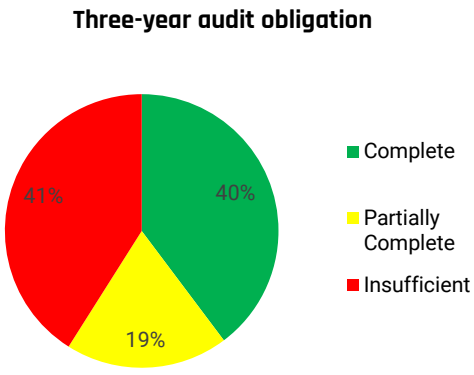
Audit program compliance decreased by 2 percent

Agencies generally submit IT security audit plans as required. IT security audit plans are important measurements because they demonstrate the agencies' intentions to complete the required audits of their sensitive information systems within the required timeframes. In 2019, 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.



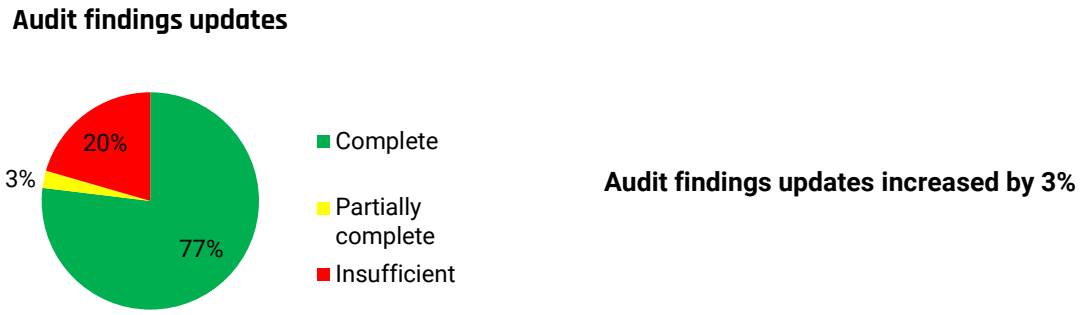
IT security audit plan status remained the same

Agency three-year audit obligation metrics continue to improve. Of the agencies that have established an audit plan, 40% have fulfilled their obligation to audit every sensitive system audited at least once every three years, an increase from 36%. This moderate increase is attributed to VITA audit services completing audits for agencies that had not conducted IT security audits in the past and agencies using funds provided for security services to conduct audits of their sensitive systems. CSRM anticipates that this metric will progress.

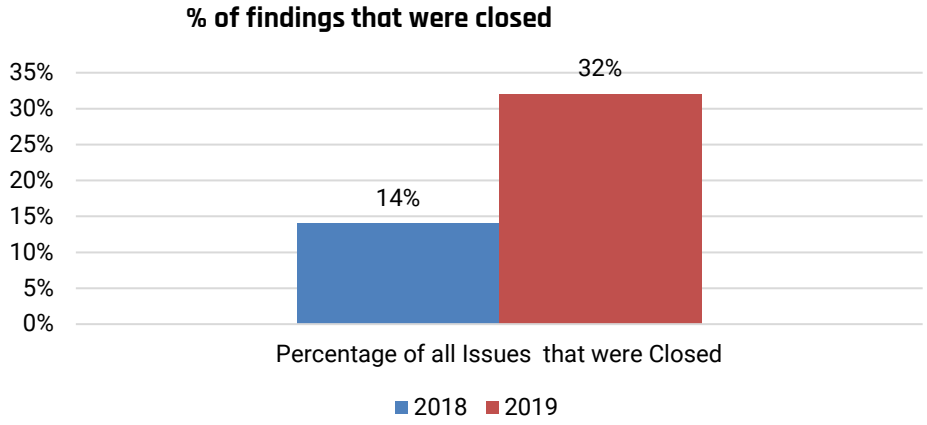


Three-year audit obligation completions increased by 4%

Most agencies that perform IT security audits provide the required quarterly updates to the findings. Our analysis indicates that 77% of agencies provided the necessary quarterly updates indicating that they are working towards addressing the issues that were identified during the IT security audits. CSRM anticipates agencies will continue to make progress in this metric as agencies are encouraged to prioritize their resources to address the most significant findings first, especially those findings that are related to CIS critical controls.

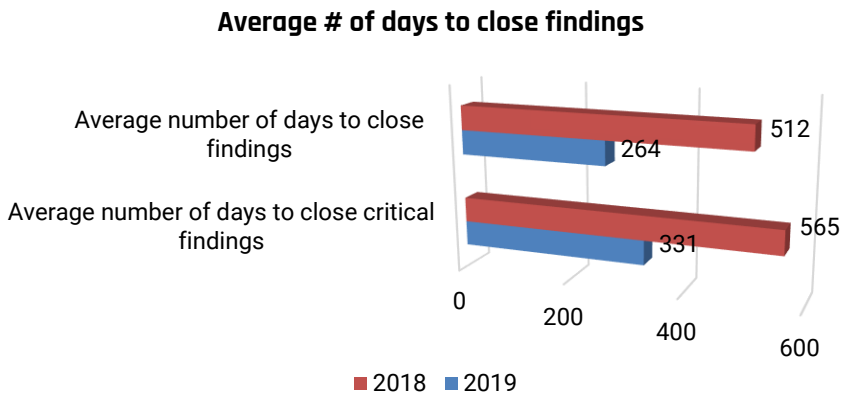


Agencies have improved the timeliness of remediating audit and risk findings. Agencies reported that they closed 1,662 of 5,179 findings, or 32% of open findings in 2019. This is a significant improvement over the previous calendar year when only 14% of open findings were closed (remediated).



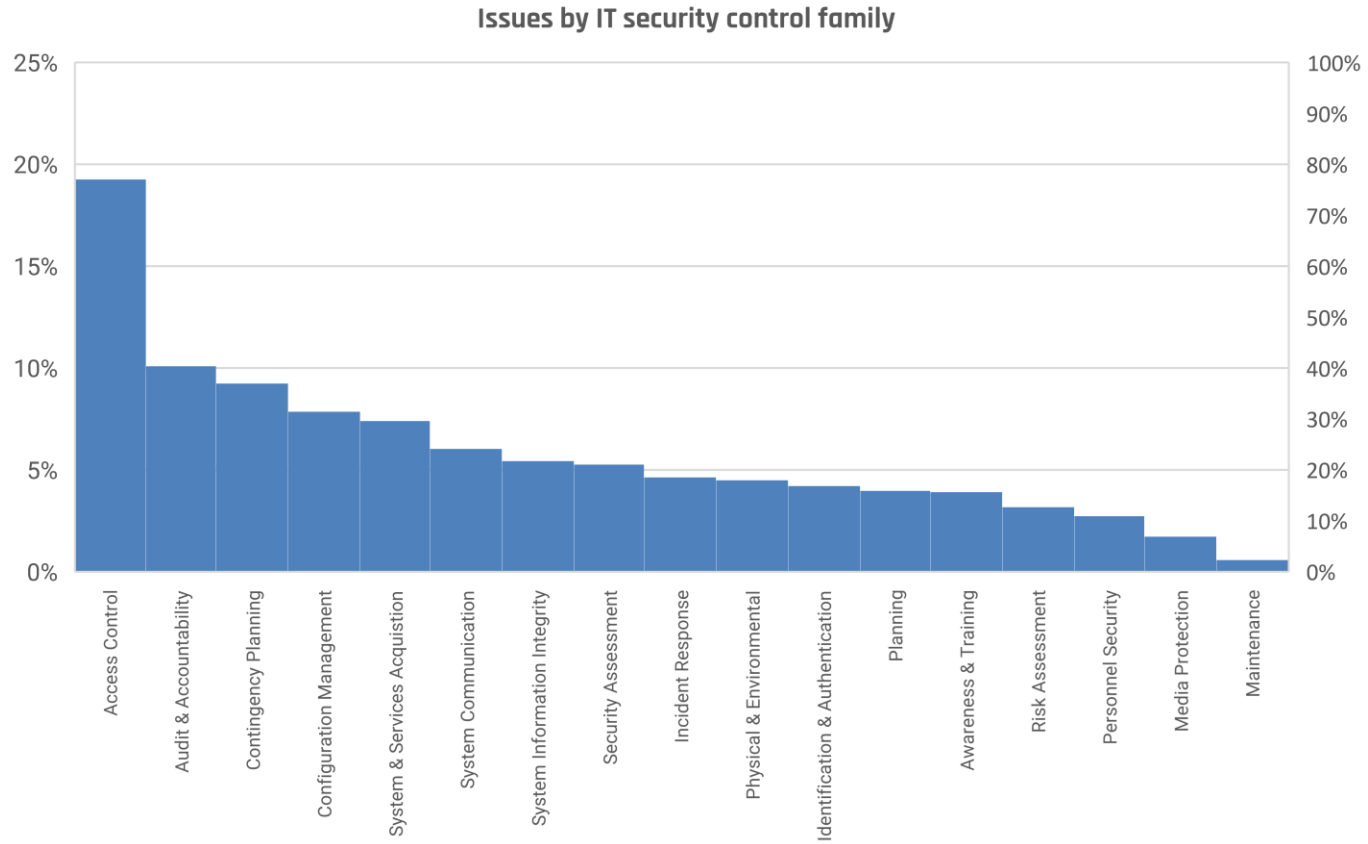
Additionally, agencies improved the timeliness of remediating findings. In 2018, findings were open an average of 512 days, taking more than a year to remediate and close information security issues that had been identified. However, in 2019, the average time it took to remediate findings reduced to 264 days, cutting the average number of days almost in half.

In addition, the timeliness for remediating critical controls also improved. We consider critical controls to be those associated with the Center for Internet Security (CIS) controls. CIS has determined that implementing effective critical controls is a best practice to protect organizations from known cyberattack vectors. In 2018, it took agencies an average of 565 days to close findings associated with critical controls. In 2019, the average number of days to remediate critical controls reduced to 331 days.



Although far from ideal, this improvement shows that CSRM's directive and encouragement to agencies to remediate findings quickly has reduced the number of critical vulnerabilities that expose the Commonwealth. CSRM will continue to investigate new methods to report outstanding and overdue findings to further encourage agencies to remediate critical findings quickly. We recommend that agencies dedicate the appropriate resources to remediate their findings timely. Agencies should prioritize and remediate findings by criticality, first addressing the findings that area associated with critical controls.

We also did an analysis on the types of findings/issues identified in 2019 through audits or risk assessments. All issues were categorized into 17 different IT security control families. The most frequently encountered issues occurred in the family of access controls (19%), followed by the family of audit & accountability (10%) and contingency planning (9%).

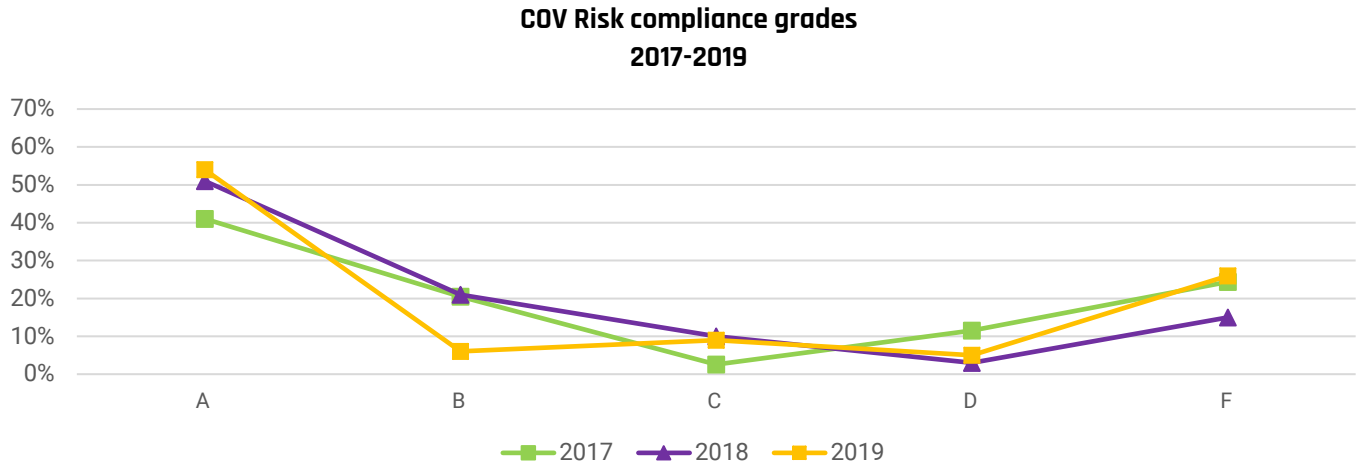


Commonwealth IT risk management program

The Commonwealth IT risk management program includes review and oversight of the agencies' IT risk management activities, including submission of their data sets, business impact analysis (BIA), risk assessment plans, risk assessments, risk findings updates, and intrusion detection reporting. The completion of these items are used to determine the agencies' overall risk program score.

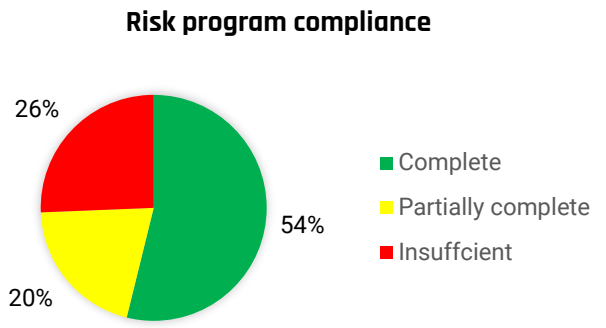
Risk compliance report card

The risk compliance grades reflect the varying maturity of risk management programs at the agencies. While the percentage of agencies that have A grades has increased, there has also been a slight increase in the agencies with failing grades as well. The risk metric was impacted by including the new requirement that agency ISO's report to their agency head and agencies that did not consistently report their corrective actions on open risk findings. CSRM anticipates the risk program compliance will increase with agencies as agencies comply with ISO reporting requirements, continue to complete IT risk assessments, and provide quarterly updates on the corrective actions taken to address risk assessment findings.



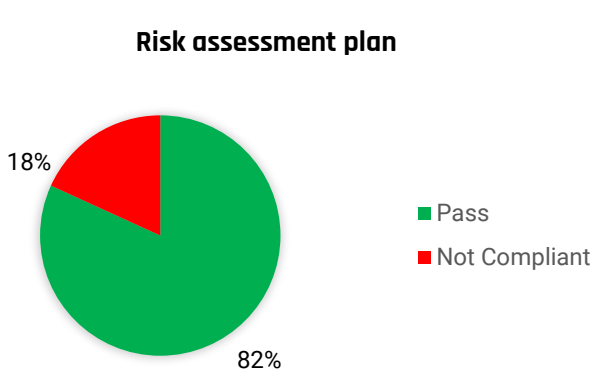
IT risk management program monitoring

Risk management program compliance slightly improved. Risk management program compliance increased 3% from last year due to agencies implementing a comprehensive risk management program, including business impact analysis, risk assessment plans and risk assessments. Agencies have continued to improve these risk management activities. ISO services compliance efforts have also contributed to this improvement. CSRM recommends that agencies continue to support risk management efforts by dedicating the necessary resources to their IT risk management programs.



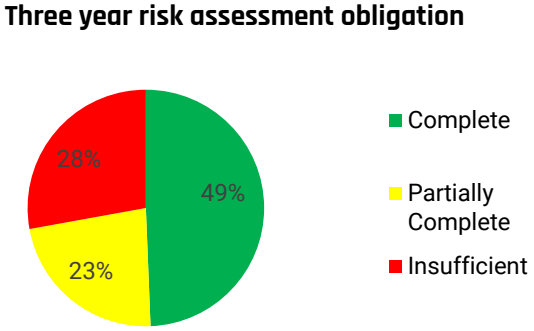
Overall risk program compliance increased by 3%

Most agencies complete their risk assessment plans. Agencies are required to submit a risk assessment plan on annual basis that indicates how they plan to complete the required risk assessments for each of their sensitive systems. Risk assessment plan submissions remained at 82%, the same metric as last year. 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 remain the same

Three-year risk assessment obligation slightly improves. This metric demonstrates agency submission of risk assessments for their sensitive applications at least once every three years. Risk assessments are important to ensure that agencies are monitoring and mitigating critical risks. Analysis shows that agencies that were insufficient decreased by 2% and agencies that were complete improved by 1%, indicating a slight shift towards agencies completing the required risk assessments. As more agencies opt in to ISO services and dedicate necessary resources to the risk programs, we anticipate this improved compliance and improvement.



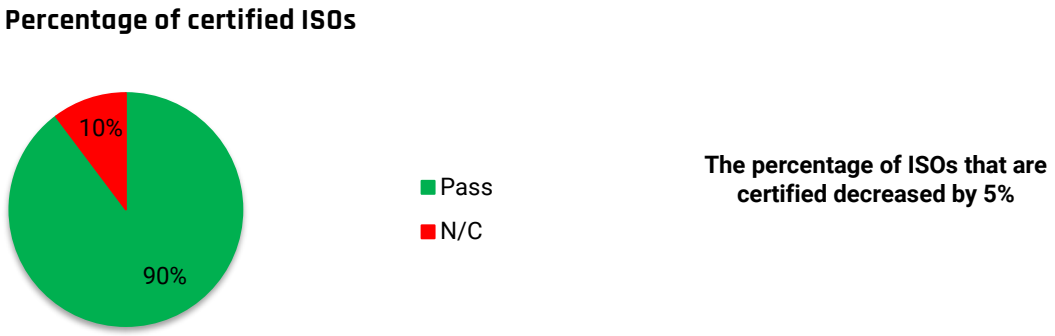
Three-year risk assessment obligation increased by 1%

The percentage of agency ISO's that are certified has declined since last year. ISO certification is one way to demonstrate an ISO's proficiency in managing the agency's IT security program. The

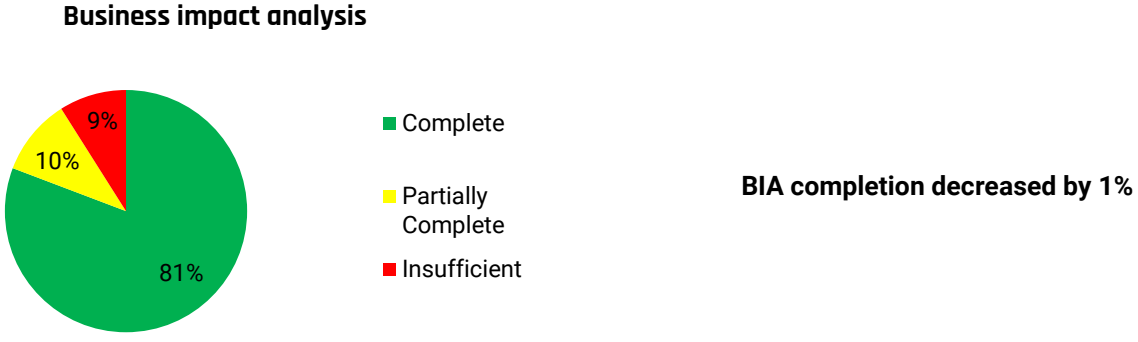
Commonwealth ISO certification demonstrates that the ISO has received annual information security training and have some knowledge of Commonwealth information security requirements. Agencies that do not have a certified ISO consistently have inferior audit compliance and risk compliance grades, with an average IT security audit grades of F and scores of 58% and risk compliance grades of 44% F. The following agencies do not have certified ISOs at the conclusion of 2019:

- Department of Behavioral Health and Development Services
- Department of Education
- Richard Bland College
- Tobacco Region Revitalization Commission
- Virginia Commission for the Arts
- Virginia Economic Development Partnership
- Virginia Resources Authority
- Virginia School for the Deaf and Blind

CSRM recommends that these agencies commit to recruiting, hiring, and training ISO staff to drive improvements in their agencies IT security posture. Recent changes to the IT security standard require that the ISO report to the agency head. CSRM is monitoring compliance and using it as criteria for ISO certification.



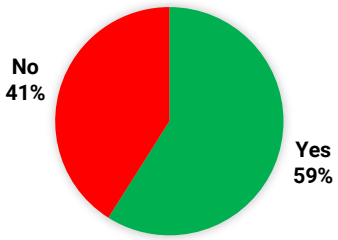
BIA metrics slightly decline. While the percentage of completed BIAs had a slight decrease, there was also a decrease in the insufficient BIA submissions by 4%, indicating there has been some improvement in the agency submission of BIAs. This improvement can likely be attributed to support from VITA ISO services and increased attention on addressing this key metric.



Over half of agency ISOs meet the requirement to report to their agency head. Commonwealth security standards require agency ISOs to report to their agency head. This organizational structure allows agency ISOs the necessary authority to carry out the Commonwealth's information security mandates and implement the

necessary safeguards to protect the Commonwealth's sensitive information. Slightly more than half of the agencies (59%) have met this requirement, leaving 41% of agencies that have not met this requirement. While we recognize that each agency has its own unique organization, CSRM recommends that agencies take the necessary steps to ensure that the ISO reports directly to the agency head to confirm information security has the needed emphasis and support in every agency in the Commonwealth.

ISO reporting to agency heads



This is a new metric for 2019 so no comparative data is available

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.

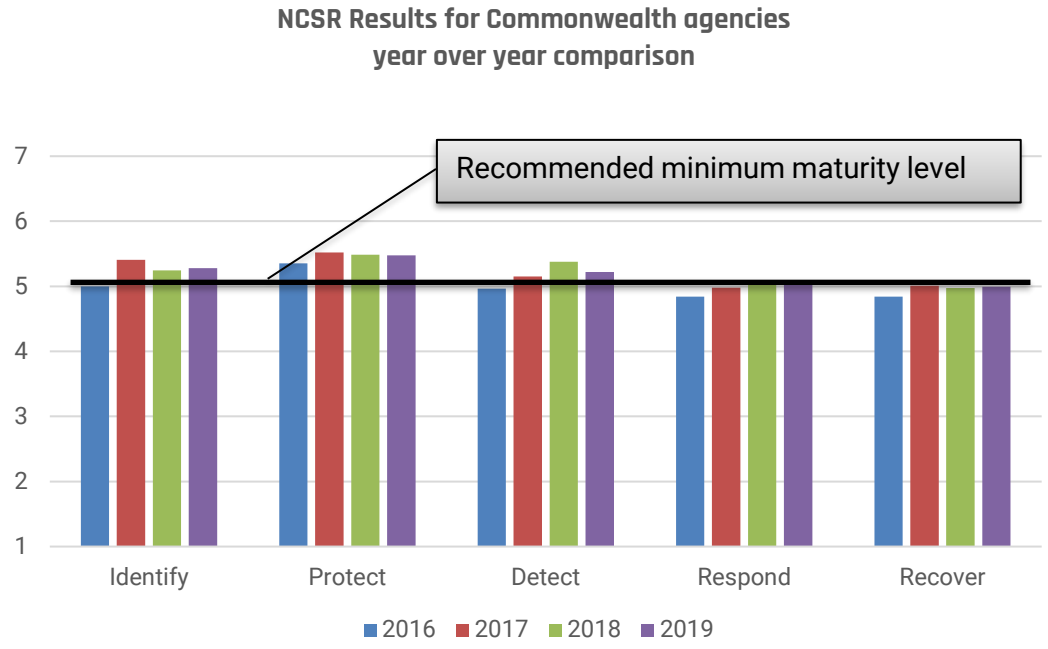
The five main functions surveyed in the NCSR are: *Identify, Protect, Detect, Respond* and *Recover*. Each function is subdivided into several categories:

- **Identify**: These activities are key for an organization's understanding of their internal culture, infrastructure and risk tolerance.
    - Categories: Asset management; business environment; governance; risk assessment; risk management strategy; and supply chain risk management.
- **Protect**: Activities under the protect function pertain to the methods that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services.
    - Categories: Access control; awareness & training; data security; information protection processes & procedures; maintenance; and protective technology.
- **Detect**: These activities identify an organization's ability to identify incidents so that they can be quickly remediated and reduce the consequences of the event.
    - Categories: Anomalies & events; security continuous monitoring; and detection processes.
- **Respond**: Responding quickly and appropriately to an incident greatly to reduces the consequences of an incident. These activities examine how an organization plans, analyzes, communicates, mitigates and improves its response capabilities.
    - Categories: Response planning; communications; mitigation; and improvements.
- **Recover**: These activities are key to an organization's ability to return to its baseline after an incident has occurred.
    - Categories: Recovery planning; improvements; and communications.

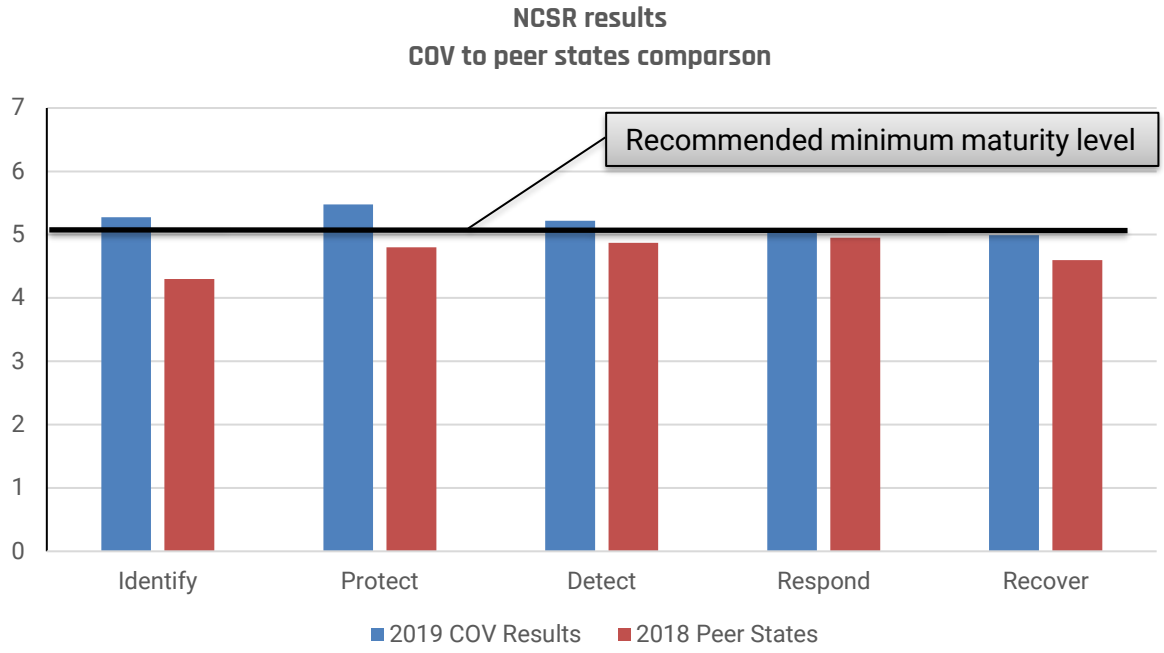
The number of Commonwealth agencies who participated in the survey increased from 65 agencies in 2018 to 70 agencies in 2019, an increase of 7%. The survey requires agencies to evaluate the maturity level of their processes and controls using the scoring described in the table below from the Nationwide Cyber Security Review.

Maturity Level		
Score	***The recommended minimum maturity level is set at a score of 5 and higher***	
7	**Optimized**	Your organization has formally documented policies, standards, and procedures. Implementation is test, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested & Verified**	Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process**	Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
5	**Risk Formally Accepted**	Your organization has chosen not to implement based on a risk assessment.
4	**Partially Documented Standards and/or Procedures**	Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy**	Your organization has a formal policy in place.
2	**Informally Performed**	Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed**	Activities, processes and technologies are not in place to achieve the referenced objective.

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 2019, 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.

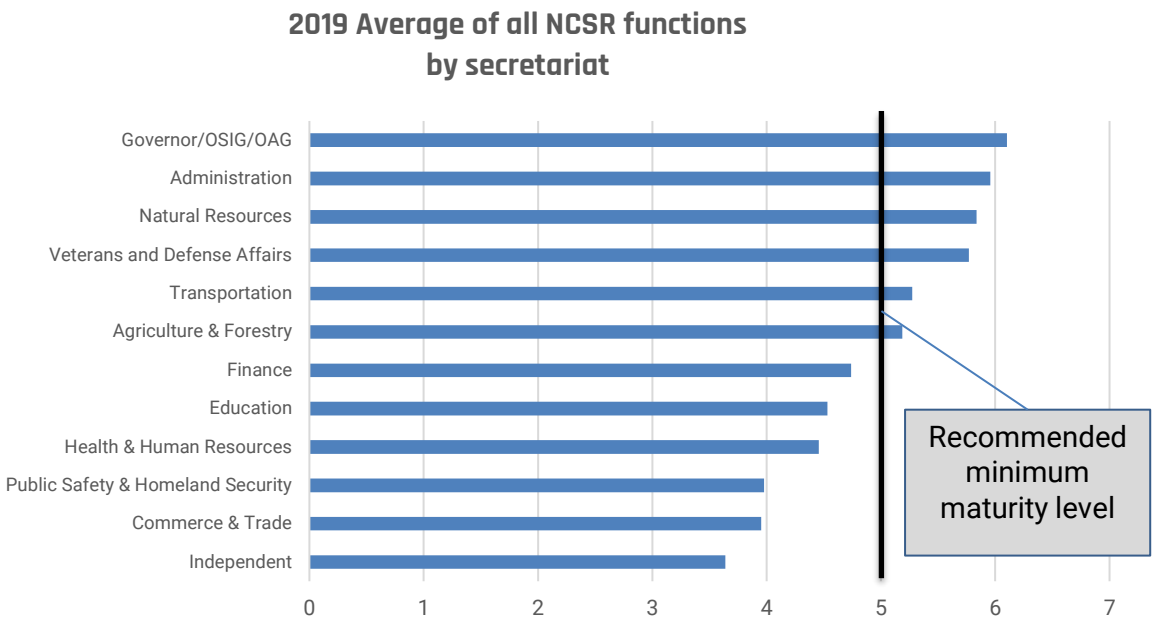


Commonwealth agencies compared favorably with their peers in other states.
The results demonstrate that Commonwealth agencies reported maturity levels slightly higher than the maturity level of peer state agencies that took part in the survey in 2018 for every function in the framework. The most significant difference is found in the identify function, where Commonwealth agencies reported they were 18% more mature than their peer agencies on average.



NCSR analysis by secretariat

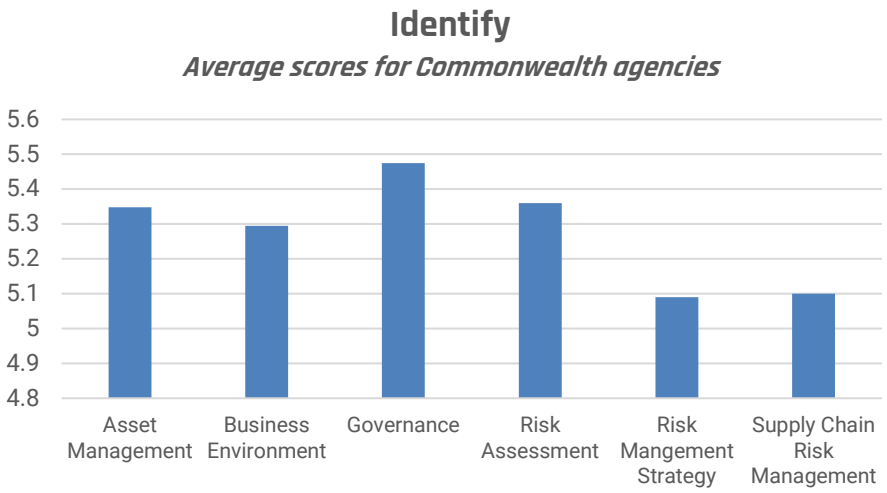
Analysis of all NCSR self-assessments by Commonwealth secretariat shows that five secretariats are performing at higher than the minimum recommended maturity level of five (implementation in process/risk formally accepted). Two of those secretariats are nearly at or above level six (tested and verified). Five secretariats are performing in the level four range (partially documented standards or procedures). Independent agencies are generally reporting that they are only in the level three range (documented policy).



Cybersecurity framework – analysis by function

Identify

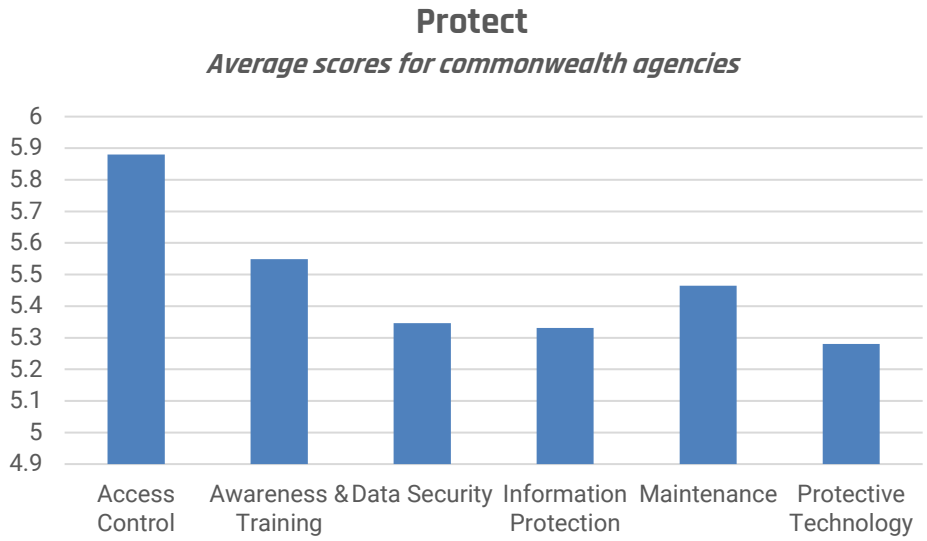
The activities under this functional area are key for an agency's understanding of their current internal culture, infrastructure and risk tolerance. This functional area tends to be one of the lowest-rated functions for many agencies. Immature capabilities in the identify function may hinder an agency's ability to effectively apply risk management principles for cybersecurity. By incorporating sound risk management principles into cybersecurity programs, agencies will be able to continuously align their efforts towards protecting their most valuable assets against the most relevant risks.



The category of "risk management strategy" was the least mature category within the identify function. This may indicate that additional resources to assist with formal risk management assessments could be beneficial to Commonwealth agencies.

Protect

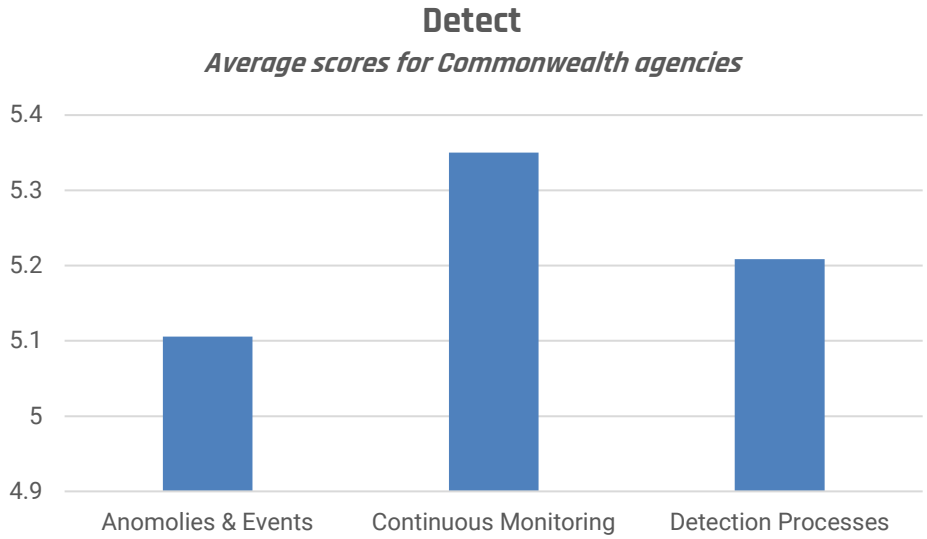
The activities under the protect function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services. These controls are focused on preventing cybersecurity events from occurring through common attack vectors, including attacks targeting users and attacks leveraging inherent weakness in applications and network communication.



"Protective technology" is the least mature category in the protect function. This refers to the technical security solutions that are used to manage the security and resilience of systems and assets and their consistency with related policies, procedures, and agreements. This indicates that agencies may need more information regarding technical security solutions and assistance in procuring the appropriate protective technologies.

Detect

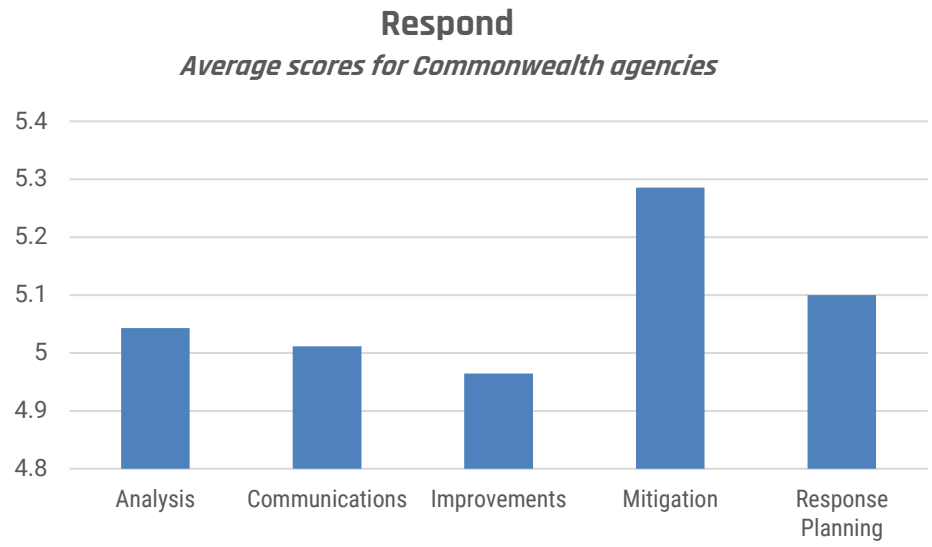
The quicker an agency is able to detect a cybersecurity incident, the better positioned it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the detect function pertain to an agency's ability to identify incidents. These controls are becoming more important as the quantity of logs and events occurring within an environment can be overwhelming to handle and can make it difficult to identify the key concerns.



Within the detect function, agencies scored the lowest in “anomalies and events.” This measures capabilities related to detecting anomalous activity and understanding the potential impact of events that are detected. We believe this could indicate that agencies need more resources to establish and understand a baseline of normal activity on their networks, in order to be able to identify anomalies.

Respond

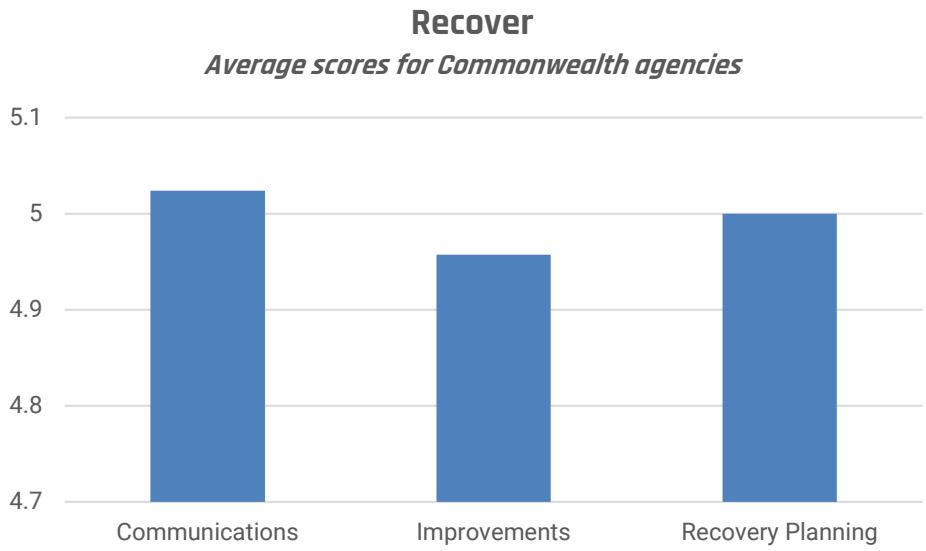
An agency’s ability to quickly and appropriately respond to an incident plays a large role in reducing the incident’s consequences. As such, the activities within the respond function examine how an agency plans, analyzes, communicates, mitigates and improves its response capabilities. For many agencies, integration and cooperation with other entities is key. Many Commonwealth agencies do not have the internal resources to handle all components of incident response. One example is the ability to conduct forensics after an incident, which helps agencies identify and remediate the original attack vector.



The “improvements” category is the lowest within the respond function. CSRM recommends that agencies allocate more time, develop policy to properly document, and analyze lessons learned following incidents and incident response exercises. Additionally, response strategies should be updated, if necessary, following incidents and exercises.

Recover

Activities within the recover function pertain to an agency’s ability to return to its baseline after an incident has occurred. Such controls are focused not only on activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their lifecycle.

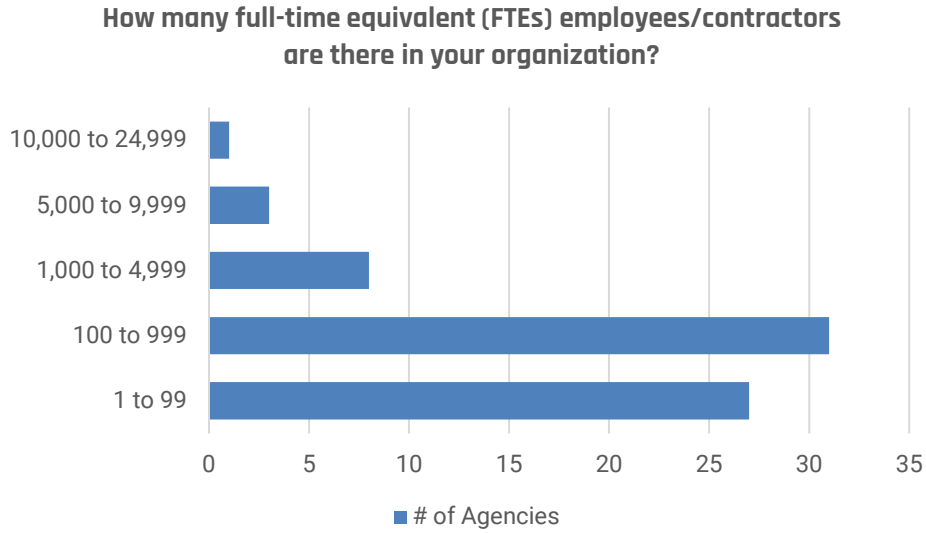


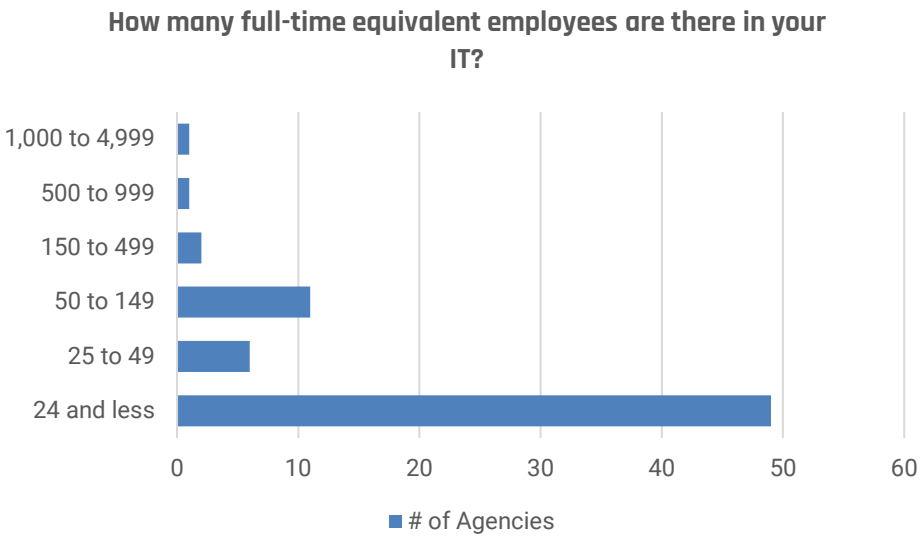
Within the recover function, “improvements” documents the maturity level of incorporating lessons learned from handling IT security incidents into improving recovery planning and processes. CSRM recognizes that agencies need assistance and training to develop and implement policies that regularly exercise and enhance incident response and business resiliency.

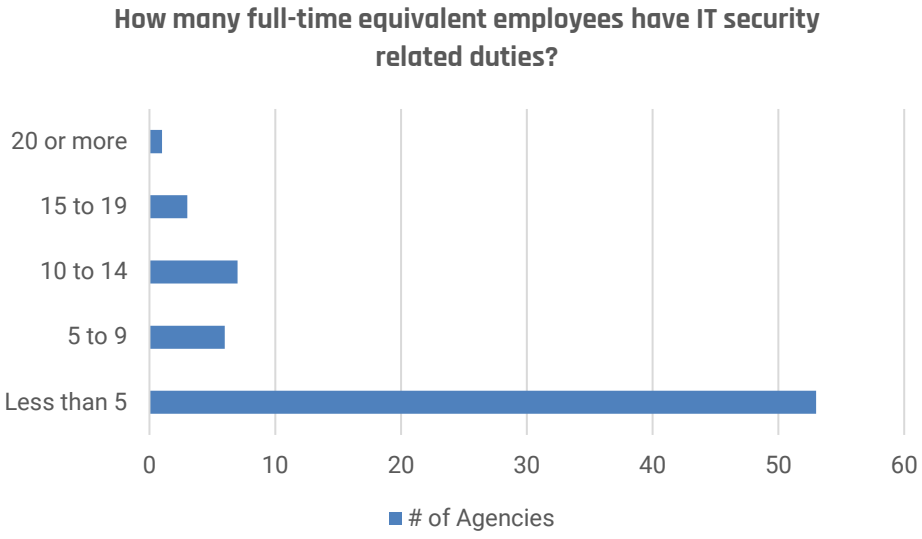
NCSR survey demographic analysis

Number of employees and contractors on staff

Commonwealth agencies were surveyed as to the number of full-time equivalent **(FTE)** personnel who were on staff.

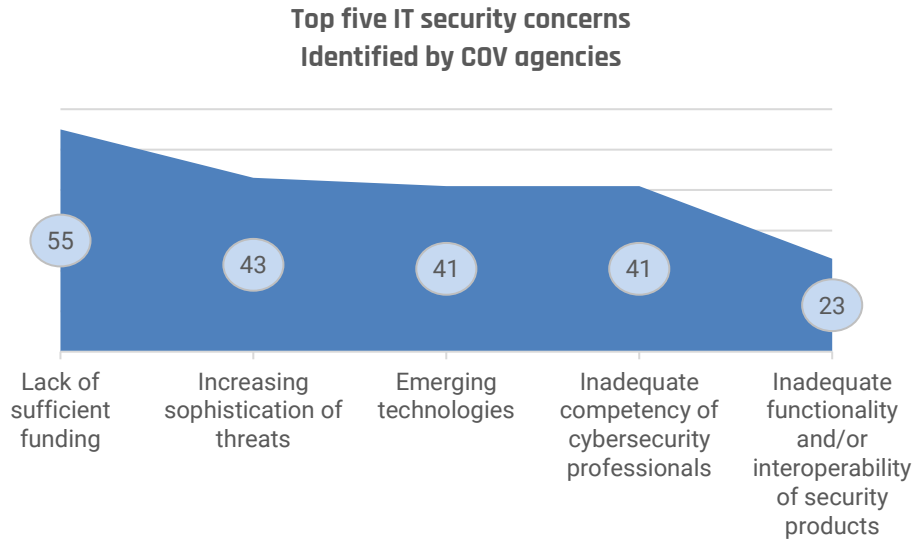



How many full-time equivalent employees are there in your IT?
1,000 to 4,999
500 to 999
150 to 499
50 to 149
25 to 49
24 and less
0
10
20
30
40
50
60
# of Agencies


How many full-time equivalent employees have IT security related duties?
20 or more
15 to 19
10 to 14
5 to 9
Less than 5
0
10
20
30
40
50
60
# of Agencies

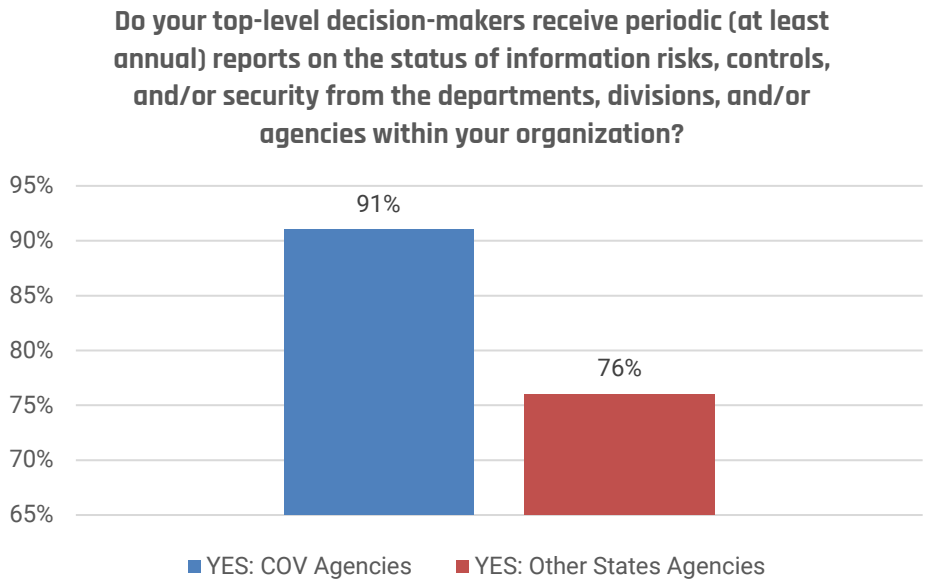
Top five security concerns

Commonwealth agencies participating in the NCSR survey were asked to identify their top five IT security concerns.



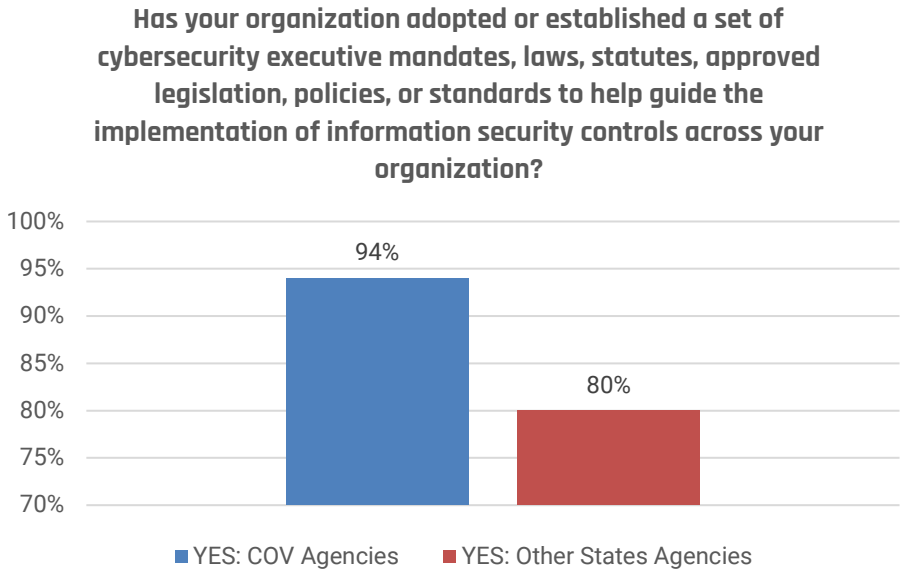
Agency top-level decision makers

According to the national NCSR survey, an average of 76% of top-level decision makers are receiving periodic IT security and risk management reports. In the COV, 91% of top-level decision makers are receiving these reports.



Adoption of established cybersecurity policies

Nationally, 80% of state agencies surveyed in the NCSR have adopted or established a set of cybersecurity mandates, laws, statutes, policies or standards. In the Commonwealth, 94% of the agencies indicate that they have adopted cybersecurity policies.



Summary of NCSR survey results

The 2019 Nationwide Cybersecurity Review (NCSR) provides insight on the level of maturity and risk awareness of Commonwealth agencies' information security programs from year to year. In addition, we are able to benchmark our survey results with the results from 43 peer states. Using the results of this report, CSRM works with individual agencies on improving their cybersecurity maturity.

Although Commonwealth agencies are self-reporting at a higher maturity level than our peers, there is still significant room for improvement. CSRM recommends additional training and an investment in more resources to assist agencies in managing and improving their overall IT security posture.

Appendix I –Agency compliance report card

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Administration	Audit, ISO	CB	Compensation Board	D	A
Administration	ISO	ELECT	Department of Elections	D	A
Administration		DGS	Department of General Services	B	A
Administration	Audit, ISO	DHRM	Department of Human Resource Management	A	A
Administration	ISO	VITA	Virginia Information Technologies Agency	A	C
Agriculture & Forestry	Audit, ISO	DOF	Department of Forestry	F	A
Agriculture & Forestry		VDACS	Virginia Department of Agriculture and Consumer Services	A	F
Agriculture & Forestry	Audit, ISO	VRC	Virginia Racing Commission	A	A
Commerce and Trade	Audit, ISO	BOA	Board of Accountancy	D	A
Commerce and Trade	Audit	DHCD	Department of Housing and Community Development	A	C
Commerce and Trade	Audit, ISO	DOLI	Department of Labor and Industry	A	A
Commerce and Trade	Audit, ISO	DMME	Department of Mines, Minerals and Energy	A	A
Commerce and Trade		DPOR	Department of Professional and Occupational Regulation	D	A
Commerce and Trade	Audit, ISO	SBSD	Department of Small Business and Supplier Diversity	A	A

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Commerce and Trade		TIC	Tobacco Region Revitalization Commission	B	F
Commerce and Trade		VEDP	Virginia Economic Development Partnership	F	F
Commerce and Trade		VEC	Virginia Employment Commission	A	A
Commerce and Trade		VRA	Virginia Resources Authority	F	F
Commerce and Trade		IEIA	Center for Innovative Technologies	D	A
Education	Audit	DOE	Department of Education	A	A
Education	ISO	FCMV	Frontier Culture Museum of Virginia	D	A
Education	ISO	GH	Gunston Hall	A	A
Education	Audit, ISO	JYF	Jamestown-Yorktown Foundation	B	B
Education		LVA	Library of Virginia	D	B
Education	Audit, ISO	NSU	Norfolk State University	C	F
Education		RBC	Richard Bland College	F	F
Education	ISO	SMV	Science Museum of Virginia	D	A
Education	ISO	SVHEC	Southern Virginia Higher Education Center	A	A
Education		SWVHEC	Southwest Virginia Higher Education Center	F	F

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Education	Audit, ISO	SCHEV	State Council of Higher Education for Virginia	F	A
Education		VCA	Virginia Commission for the Arts	F	F
Education	Audit	VMFA	Virginia Museum of Fine Arts	D	D
Education		VSDB	Virginia School for the Deaf and Blind	D	F
Education	Audit, ISO	VSU	Virginia State University	A	A
Executive		OAG	Office of Attorney General	F	F
Executive		OSIG	Office of State Inspector General	A	C
Executive	ISO	GOV	Office of the Governor	D	A
Finance	Audit	DOA	Department of Accounts	A	A
Finance	Audit, ISO	DPB	Department of Planning and Budget	A	A
Finance		TAX	Department of Taxation	A	D
Finance		TD	Department of Treasury	D	A
Health and Human Resources		DARS	Department for Aging and Rehabilitative Services	B	F
Health and Human Resources	Audit	DDHH	Department for the Deaf and Hard of Hearing	A	F
Health and Human Resources		DBHDS	Department of Behavioral Health and Development Services	C	F

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Health and Human Resources		DHP	Department of Health Professions	D	A
Health and Human Resources		DMAS	Department of Medical Assistance Services	A	B
Health and Human Resources		DSS	Department of Social Services	F	F
Health and Human Resources		CSA	Office for Children's Services	F	A
Health and Human Resources		VDH	Virginia Department of Health	D	A
Health and Human Resources		VFHY	Virginia Foundation for Healthy Youth	F	F
Independent	Audit, ISO	IDC	Indigent Defense Commission	D	A
Independent		SCC	State Corporation Commission	A	F
Independent		SLD	State Lottery Department	B	F
Independent		VCSP	Virginia College Savings Plan	A	C
Independent		VRS	Virginia Retirement System	A	B
Independent	Audit	VWC	Virginia Workers Compensation Commission	A	A
Independent		ABC	Alcoholic Beverage Control	B	C
Natural Resources	ISO	DCR	Department of Conservation and Recreation	A	A
Natural Resources	Audit, ISO	DEQ	Department of Environmental Quality	A	A

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Natural Resources	ISO	DGIF	Department of Game and Inland Fisheries	D	D
Natural Resources	Audit, ISO	DHR	Department of Historic Resources	D	A
Natural Resources	Audit	MRC	Marine Resources Commission	A	A
Natural Resources	Audit, ISO	VMNH	Virginia Museum of Natural History	A	A
Public Safety		CASC	Commonwealths Attorneys Services Council	A	A
Public Safety		DOC	Department of Corrections	D	C
Public Safety	Audit, ISO	DCJS	Department of Criminal Justice Services	A	A
Public Safety		DFP	Department of Fire Programs	F	F
Public Safety	Audit, ISO	DFS	Department of Forensic Science	A	A
Public Safety	ISO	DJJ	Department of Juvenile Justice	F	F
Public Safety		DMA	Department of Military Affairs	D	C
Public Safety		DVS	Department of Veterans Services	A	A
Public Safety		VDEM	Virginia Department of Emergency Management	F	F
Public Safety	Audit, ISO	VSP	Virginia State Police	F	D
Transportation		DOAV	Department of Aviation	A	A

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Transportation		DMV	Department of Motor Vehicles	B	B
Transportation	Audit	DRPT	Department of Rail and Public Transportation	A	A
Transportation	Audit, ISO	MVDB	Motor Vehicle Dealer Board	A	A
Transportation		VDOT	Virginia Department of Transportation	A	A

Appendix II - Agency information security data points

Agency information security data points detail - Legend

Audit plan status
Pass - Documents received as scheduled
N/C - Missing audit plan

Percentage of audit findings updates received
X% - The percentage of due findings updates received
N/A - Not applicable as the agency had no 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 assessments 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

Percentage of risk findings updates received
X% - The percentage of due risk findings updates received
N/A - Not applicable as the agency had no risk updates due

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

ISO report to Agency Head
Yes - Agency ISO reports to Agency Head
No - Agency ISO does not report directly to Agency

Agency Secretariat	Agency Acronym	Agency Name	ISO Centralized Services?	Audit Centralized Services	Audit Plan Status	Current year percentage of Audit findings updates received	3 Year Audit Obligation	Risk Assessment Plan Status	Three Year Risk Assessment Obligation	BIA Status	Current year percentage of Risk findings updates received	IDS Quarterly Reports	Data Set Inventory	ISO Certification Status	ISO Reports to Agency Head
Administration	CB	Compensation Board	Yes	Yes	Pass	N/A	0.00	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Administration	ELECT	Department of Elections	Yes	No	Pass	100%	0.00	Pass	100%	100%	100%	Pass	Compliant	Pass	No
Administration	DGS	Department of General Services	No	No	Pass	75%	0.94	Pass	94%	100%	N/A	Pass	Compliant	Pass	Yes
Administration	DHRM	Department of Human Resource Management	Yes	Yes	Pass	100%	0.84	Pass	100%	100%	24%	Pass	Compliant	Pass	Yes
Administration	VITA	Virginia Information Technologies Agency	Yes	No	Pass	100%	0.85	Pass	39%	100%	100%	Pass	Compliant	Pass	Yes
Agriculture & Forestry	DOF	Department of Forestry	Yes	Yes	Pass	55%	0.00	Pass	78%	100%	0%	Pass	Compliant	Pass	No
Agriculture & Forestry	VDACS	Virginia Department of Agriculture and Consumer Services	No	No	Pass	100%	1.00	N/C	N/C	100%	26%	Pass	Compliant	Pass	Yes
Agriculture & Forestry	VRC	Virginia Racing Commission	Yes	Yes	Pass	100%	0.75	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Commerce and Trade	BOA	Board of Accountancy	Yes	Yes	Pass	100%	0.00	Pass	100%	100%	N/A	Pass	Compliant	Pass	yes
Commerce and Trade	IEIA	Center for Innovative Technologies	No	No	Pass	0%	1.00	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Commerce and Trade	DHCD	Department of Housing and Community Development	No	Yes	Pass	100%	1.00	Pass	40%	100%	N/A	Pass	Compliant	Pass	No
Commerce and Trade	DOLI	Department of Labor and Industry	Yes	Yes	Pass	100%	1.00	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Commerce and Trade	DMME	Department of Mines, Minerals and Energy	Yes	Yes	Pass	100%	1.00	Pass	100%	100%	N/A	Pass	Compliant	Pass	Yes
Commerce and Trade	DPOR	Department of Professional and Occupational Regulation	Yes	No	Pass	N/A	0.00	Pass	100%	100%	100%	Pass	Compliant	Pass	No
Commerce and Trade	SBSD	Department of Small Business and Supplier Diversity	Yes	Yes	Pass	100%	1.00	Pass	100%	100%	N/A	Pass	Compliant	Pass	Yes
Commerce and Trade	TIC	Tobacco Region Revitalization Commission	No	No	Pass	50%	1.00	N/C	N/C	100%	N/A	Fail	Compliant	N/C	No
Commerce and Trade	VEDP	Virginia Economic Development Partnership	No	No	N/C	N/A	N/C	N/C	N/C	N/C	N/A	Fail	Compliant	N/C	No
Commerce and Trade	VEC	Virginia Employment Commission	No	No	Pass	96%	89%	Pass	100%	100%	97%	Pass	Compliant	Pass	Yes
Commerce and Trade	VRA	Virginia Resources Authority	No	No	N/C	N/A	N/C	N/C	N/C	N/C	N/A	Fail	Compliant	N/C	No
Education	DOE	Department of Education	No	Yes	Pass	94%	1.00	Pass	100%	100%	79%	Pass	Compliant	N/C	Yes
Education	FCMV	Frontier Culture Museum of Virginia	Yes	No	Pass	N/A	0.00	Pass	100%	100%	N/A	Pass	Compliant	Pass	Yes
Education	GH	Gunston Hall	Yes	No	Pass	N/A	N/A	Pass	100%	100%	N/A	Pass	Compliant	Pass	Yes
Education	JYF	Jamestown-Yorktown Foundation	Yes	Yes	Pass	N/A	0.50	Pass	58%	100%	100%	Pass	Compliant	Pass	No
Education	LVA	Library of Virginia	No	No	Pass	N/A	0.00	Pass	64%	100%	N/A	Pass	Compliant	Pass	Yes
Education	NSU	Norfolk State University	Yes	Yes	Pass	N/A	0.24	Pass	0%	100%	N/A	Fail	Compliant	Pass	yes

Agency Secretariat	Agency Acronym	Agency Name	ISO Centralized Services?	Audit Centralized Services	Audit Plan Status	Current year percentage of Audit findings updates received	3 Year Audit Obligation	Risk Assessment Plan Status	Three Year Risk Assessment Obligation	BIA Status	Current year percentage of Risk findings updates received	IDS Quarterly Reports	Data Set Inventory	ISO Certification Status	ISO Reports to Agency Head
Education	RBC	Richard Bland College	No	No	Pass	15%	0.64	N/C	N/C	100%	N/A	Fail	Compliant	N/C	No
Education	SMV	Science Museum of Virginia	Yes	No	Pass	N/A	0.00	Pass	86%	100%	N/A	Pass	Compliant	Pass	Yes
Education	SVHEC	Southern Virginia Higher Education Center	Yes	No	Pass	N/A	N/A	Pass	N/A	100%	N/A	Incomplete	Compliant	Pass	No
Education	SWVHEC	Southwest Virginia Higher Education Center	No	No	N/C	N/A	N/C	N/C	N/C	0%	N/A	Fail	Compliant	Pass	No
Education	SCHEV	State Council of Higher Education for Virginia	Yes	Yes	Pass	0%	0.75	Pass	100%	100%	0%	Pass	Compliant	Pass	Yes
Education	VCA	Virginia Commission for the Arts	No	No	N/C	N/A	N/C	N/C	N/C	100%	N/A	Pass	Compliant	N/C	Yes
Education	VMFA	Virginia Museum of Fine Arts	No	Yes	Pass	100%	0.00	Pass	0%	100%	N/A	Pass	Compliant	Pass	Yes
Education	VSDB	Virginia School for the Deaf and Blind	No	No	Pass	N/A	0.00	N/C	N/C	100%	N/A	Fail	Compliant	N/C	yes
Education	VSU	Virginia State University	Yes	Yes	Pass	100%	0.75	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Executive	OAG	Office of Attorney General	Yes	No	N/C	56%	N/C	Pass	0%	50%	N/A	Fail	Non-Compliant	Pass	No
Executive	OSIG	Office of State Inspector General	No	No	Pass	N/A	1.00	Pass	40%	100%	N/A	Pass	Compliant	Pass	No
Executive	GOV	Office of the Governor	Yes	No	Pass	N/A	0.00	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Finance	DOA	Department of Accounts	No	Yes	Pass	N/A	1.00	Pass	100%	100%	N/A	Pass	Compliant	Pass	yes
Finance	DPB	Department of Planning and Budget	Yes	Yes	Pass	100%	1.00	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Finance	TAX	Department of Taxation	No	No	Pass	100%	0.82	Pass	0%	100%	13%	Pass	Compliant	Pass	Yes
Finance	TD	Department of Treasury	No	No	Pass	3%	0.79	Pass	86%	100%	0%	Pass	Compliant	Pass	Yes
Health and Human Resources	DARS	Department for Aging and Rehabilitative Services	No	No	Pass	56%	1.00	N/C	N/C	6%	0%	Pass	Compliant	Pass	Yes
Health and Human Resources	DDHH	Department for the Deaf and Hard of Hearing	No	Yes	Pass	78%	1.00	N/C	N/C	38%	0%	Pass	Compliant	Pass	Yes
Health and Human Resources	DBHDS	Department of Behavioral Health and Development Services	No	No	Pass	30%	0.82	N/C	69%	N/C	N/A	Pass	Compliant	N/C	No
Health and Human Resources	DHP	Department of Health Professions	Yes	Yes	Pass	N/A	0.00	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Health and Human Resources	DMAS	Department of Medical Assistance Services	No	No	Pass	97%	0.93	Pass	92%	100%	69%	Pass	Partial	Pass	Yes
Health and Human Resources	DSS	Department of Social Services	No	No	Pass	0%	0.68	Pass	70%	N/C	0%	Pass	Partial	Pass	No
Health and Human Resources	CSA	Office for Children's Services	No	Yes	Pass	0%	0.00	Pass	100%	100%	0%	Pass	Compliant	Pass	Yes
Health and Human Resources	VDH	Virginia Department of Health	No	No	Pass	24%	0.64	Pass	100%	100%	80%	Pass	Compliant	Pass	no
Health and Human Resources	VFHY	Virginia Foundation for Healthy Youth	No	No	N/C	N/A	N/C	N/C	N/C	50%	N/A	Fail	Compliant	Pass	no
Independent	ABC	Alcoholic Beverage Control	No	No	Pass	100%	0.61	Pass	0%	100%	N/A	Fail	Compliant	Pass	No
Independent	IDC	Indigent Defense Commission	Yes	Yes	Pass	N/A	0.00	Pass	100%	100%	29%	Fail	Compliant	Pass	No

Agency Secretariat	Agency Acronym	Agency Name	ISO Centralized Services?	Audit Centralized Services	Audit Plan Status	Current year percentage of Audit findings updates received	3 Year Audit Obligation	Risk Assessment Plan Status	Three Year Risk Assessment Obligation	BIA Status	Current year percentage of Risk findings updates received	IDS Quarterly Reports	Data Set Inventory	ISO Certification Status	ISO Reports to Agency Head
Independent	SCC	State Corporation Commission	No	No	Pass	100%	0.89	Pass	0%	100%	N/A	Fail	Non-Compliant	Pass	Yes
Independent	SLD	State Lottery Department	No	No	Pass	100%	0.68	N/C	N/C	100%	N/A	Fail	Compliant	Pass	No
Independent	VCSP	Virginia College Savings Plan	No	No	Pass	100%	1.00	Pass	100%	100%	N/A	Fail	Non-Compliant	Pass	Yes
Independent	VRS	Virginia Retirement System	No	No	Pass	100%	1.00	Pass	100%	100%	60%	Pass	Non-Compliant	Pass	No
Independent	VWC	Virginia Workers Compensation Commission	No	Yes	Pass	N/A	1.00	Pass	100%	100%	N/A	Fail	Compliant	Pass	Yes
Natural Resources	DCR	Department of Conservation and Recreation	Yes	No	Pass	100%	1.00	Pass	100%	100%	100%	Pass	Compliant	Pass	No
Natural Resources	DEQ	Department of Environmental Quality	Yes	Yes	Pass	100%	0.90	Pass	80%	100%	100%	Pass	Compliant	Pass	Yes
Natural Resources	DGIF	Department of Game and Inland Fisheries	Yes	No	Pass	N/A	N/C	Pass	0%	100%	N/A	Pass	Compliant	Pass	No
Natural Resources	DHR	Department of Historic Resources	Yes	Yes	Pass	100%	0.00	Pass	100%	100%	0%	Pass	Compliant	Pass	Yes
Natural Resources	MRC	Marine Resources Commission	No	Yes	Pass	100%	1.00	Pass	100%	100%	N/A	Pass	Compliant	Pass	Yes
Natural Resources	VMNH	Virginia Museum of Natural History	Yes	Yes	Pass	100%	1.00	Pass	100%	100%	25%	Pass	Compliant	Pass	Yes
Public Safety	CASC	Commonwealths Attorneys Services Council	No	No	Pass	N/A	N/A	Pass	N/A	100%	N/A	Fail	Compliant	Pass	no
Public Safety	DOC	Department of Corrections	No	No	Pass	41%	0.39	Pass	77%	2%	N/A	Pass	Compliant	Pass	No
Public Safety	DCJS	Department of Criminal Justice Services	Yes	Yes	Pass	N/A	1.00	Pass	100%	100%	100%	Pass	Compliant	Pass	No
Public Safety	DFP	Department of Fire Programs	No	No	N/C	0%	N/C	Pass	1%	5%	N/A	Pass	Compliant	Pass	No
Public Safety	DFS	Department of Forensic Science	No	Yes	Pass	N/A	1.00	Pass	100%	100%	50%	Pass	Compliant	Pass	No
Public Safety	DJJ	Department of Juvenile Justice	Yes	No	Pass	25%	0.00	Pass	0%	N/C	N/A	Pass	Compliant	Pass	yes
Public Safety	DMA	Department of Military Affairs	No	No	Pass	N/A	0.00	Pass	N/A	20%	N/A	Fail	Compliant	Pass	No
Public Safety	DVS	Department of Veterans Services	No	No	Pass	100%	1.00	Pass	100%	100%	N/A	Pass	Compliant	Pass	Yes
Public Safety	VDEM	Virginia Department of Emergency Management	No	No	N/C	N/A	N/C	N/C	N/C	N/C	N/A	Pass	Compliant	Pass	No
Public Safety	VSP	Virginia State Police	Yes	Yes	Pass	43%	0.02	Pass	0%	100%	N/A	Pass	Compliant	Pass	No
Transportation	DOAV	Department of Aviation	No	No	Pass	100%	1.00	Pass	100%	100%	100%	Pass	Compliant	Pass	yes
Transportation	DMV	Department of Motor Vehicles	No	No	Pass	96%	0.56	Pass	45%	100%	N/A	Pass	Compliant	Pass	Yes
Transportation	DRPT	Department of Rail and Public Transportation	No	Yes	Pass	100%	1.00	Pass	100%	100%	100%	Pass	Compliant	Pass	No
Transportation	MVDB	Motor Vehicle Dealer Board	Yes	Yes	Pass	100%	1.00	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes
Transportation	VDOT	Virginia Department of Transportation	No	No	Pass	100%	0.89	Pass	81%	100%	N/A	Pass	Compliant	Pass	No

Appendix III - Cybersecurity framework results - Detail

National Cybersecurity 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	Identify	Protect	Detect	Respond	Recover	Average
Alcoholic Beverage Control	2.32	2.34	1.93	2.07	1.94	2.12
Board of Accountancy	5.74	5.85	5.74	5.48	6	5.762
Center for Innovative Technologies	4.85	5.29	4.13	2.39	2.67	3.866
Commonwealths Attorneys Services Council	6.7	6.8	7	7	7	6.9
Compensation Board	6	5.97	5.96	6	6	5.986
Department for Aging and Rehabilitative Services	4.74	6.07	5.77	5.92	5.89	5.678
Department for the Deaf and Hard of Hearing	5.04	6.08	6	5.96	5.56	5.728
Department of Accounts	6.67	6.73	6.11	7	5.67	6.436
Department of Aviation	6.87	7	7	7	7	6.974
Department of Behavioral Health and Development Services	2.79	3.11	2.93	2.76	2.67	2.852
Department of Conservation and Recreation	6.89	6.75	7	6.6	7	6.848
Department of Corrections	4.08	4.5	4.64	4.08	5.11	4.482
Department of Criminal Justice Services	2.19	3.09	4.03	2.55	1.22	2.616
Department of Education	4.22	4.75	3.64	1.8	1.67	3.216
Department of Elections	6	6	6	6	6	6
Department of Environmental Quality	5.62	4.98	3.25	4.65	3.56	4.412
Department of Fire Programs	2.52	3.6	1.93	2	2	2.41
Department of Forensic Science	5	4.51	5	5	5	4.902
Department of Forestry	6	4.7	2.8	2.2	2	3.54
Department of Game and Inland Fisheries	5.8	5.5	5.93	4.79	5.78	5.56
Department of General Services	6	5.99	5.27	5.47	5.11	5.568
Department of Health Professions	6	6	6	5.96	6	5.992
Department of Historic Resources	7	6.93	7	7	7	6.986
Department of Housing and Community Development	4.07	5.3	3.06	3.1	3.22	3.75
Department of Human Resource Management	5.88	5.89	5.85	5.86	6	5.896
Department of Juvenile Justice	2.1	2.82	3	2.4	2	2.464

Agency	Identify	Protect	Detect	Respond	Recover	Average
Department of Labor and Industry	6	5.99	6	6	6	5.998
Department of Medical Assistance Services	5.86	5.78	5.66	5.8	5.22	5.664
Department of Military Affairs	5.93	6.62	6.83	6.58	5.94	6.38
Department of Mines, Minerals and Energy	5.15	5.82	4.67	5.12	5.67	5.286
Department of Motor Vehicles	6.46	6.39	6.33	6.48	6.83	6.498
Department of Planning and Budget	5.93	5.97	5.96	5.92	6	5.956
Department of Professional and Occupational Regulation	6	6	6	6	6	6
Department of Rail and Public Transportation	7	7	7	7	7	7
Department of Small Business and Supplier Diversity	5.93	5.97	6	6	6	5.98
Department of Social Services	4.66	4.38	4.68	5.57	3.78	4.614
Department of Taxation	3.35	3.68	3.75	4.81	5	4.118
Department of Treasury	6.26	6.31	6.37	6	5.89	6.166
Department of Veterans Services	4.5	5.85	6.47	4.64	4.33	5.158
Frontier Culture Museum of Virginia	2.37	2.6	1.45	1.73	2.56	2.142
Gunston Hall	5.9	5.92	5.96	5.76	6	5.908
Indigent Defense Commission	6	5.94	5.93	5.86	5.83	5.912
Jamestown-Yorktown Foundation	5.92	6.74	3.28	6.15	4.89	5.396
Library of Virginia	6	6.21	5.71	5.77	6.06	5.95
Marine Resources Commission	5.05	5.56	5.67	5.48	5.11	5.374
Motor Vehicle Dealer Board	2.74	2.99	2.17	1.4	2	2.26
Norfolk State University	3.71	4.32	3.37	1.64	1.78	2.964
Office for Children's Services	5.2	5.69	5.42	5.55	5.17	5.406
Office of Attorney General	5.85	5.86	6	5.96	6	5.934
Office of State Inspector General	7	6.93	5.77	5.68	7	6.476
Office of the Governor	5.96	5.91	5.89	5.72	6	5.896
Richard Bland College	0	0	0	0	0	0
Science Museum of Virginia	5.74	5.89	6	6	6	5.926
Southern Virginia Higher Education Center	6	5.92	6	6	6	5.984
Southwest Virginia Higher Education Center	5.71	5.86	6	5.96	6	5.906
State Corporation Commission	0	0	0	0	0	0
State Council of Higher Education for Virginia	5.25	5.8	7	5	5	5.61
State Lottery Department	2.9	4.18	3.79	4.2	4.67	3.948
Tobacco Region Revitalization Commission	0	0	0	0	0	0
Virginia College Savings Plan	0	0	0	0	0	0
Virginia Commission for the Arts	0	0	0	0	0	0
Virginia Department of Agriculture and Consumer Services	6.74	6.54	6.89	7	6.11	6.656
Virginia Department of Emergency Management	2.79	2.51	2.71	1.96	2.17	2.428
Virginia Department of Health	5.58	5.28	5.5	3.56	1	4.184
Virginia Department of Transportation	3.96	4.04	3.93	2.96	3.33	3.644

Agency	Identify	Protect	Detect	Respond	Recover	Average
Virginia Economic Development Partnership	0	0	0	0	0	0
Virginia Employment Commission	5.34	5.22	5.5	4.38	3	4.688
Virginia Foundation for Healthy Youth	0	0	0	0	0	0
Virginia Information Technologies Agency	6.3	6.11	6.24	6.83	6.17	6.33
Virginia Museum of Fine Arts	7	7	7	7	7	7
Virginia Museum of Natural History	4.79	5.9	6	6	6	5.738
Virginia Racing Commission	5.42	5.63	5.45	5.33	5	5.366
Virginia Resources Authority	0	0	0	0	0	0
Virginia Retirement System	6.83	7	7	6.6	7	6.886
Virginia School for the Deaf and Blind	4	4	4	4	4	4
Virginia State Police	5.85	5.97	4.12	5.84	6.33	5.622
Virginia State University	6.73	6.59	6.83	6.8	7	6.79
Virginia Workers Compensation Commission	6.69	6.83	6.24	6.58	6.67	6.602