2021
COMMONWEALTH OF VIRGINIA
INFORMATION SECURITY REPORT

Commonwealth Security and Risk Management

Connecting – Protecting - Innovating

Comments on the
2021 Commonwealth of Virginia Information Security Report are welcome.
Suggestions may be conveyed electronically to CommonwealthSecurity@vita.virginia.gov

Please submit written correspondence to:

Chief Information Officer of the Commonwealth
Virginia Information Technologies Agency
Boulders VII
7325 Beaufont Springs Drive
Richmond, Va. 23225

cio@vita.virginia.gov

Prepared and published by:

Virginia Information Technologies Agency

Table of Contents

Executive Summary

This 2021 Commonwealth of Virginia (COV) Information Security Report is the 12th 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 shall annually report to the Governor, the Secretary, and General Assembly on 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.*"

In addition, this report includes the requirements directed by § 2.2-2009(C) of the Code of Virginia, which says, "*The CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on any breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures. Upon completion of the annual review, the CIO shall issue a report of his findings to the Chairman of the House Committee on Appropriations and the Senate Committee on Finance. Such report shall not contain technical information deemed by the CIO to be security sensitive or information that would expose security vulnerabilities*."

This report combines the requirements of § 2.2-2009(B)(1) and § 2.2-2009(C) into a single report.

The scope of this report is limited to the executive branch agencies, six independent agencies, and three Level I institutions of higher education. This report does not address the judicial branch, the legislative branch, and Level II and Level III higher education institutions, which are either statutorily exempted from compliance with Commonwealth policies and standards or outside the scope of VITA's compliance review.

The CIO has established a Commonwealth security and risk management (CSRM) group within the Virginia Information Technologies Agency (VITA) to fulfill statutory 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 utilizes a series of compliance metrics established by CSRM to assess the strength of the agency information technology (IT) security programs that protect Commonwealth data and systems. A listing of the agencies in scope to this report and their security, compliance, and cybersecurity assessment metrics are in the appendices of this document.

Commonwealth Threat Management Program

Information security incidents were largely due to the end user. In 2021, information disclosure incidents rose to first place as the largest category of incidents, with physical theft and loss in a close second. Cyber attackers have determined that the easiest target is the employee. 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.

Cybersecurity Awareness Training is key. To protect COV systems and data, more emphasis needs to be given to security awareness training of employees. While training is required for all users training at least once a year, it is not sufficient to protect users against attack. Phishing is used by hackers to target users and can be highly successful if the user is not adequately trained to identify a potential attack and how to respond to it. To provide more realistic training, CSRM purchased a tool that simulates a phishing attack. In the event an employee clicks a link or provides a login credential, the tool denotes the event, and the employee is required to complete additional training.

CSRM hosted the annual Commonwealth cybersecurity preparedness exercise. The goal of this event was to test the awareness, effectiveness, and efficiency of agencies and service provider's incident response tools and processes. The exercise concentrated on the various aspects of planning and executing the response to an incident and on the lessons learned from various scenarios. CSRM saw significant improvement in this year's exercise from the previous year, and we look forward to continuing to build on the success of this exercise to improve the Commonwealth's ability to respond to IT security incidents.

Attack attempts on the Commonwealth spiked in 2021. During 2021, over 33 million attack attempts (see Figure 5) were detected against Commonwealth systems. This is a rate of 1.05 attacks every second. The spikes in attempted attacks are indicative of new types of attack traffic being observed. Fortunately, the vast majority of attacks are blocked and prevented by Commonwealth monitoring systems and security tools.

Ransomware attacks continue to be a threat to the Commonwealth. CSRM threat management works with the Multi-State Information Sharing & Analysis Center (MS-ISAC) to share threat information with Commonwealth agencies and Higher Education Institutions. Based on the analysis of data from the MS-ISAC, higher education comprised 10% of all security investigations and cost those institutions $3.56 billion in downtime nationwide. During 2021, some of our state agencies experienced newsworthy ransomware attacks. In addition, third-party ransomware attacks that target suppliers or software managed by outside entities are a concern for all Commonwealth agencies.

Data breach costs rose significantly. In 2021, an international security consulting firm estimated that the average cost per incident for the public sector rose from $1.08M to $1.93M. This is a 78% increase in cost over 2020. A key factor that plays into the cost of a data breach is the life cycle of the cyber incident. The longer the incident life cycle, the larger the cost to the organization. A second contributor to the cost of data breaches is regulatory compliance failures, such as loss of data or neglecting to follow required security controls or policies. Compliance failures can lead to additional fines and penalties, adding to the overall cost. CSRM utilized this information to estimate that the cost of response and recovery efforts for all major and minor incidents and investigations in the Commonwealth was over $11 million in 2021.

CSRM provided IT security support for elections in the Commonwealth. In an ongoing effort to ensure safe and secure elections, CSRM performed a comprehensive security review of all systems and infrastructure supporting Virginia elections. In addition, CSRM provided monitoring of local county and city policies and procedures. Over the past 10 years, CSRM has established a cybersecurity command center for every major state or federal election to allow handling of any issues that occur during the election process. CSRM will continue to collaborate with the Department of Elections to provide support for upcoming elections.

Commonwealth Information Security Governance Program

CSRM ensures Commonwealth agencies develop and maintain their information security program. CSRM's information security governance program is responsible for monitoring performance and compliance against the Commonwealth's IT security policies, standards, and guidelines for the executive and independent branch agencies. The program provides support to agencies during their work to foster a mature IT security environment, while promoting information security training and awareness. Annually agencies receive a letter grade based on their overall compliance with our governance metrics.

CSRM's governance program also facilitates monthly opportunities for information security professionals. Monthly meetings are provided for Commonwealth security personnel to receive training, enterprise updates, and networking through the Information Security Officer Advisory Group (ISOAG). Additionally, the information security officers (ISO) Council was formed to recommend strategic direction for information security and privacy initiatives in the Commonwealth. CSRM has also formed a Risk Management Committee made up of risk specialists from CSRM's IT Risk Management division and information security officers from other Commonwealth agencies. The committee meets monthly to discuss approaches to addressing risks and issues identified as significant. The Risk Management determines the prioritization of risk mitigation and provides feedback on the current approaches to maintain established risk thresholds.

VITA CSRM integrates third-party risk management in the COV risk management program. As part of the VITA governance program, CSRM has developed and implemented methodologies for monitoring and managing risks associated with third-party service providers. The amount of risk introduced by third parties is quantified to ensure the Commonwealth maintains established risk thresholds. Within the multi-sourcing service integration (MSI) model that VITA has adopted, CSRM plays an integral role in identifying cybersecurity risks and tracking them until they are resolved. In addition, VITA's Enterprise Cloud Oversight Service (ECOS) reviews and approves contract terms and provides oversight of third-party vendors offering Software as a Service (SaaS) applications.

Continuing to refine the quantitative cyber risk analysis model that was implemented in 2020. The CSRM risk management team developed a methodology to estimate financial costs associated with the detection, response, and

recovery activities associated with cybersecurity incidents. Quantifying cybersecurity incidents from a financial perspective helped the Department of Treasury determine how much cyber liability insurance is needed in the event a system is breached or incapacitated. In addition, it allows executive leadership to make better and more informed decisions related to their agency's IT assets. Using this methodology also helps CSRM to prioritize security decisions based on quantifiable risk.

Commonwealth IT Audit and Risk Management Program

IT audit and risk assessment issues are tracked and monitored. Each issue indicates a gap or deficiency of an IT security control. When identified, CSRM ensures the agency has a reasonable corrective action plan to address the deficiency. If a corrective action plan is found to be inadequate, CSRM will work with the agency to address the deficiency and, if necessary, discuss with the risk management committee. Across all agencies, the most frequently identified area with inadequate security controls (19% of all reported issues) is "access control." Poor access controls increase the risk agencies are exposed to unauthorized access of data, fraud, or disruption of IT services.

Audit program compliance grades declined significantly in 2021. Audit program compliance decreased 16% from the prior year, with only 31% of agencies receiving a score of "A" in 2021 compared to the previous year when 47% of all agencies received an "A". This decrease is mainly attributed to the extraordinary demands of the pandemic resulting in reduced performance of normal IT security audits on sensitive systems. CSRM expects that more attention will be focused on auditing sensitive systems now that normal agency operations have resumed.

Risk program compliance grades declined slightly in 2021. Risk management compliance experienced a slight 2% downturn during 2021. In 2021, an "A" score was achieved by 27% of agencies compared to 29% receiving an "A" in 2020. CSRM recommends agencies place more emphasis on implementing comprehensive risk management programs by providing additional attention to risk assessments and dedicating the necessary resources to their IT risk management programs.

Agencies need to improve the timeliness of remediating audit and risk findings. CSRM analysis found that the average number of days to remediate a finding (*i.e.*, a security issue) is excessive. Audit findings average 495 days to close, and findings from risk assessments averaged 382 days. This is a slight improvement of about 5% over the previous year. CSRM notifies agencies of outstanding and overdue findings to further encourage agencies to remediate critical findings quickly. Agencies that are consistently and significantly behind in remediating findings are subject to formal notifications and restrictions in their ability to procure future IT services.

Commonwealth Centralized Security Services

Centralized services continue to address agency audit and risk management needs. VITA offers a centralized service to help Commonwealth agencies meet the requirements for IT system auditing, risk management (called ISO services), and vulnerability scanning. Use of audit and ISO services has helped agencies that lack dedicated resources to comply with the Commonwealth IT security requirements. Agencies using VITA's centralized services scored an entire letter grade higher on average than agencies that are not utilizing the centralized services. This most likely can be attributed to the additional attention to compliance that is provided by the centralized services.

Centralized vulnerability scanning identifies vulnerabilities before they can be exploited. The web application vulnerability scanning program provides automated scans of Commonwealth websites to identify potential security weaknesses. These scans are used to identify and mitigate vulnerabilities to prevent attacks. CSRM performed over 6,000 scans of public sites and private websites. In addition, CSRM's vulnerability scanning service has helped to reduce the number and impact of vulnerabilities (see Figure 24).

Nationwide Cyber Security Review

The Commonwealth participated in the Nationwide Cybersecurity Review (NCSR). The NCSR is a self-assessment survey aligned with the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF). The survey allows CSRM to review how agencies evaluate their own cybersecurity posture and to compare results with other

Commonwealth agencies and with those from other states. The most current NCSR survey results indicated Commonwealth agencies have an average score (on a scale of 1 to 7) that is slightly better than the national average and that has improved over the prior year.

The Cyber Security Framework was utilized as a methodology to assess and measure security outcomes. The Cyber Security Framework is built on five key security functions that are divided into 23 categories. Each category is further divided into many sub-categories. Agencies were asked questions on how it views cybersecurity risks and the outcomes it has obtained. These answers help CSRM establish a security baseline where steps can be defined to achieve optimal results. Overall, the 2021 NCSR showed that Commonwealth agencies generally report functioning at slightly higher than the minimum recommended level of "implementation in process" and consistent with the 2020 NCSR scores.

Commonwealth secretariats are showing overall improvement. Overall, the average NCSR score for Commonwealth agencies in 2021 was a 5.15 which is slightly above the minimum recommended level of five (5, implementation in process). When scores were consolidated by Commonwealth secretariats, it showed that eleven secretariats rated themselves higher than the minimum recommended level of five. Only two secretariats reported survey results that were slightly less that the recommended minimum score.

Key Takeaways

- Cyber attacks against Commonwealth targets continued to escalate in calendar year 2021. Commonwealth security detected over 33 million cyber attacks – approximately 1 attack every second.

- Ransomware attacks were a continuing threat to the government agencies in 2021. The Commonwealth experienced one ransomware attack that severely impacted an agency in the legislative branch. Another ransomware attack impacted a private company that provides cloud-based timekeeping software used by some agencies. The incident was quickly mitigated, and no Commonwealth data was compromised.

- Information security incidents were largely due to the end user. Cyber criminals know that users are generally the weakest link and most easily exploited through social engineering tactics. Security training and preparedness exercises are essential tools for educating users in how to identify potential social engineering attacks and taking the proper responses.

- Commonwealth security (CSRM) monitors and scores each in-scope agency's overall compliance with information security standards and policies. In 2021, that was a slight decline in agency compliance scores over the previous year.

- IT security issues and vulnerabilities identified by audits, risk assessments, and security scanning tools are not mitigated in a timely manner by many agencies. Failure to mitigate issues increases the possibility of an issue being exploited by cyber criminals.

- CSRM's centralized auditing and security services provide extra assistance to agencies that are not adequately staffed and resourced to provide these services on their own. Agencies that subscribed to CSRM's centralized services in 2021 generally scored higher on our compliance monitoring metrics.

- Commonwealth agencies once again participated in the Nationwide Cyber Security Review (NCSR), an annual self-assessment survey facilitated by the Multi-State Information Sharing and Analysis Center (MS-ISAC). The survey covers the components of the internationally recognized Cyber Security Framework (CSF) developed by the National Institute of Standards and Technology (NIST). In 2021, Commonwealth agencies scored themselves at a compliance level for IT security that compares favorably to agencies in other states. CSRM will use the data from the NCSR survey to identify areas that can be improved or reinforced.

2021 Annual Information Security Report

The 2021 Annual Security Report for the Commonwealth of Virginia report includes an analysis of the Commonwealth's threat management program, information security governance program, and risk management program.

Commonwealth Threat Management Program

The *Code of Virginia*, § 2.2-603(G) throughout 2021, 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 *Computer Security Incident Response Team* (CSIRT) then categorizes each security incident based on the type of activity.

During 2021, the Commonwealth of Virginia continued to be a target for cyberattacks. The Commonwealth experienced over 33 million attack attempts on the network and blocked 615,925 pieces of malware. Despite many layers of protection, the Commonwealth still experienced 201 successful IT security incidents.

IT Security Incidents

Information disclosure incidents were the main category of incidents in the Commonwealth. In 2021, information disclosure incidents rose to first place as the largest category of incidents with physical theft and loss in a close second. Cyber attackers have determined that the most vulnerable target is the employee as human error is the easiest to exploit. 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. However, the website is designed to capture and steal any information the user enters on the page.

Malspam email may contain a malicious attachment but more frequently 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.

As users become more dependent on technology, the threat of physical theft or loss of electronic devices increases. Users are not only using laptops today, but they also have tablets and smartphones that allow them to check email, perform banking transactions, surf the internet, and communicate with friends and family. With users keeping all their information in these devices, the theft or loss of a device could result in an attacker gaining enough personal information to steal a victim's identity.

Cybersecurity Awareness Training is key. In the 2020 legislative Session, Code of Virginia § 2.2-2009 was amended to require VITA to provide expanded security awareness training for the Commonwealth. This legislation recognized that to protect employees and Commonwealth systems and data, more emphasis needs to be given to security awareness training. Employees must be able to identify a potential attack and know how to respond to it. It is easy for employees to get busy and forget what they learned. Reinforcement is required.

To support this legislation, CSRM developed new IT security awareness and more comprehensive training requirements. CSRM also started working with agencies to pilot customized, simulated phishing campaigns. In the event an employee clicks a link or provides a login credential, the response is classified as a failure. The results were provided to the agency so identified employees could receive remedial training.

The third largest category of incidents was Unauthorized Access. Several agencies were using a company called SiteVision for hosting websites. In 2021, SiteVision experienced a breach in which email for a hosted agency was exposed and offered for purchase on the dark web. While working with SiteVision, it was determined that their email solution did

not meet COV security requirements. CSRM has worked with the affected clients to migrate them to a COV email solution and eliminate their use of SiteVision for email.

CSRM recommends best practices to protect systems and data from information disclosure and unauthorized access. Commonwealth Security has implemented many layers of protection to reduce the risk of information disclosure and unauthorized access. Securing data and systems goes beyond the technology that is deployed. It also encompasses securing the user as they are the last line of defense. Best practices that should be followed as part of a cyber security program include:

- All systems must be protected with the necessary security technology
- All systems need to be patched and/or upgraded to supported versions of software
- All systems need to be continually scanned for vulnerabilities and issues promptly remediated
- All systems should implement multi-factor authentication when possible
- Users need to be given ongoing 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

Ransomware

The prevalence of ransomware continues to grow, reaching new heights. Virginia is no exception as ransomware attacks continued to target several areas of the Commonwealth. In 2021, the Division of Legislative Automated Systems, a legislative branch information agency, was attacked. The attack prevented General Assembly legislators from working on bills and locked down the website of the Capitol Police. This attack exploited known vulnerabilities to gain access to systems. VITA provided some assistance with the incident, and the affected legislative agency hired Mandiant to evaluate and clean up their environment.

Third party ransomware attacks are also a concern for executive branch agencies. In December 2021, Kronos, a global timekeeping system used by some state agencies experienced a ransomware attack. Fortunately, COV agencies that use this cloud-based system did not experience any information disclosure due to the attack.

Between 2018 and 2021, multiple Virginia school systems experienced ransomware attacks. Nationwide, 67 individual ransomware attacks affected 954 schools and colleges, potentially impacting 950,129 students. It is estimated these attacks cost education institutions $3.56 billion in downtime alone. Most schools will have also faced astronomical recovery costs as they tried to restore computers, recover data, and shore up their systems to prevent future attacks.

The *Restructured Higher Education Financial and Administrative Operations Act of 2005* permits most higher education institutions in Virginia to have operational autonomy over their information technology, which has included a lack of any centralized oversight authority related to IT security. CSRM continues to recommend higher education institutions be subject to IT security oversight, like other executive branch agencies are.

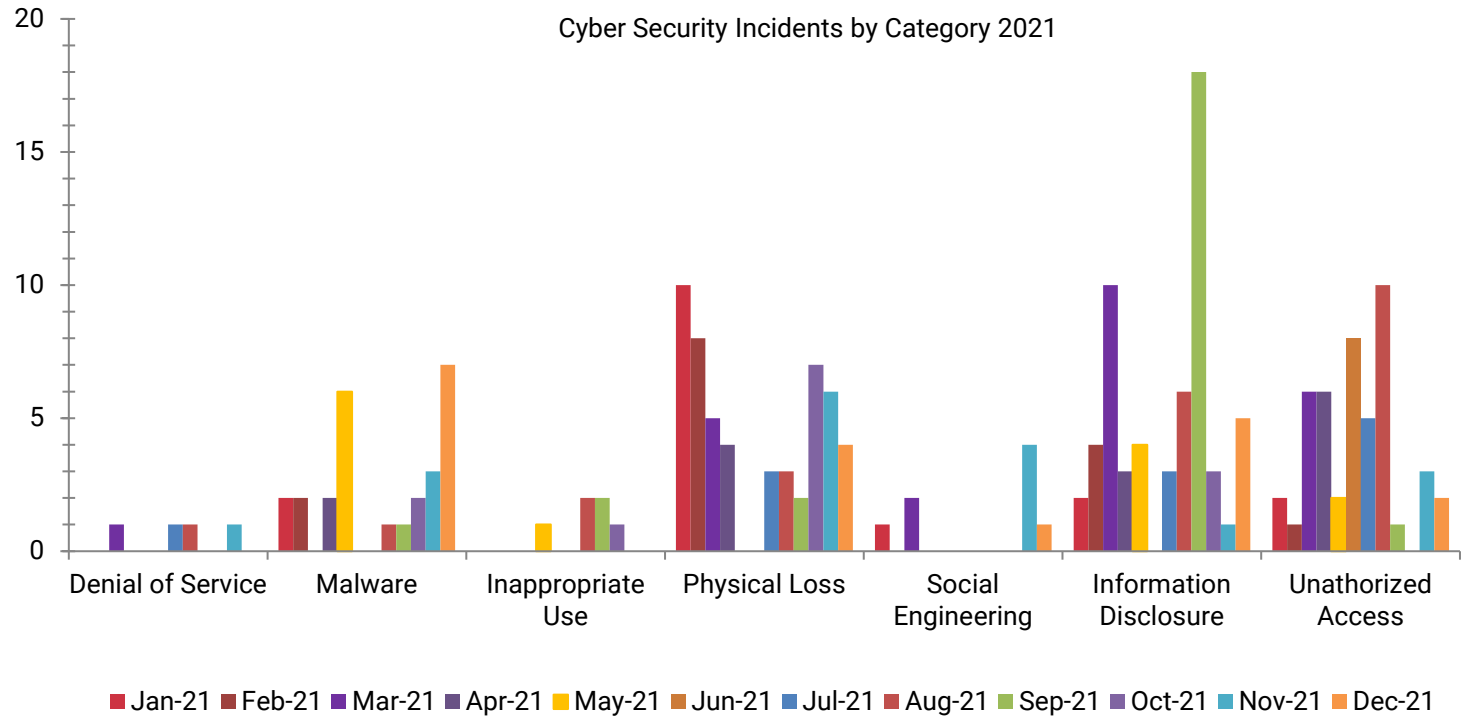


Figure 1: Cyber Security Incidents by Category

Security Awareness Training and Phishing Exercises

Security awareness training is critical. The employee is the last line of defense even as the attack landscape is evolving. While technical controls can be put in place to protect the environment, the most effective approach is employee training. The COV IT security standard requires all employees to take security awareness training annually. In some cases, this allows a large amount of time between training for attackers to develop new techniques and employees to forget what they have learned. CSRM has developed a free simulated phishing service to supplement this yearly training. These campaigns will reinforce security awareness training and allow users to practice their skills in a safe environment.

During 2021 CSRM implemented a new software platform designed to conduct large-scale simulated phishing campaigns. This product provides different levels of complexity and allows for customization to provide a unique experience for COV employees. As part of the launch, ten agencies participated in the simulated phishing campaigns and were categorized as small, medium, or large based on the number of employees. In total, 5,389 emails were delivered to the sampled employees. Of the emails delivered, 59% were opened by employees. Of the emails opened, 14.5% of the employees clicked the links in the email. When employees clicked on the links, 24% of them submitted data. Employees that clicked links in the phishing emails received additional security training. The results from these tests are provided below (Figure 2).

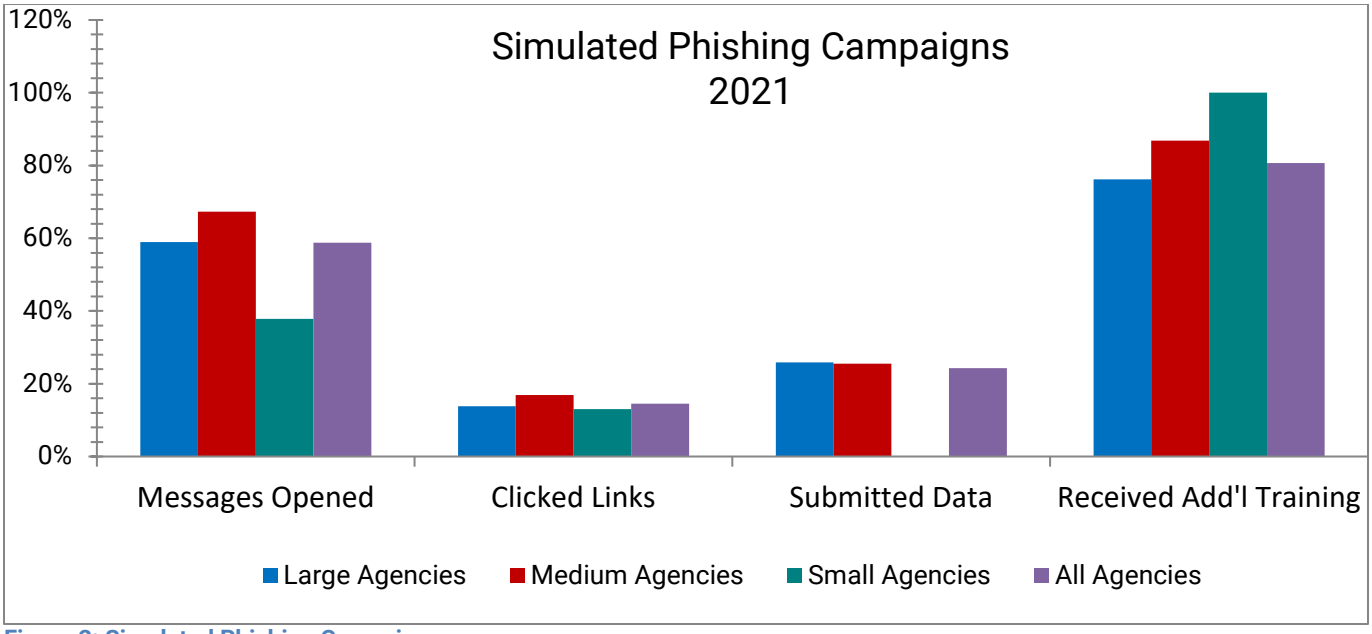


Figure 2: Simulated Phishing Campaigns

As a result of the new software platform, CSRM plans to provide quarterly phishing campaigns to executive branch agencies in 2022.

Incident Trends, Vulnerabilities and Exploits

CSRM continues to monitor cybersecurity incident trends. CSRM has been working diligently with agencies and suppliers to protect Commonwealth systems from cyber threats. Best practices were implemented, and additional layers of protection added. However, attackers continue to develop new tactics to compromise systems and incident trends have been steadily rising (Figure 3). CSRM is constantly investigating new security controls and additional practices to protect the environment from compromise. The spikes in incidents during 2021 were attributed to different types of attacks. March saw a spike in social engineering attacks. August's spike was attributed to unauthorized access. September was due to information disclosure. November was due to physical theft/loss of equipment. December was due to malware.

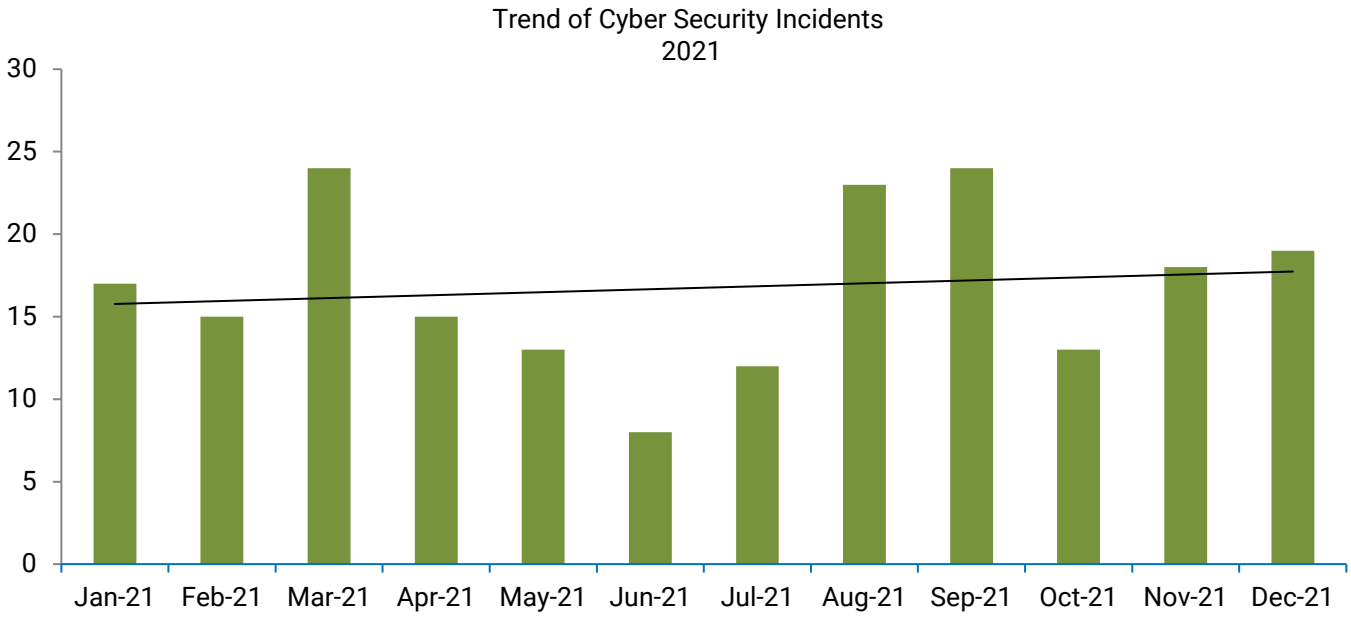


Figure 3: Trend of Cyber Security Incidents

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. We correlate this information with our intelligence partners. We then proactively block attacks from the points of origin before systems are compromised. During the past year, most attacks against the Commonwealth originated from within the United States, followed by attacks from Russia, Brazil, Egypt, United Kingdom, and India (Figure 4). It is important to remember that attack origination does not define attack attribution.

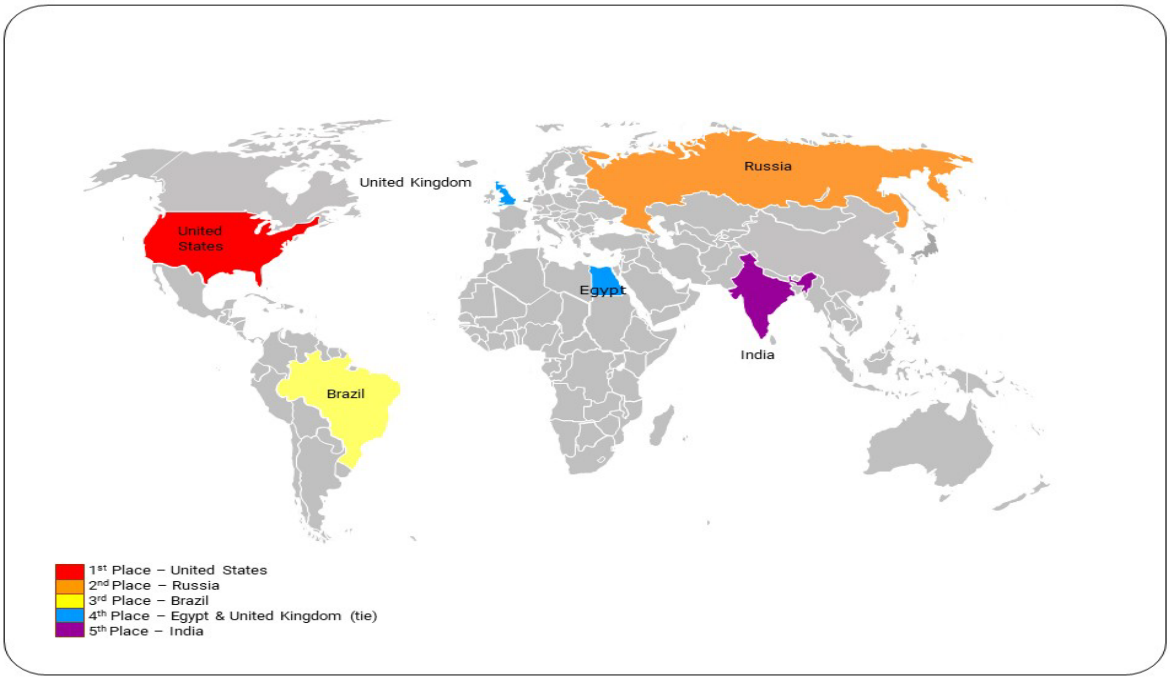


Figure 4: Cyber Attack Origins

Attack attempts are persistent. During 2021, over 33 million attack attempts were detected against Commonwealth systems. This is a rate of 1.05 attacks every second. The spikes in attempted attacks 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 (Figure 5).

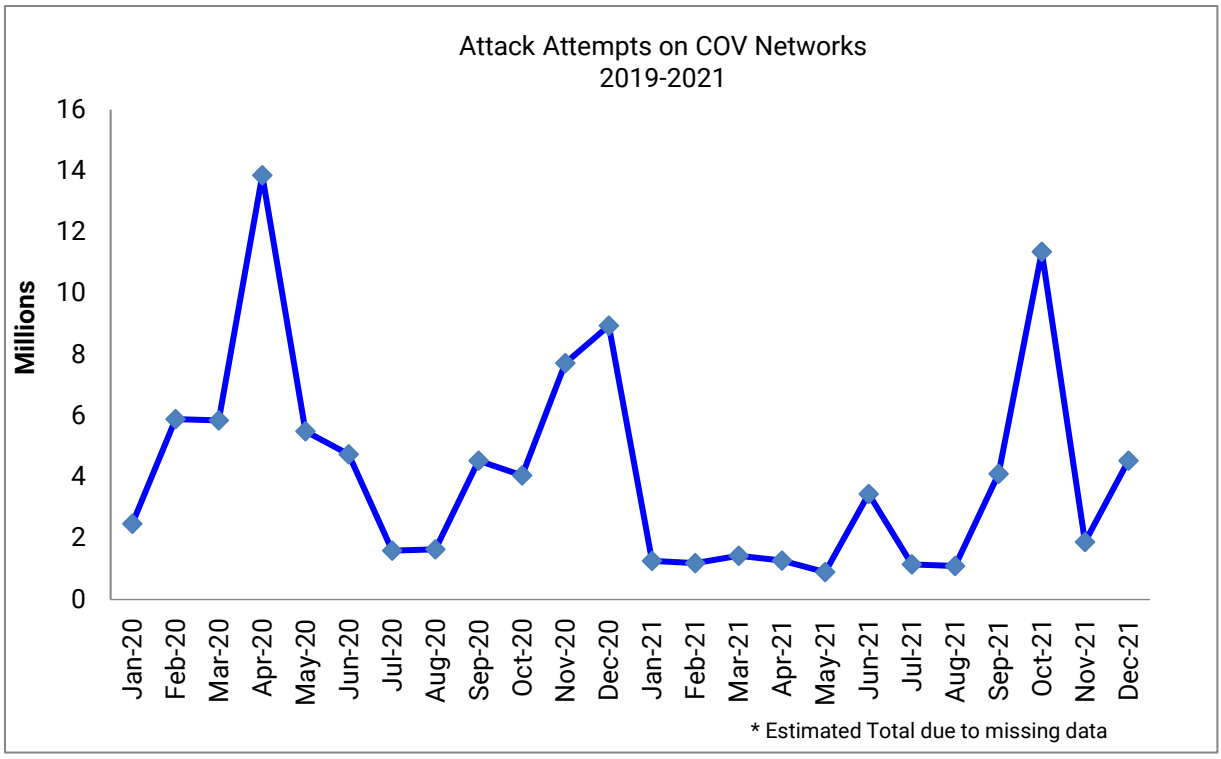


Figure 5: Attack Attempts on COV Networks

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
- **Social Engineering** – Attempt to get the user to click on a malicious link, open a malicious attachment or provide confidential information, such as account credentials
- **Physical loss** - Loss or theft of any COV resource that contains COV data
- **Unauthorized access** - Unauthorized access to COV systems and/or data

During 2021, information disclosure was the top category for security incidents. Physical loss was the second most frequent incident type, followed by unauthorized access, malware, social engineering, inappropriate use, and denial of service (Figure 6).

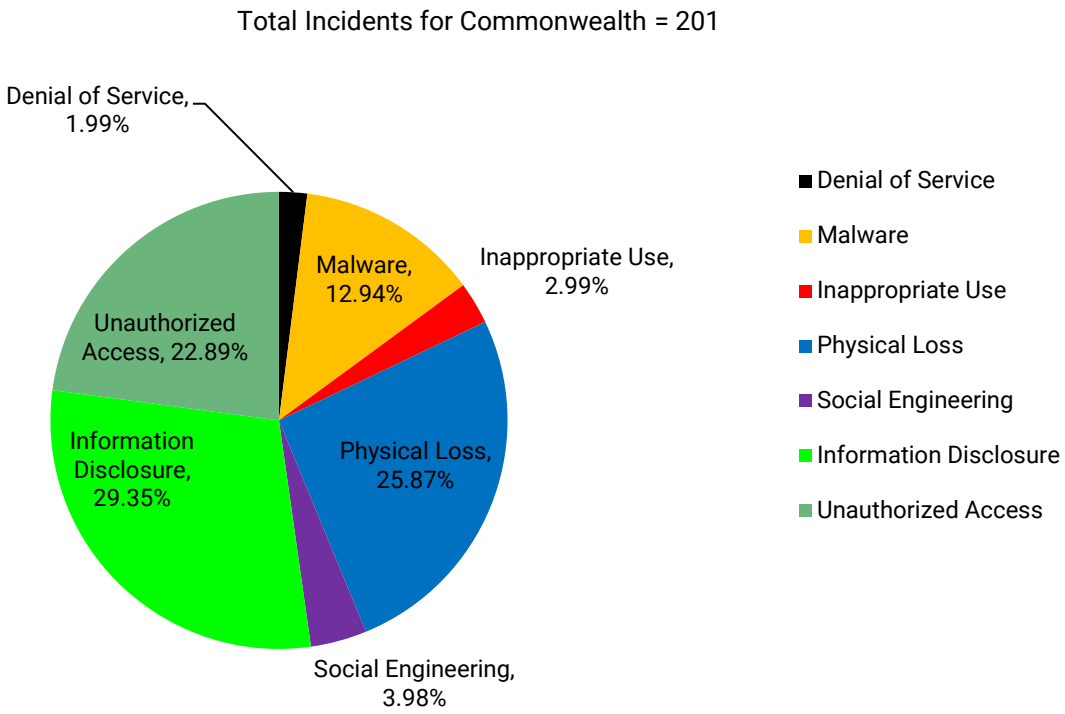


Figure 6: Security Incidents by Category

Malware is blocked. The Commonwealth has multiple layers of protection against malware infections occurring on COV devices. During 2021, these layers of protection blocked approximately 615,925 pieces of malware (See Figures 7 & 8). During January and February there was a spike in identified malware due to a new tool being introduced. This new tool scans for malware as processes are executed on an endpoint device. This is different from running a malware scan after the file has been written to a device. This means that detection can occur earlier in the process. Even with multiple layers of protection, the Commonwealth still experienced 26 successful malware infections.

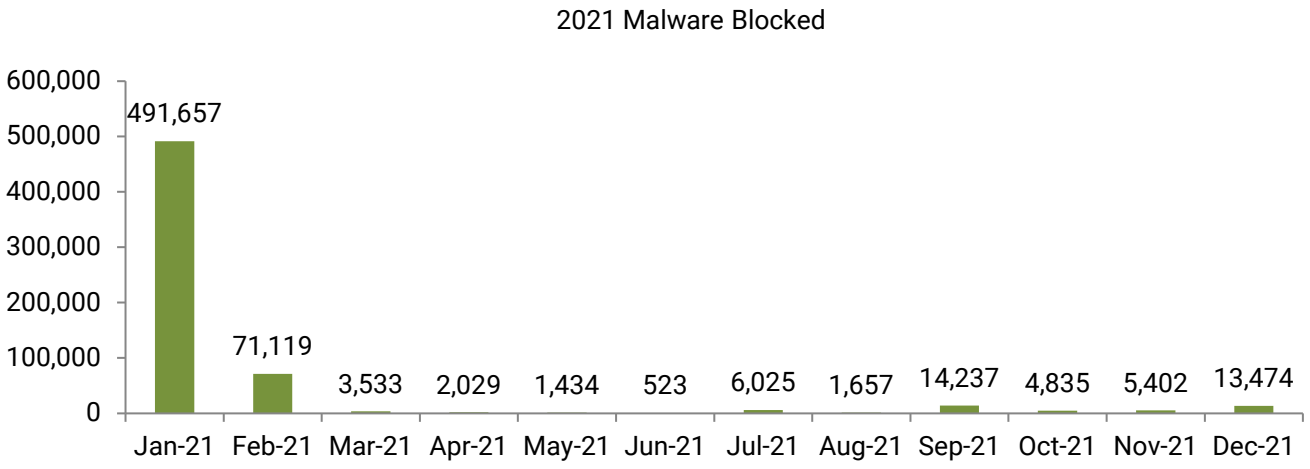


Figure 7: Malware Blocked

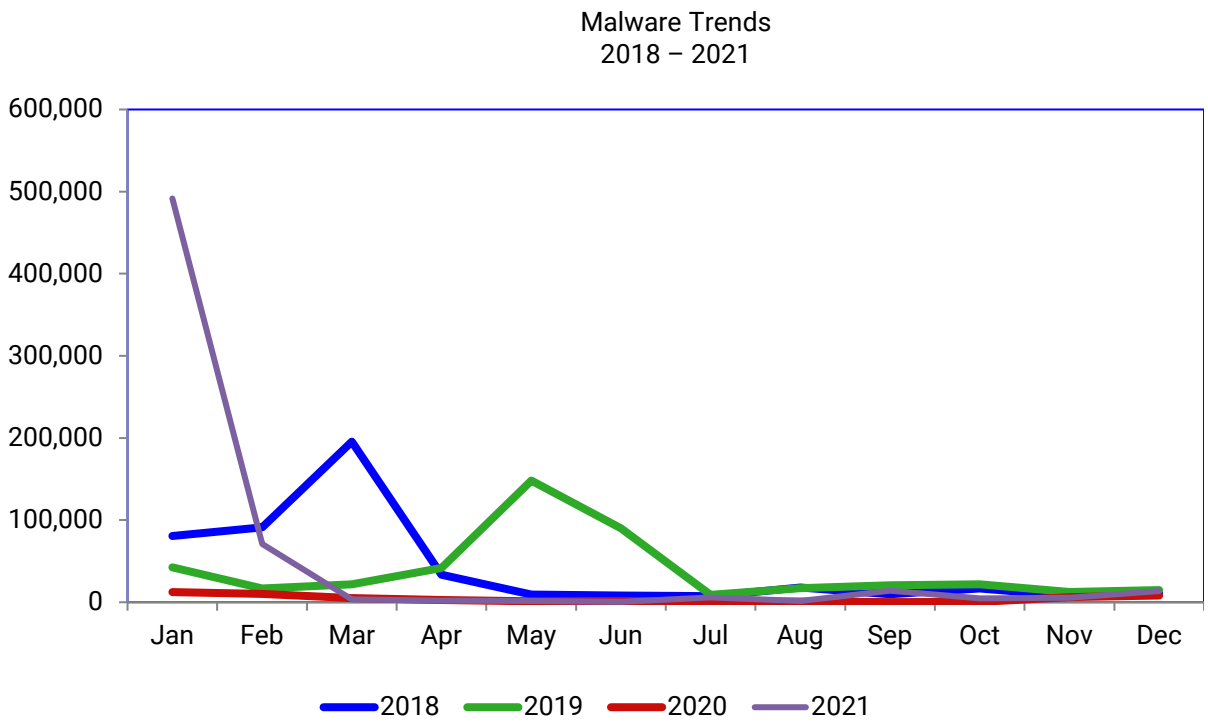


Figure 8: Malware Trends

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 advisories for those items that are critical and/or are being exploited in the wild. These advisories are distributed to localities, state agencies, and higher education institutions. In 2021, the CRSM threat management team identified 6,467 vulnerabilities that could affect Commonwealth systems. This is a slight increase (0.65%) over 2020 (Figure 9). Information security officers at each entity can use this information to ensure critical vulnerabilities are being patched in compliance with security standards.

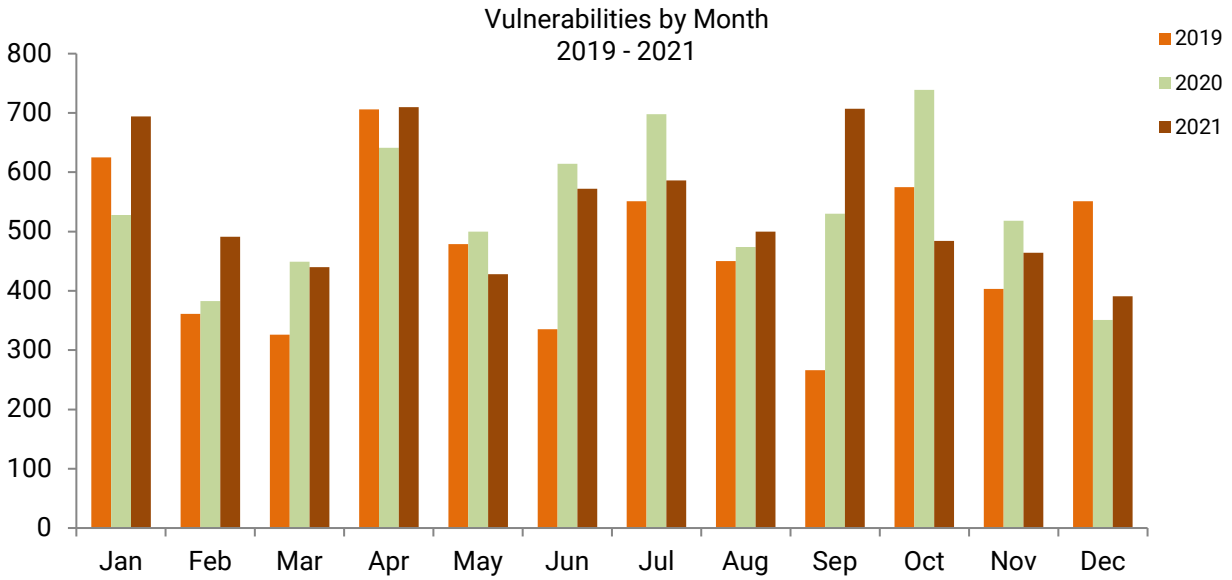


Figure 9: Vulnerabilities by Month

Critical exploits in the wild increased by 43% 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.

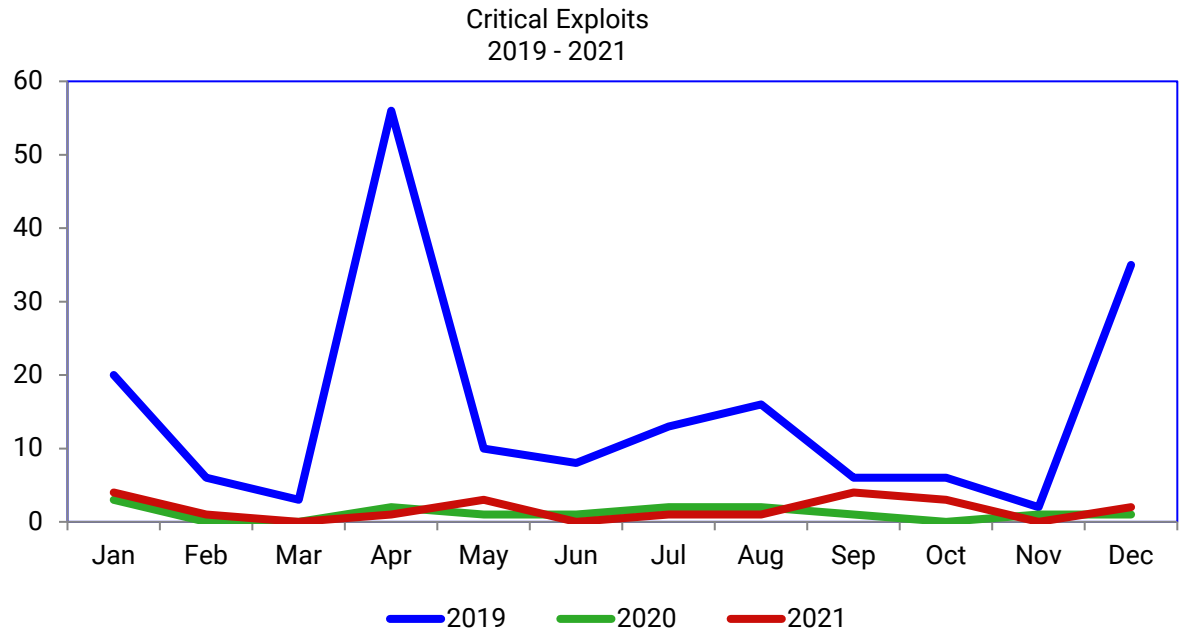


Figure 10: Critical Exploits

During 2021, the total number of zero-day vulnerabilities tracked by CSRM increased from 14 to 20, a 43% increase. As more data is collected about the systems and technologies that are in use throughout the Commonwealth, security analysts have been able to focus on the products that are being used. This allows CSRM to provide advanced warning to agencies prior to systems being attacked.

It is important to follow how these critical exploits affect the COV environment. 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 are available or can be applied.

The computer security incident response team (CSIRT) analyzes each incident to determine the root cause and uses the information to strengthen protections to mitigate the risk of future attack. However, critical exploits remain a risk, particularly zero-day exploits for which no patch or fix is available. As previously noted, a change in monitoring tools resulted in a spike in the number of pieces of malware being blocked in January and February.

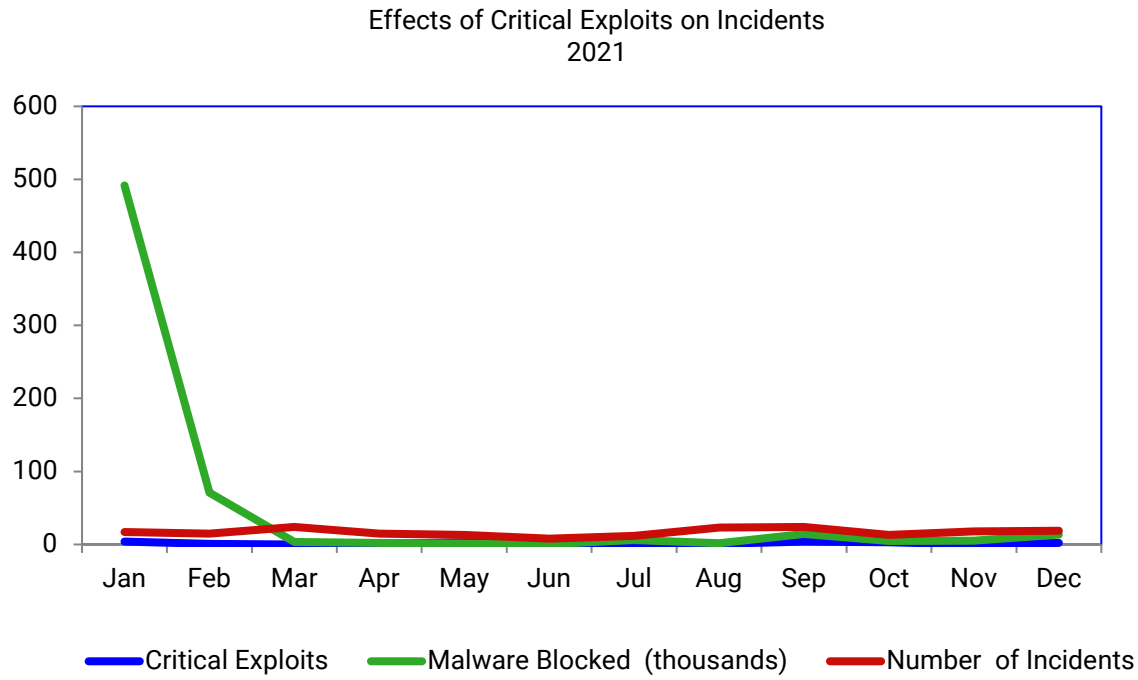


Figure 11: Effects of Critical Exploits on Incidents

Cyber intelligence from Commonwealth partners

The information received from Commonwealth partners includes data involving state and local governments, higher education institutions and public-school systems. MS-ISAC compiles data by monitoring the internet for potential events. CSRM disseminates "alerts" identified by the data to the affected entities and tracks them as investigations. Alerts are considered investigations until the results of the alerts are known.

In 2021, the Commonwealth data center moved, causing an extended disruption to the monitoring device that the MS-ISAC has in place on the COV network. This resulted in a decrease in the number of alerts being received and investigations being conducted on third party intelligence.

However, the total number of investigations conducted by the CSRM Threat Management Team remained steady. CSRM utilized a new threat intelligence platform to monitor for compromised accounts, data leaks, and malicious activity. In addition, to the intelligence received, the team performed 73 investigation requests from executive branch agencies. The data on the types and quantities on investigations conducted is listed below. The following chart (Figure 12) shows the percentage of investigations by type of entity.

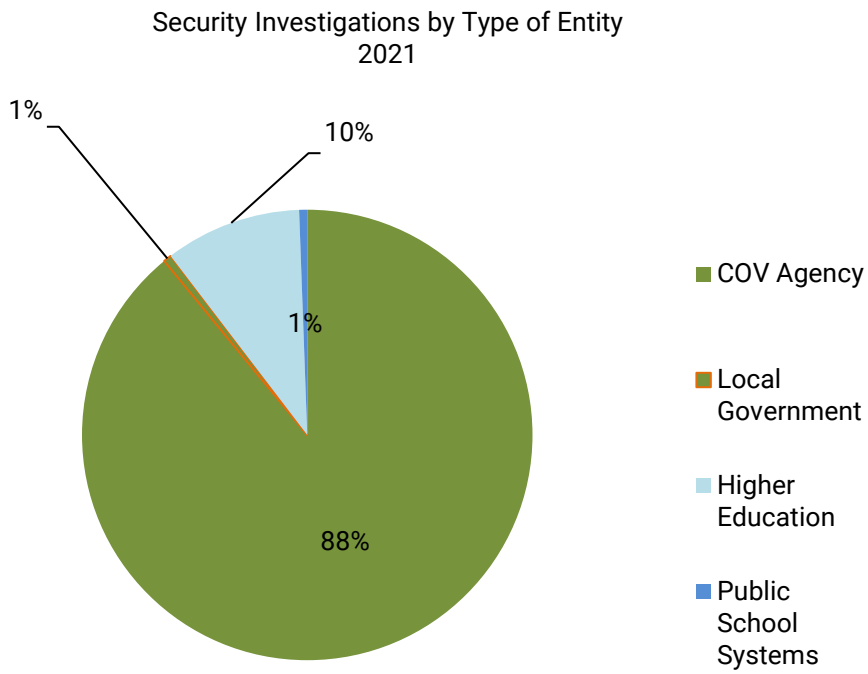
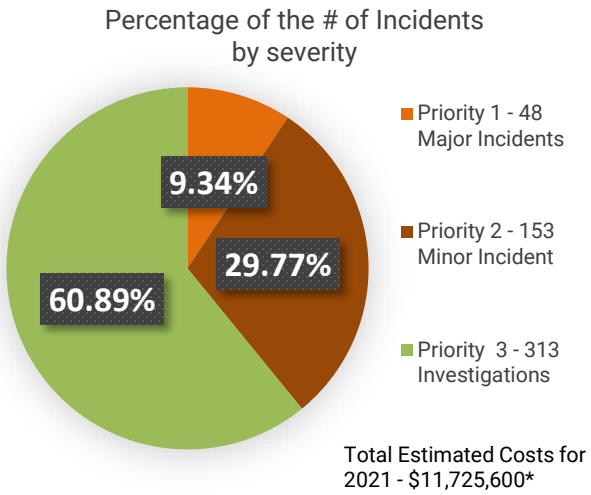


Figure 12: Investigations by Type of Entity

Costs of a Data Breach – In 2021, the Ponemon Institute Cost of a Data Breach report indicated the average cost per incident for the public sector rose from $1.08M to $1.93M, a 78% increase in cost over 2020. Using this average and $100 average labor rate, CSRM estimated the costs of response and recovery efforts for all major and minor incidents, as well as for investigations that did not rise to the level of an incident. Major incidents result in an extended incident response lifecycle, so the proportion of cost/incident is much greater. The estimated response and recovery costs for all cybersecurity incidents in 2021 in the Commonwealth was $11,725,600. Although major incidents made up only 9.34% of the total number of incidents in 2021, they still accounted for almost 98% of all response and recovery costs. The following chart (Figure 13) provides the estimated costs incurred by the Commonwealth.



Response and Recovery Costs
by incident severity

Major Incidents	$11,480,000
Minor Incidents	$ 122,400
Investigations	$ 125,200

* Costs for Major Incidents estimated using data from the Ponemon Institute 2021 Cost of Data Breach Report.

Figure 13: Estimated Incident Costs

CSRM continues to provide IT security support for elections in the Commonwealth. Election systems are part of the critical infrastructure. According to the Cybersecurity & Infrastructure Security Agency (CISA), critical infrastructure describes the physical and cyber systems and other assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety. Critical infrastructure provides the essential services that underpin American society.

To prepare for elections, CSRM performs a comprehensive security review to ensure the systems and infrastructure supporting the elections are secure. In partnership with the Department of Elections, CSRM electronically scans all election systems for security vulnerabilities. On Election Day, a cybersecurity command center is established to handle any issues that occurred. CSRM also works with the State Board of Elections to develop security regulations and standards and provide 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 partnering with state elections officials to provide support for upcoming elections.

CSRM coordinates an annual Cybersecurity Tabletop Exercise. Amid the COVID-19 pandemic, VITA hosted the third Cybersecurity Tabletop Exercise, performed on an enterprise level, in the Commonwealth of Virginia. The 2021 Tabletop Exercise brought agencies and service tower suppliers together and increased the awareness, effectiveness, and efficiency of their Incident Response (IR) tools and processes. The exercise focused on the planning and execution aspects of exercises, to include objectives, scenarios, reporting and assessment procedures, network architecture, tools, and lessons learned from utilizing the scenarios outlined during the exercise.

The overarching objective of executing real world cyber scenarios with a series of simulated events involving multiple entities was to ensure information systems and networks successfully operate in support of the exercise scenario. This was designed to improve enterprise information assurance by demonstrating the impacts of successful attacks, service area response and execution. The exercise also demonstrated the ability to identify, contain, eradicate, and recover with minimal impact to agency daily business operation. At the completion of the exercise an "After Action Report" was developed so areas of improvement could be addressed.

Significant conclusions from the exercise:

- Simulated events were engaging and reflective of the Commonwealth's information technology environment.
- The current format worked well for the COVID-19 restrictions and allowed for a significant growth in participation compared to prior year.
- Most responses from participants met and/or surpassed initial expectations, which reflects significant improvements in understanding how the incident response process works across the Commonwealth IT infrastructure.

Feedback for the event was significantly positive, with the understanding that certain limitations had to be in place due to COVID-19. The added experience and time between this year and prior year's event helped optimize the IR process and improve the quality of service to the Commonwealth of Virginia.

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. It sets security strategy for the Commonwealth, supports agencies in their efforts to foster secure IT security environment, and promotes information security training and awareness.

Statute requires compliance monitoring

Per § 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 accomplishes this undertaking by monitoring each agency's overall compliance with IT audit and

information security risk program standards and policies. CSRM continues its transition toward a level that provides additional insight into agency programs and will enable the Commonwealth to improve security endeavors.

Commonwealth Information Security Council

A select group of information security officers from various state agencies, with support of CSRM, comprise the Commonwealth Information Security (IS) Council. The purpose of the council is to increase, through education, the understanding of key business processes of state agencies; to obtain consensus and support for enterprise-wide IT security initiatives; to identify key areas for process improvement; and to coordinate agency business processes with VITA's processes.

The IS Council also helped to develop the Commonwealth's IT security awareness training program, providing insight and perspective regarding the new information security training program required for all state employees. CSRM will continue to participate with the IS Council to get agency input as we work to develop practical and effective security initiatives.

Risk Management Committee

The IT Risk Management Committee is made up of risk specialists from CSRM's IT Risk Management division and with information security officers from other Commonwealth agencies. The committee meets monthly to discuss approaches to addressing risks and issues identified as significant. In addition, the committee determines the prioritization of risk mitigation as well as provides feedback on the current approaches to maintain established risk thresholds. The committee documents and reports risk alerts to escalate issues with potential significant impact to the enterprise or customer agencies. As a result, VITA, agencies, and the associated service providers have made significant progress in the mitigation of the potential threats and impacts of the risk and issues identified.

The CSRM risk management team in coordination with the Risk Management committee developed a methodology to estimate financial costs associated with the detection, response, and recovery activities associated with cybersecurity incidents. This quantitative model continues to help the Department of Treasury determine how much cyber liability insurance is needed in the event a system is breached or incapacitated. It is a useful methodology to assist executive leadership to make better and more informed decisions related to their agency's IT assets. CSRM also uses this methodology to prioritize security decisions based on quantifiable risk.

As part of the VITA governance program, CSRM has developed and implemented methodologies for monitoring and managing risks associated with third party service providers. The amount of risk introduced by third parties is quantified to ensure the Commonwealth maintains established risk thresholds. Within the multi-sourcing service integration (MSI) model that VITA has adopted, CSRM plays an integral role in identifying cybersecurity risks and tracking them until they are resolved. CSRM hosts monthly risk management committee meetings to discuss identified risks and issues. Risks that may have a significant impact on the enterprise or customer agencies are identified and escalated for action through risk alerts. As a result, VITA and the associated service providers have addressed IT security threats before there was significant impact to COV data and systems.

As agencies continue to move toward cloud services, CSRM has established a security review process for third party systems and services to ensure that those services are secure, dependable, and resilient. The Enterprise Cloud Oversight Service (ECOS) is a service specifically created for establishing contract terms and oversight of third-party vendors offering Software as a Service (SaaS) applications. SaaS is a type of cloud service where an application runs on infrastructure not owned or managed by the Commonwealth. CSRM provides a pre-contracting assessment of systems to ensure the appropriate security controls are in place prior to being implemented.

Commonwealth IT Audit and Risk Management Program

The Commonwealth IT audit compliance 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 determines the agencies' overall audit program score.

The Commonwealth IT risk management program entails the review and oversight of agencies' IT risk management activities. The program requires the submission of agency data sets, business impact analysis (BIA), risk assessment plans, risk assessments, risk findings updates, ISO certification/reporting and intrusion detection reports. These submitted and approved pieces of data represent the components used to determine the agencies' overall risk program score.

Commonwealth Audit Program

Audit compliance report card

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 submission of an IT security audit plan, agency submission of quarterly updates to their IT security audit findings, and completion of required IT security audits. The compliance grades provide a familiar measurement tool to reflect the degree to which agencies are completing their necessary IT security audit requirements. The compliance grades identify agency IT audit strengths and opportunities for improvement.
Agency audit compliance grades have declined from the previous year, with less agencies earning "A" grades.

While the percentage of "B" and "C" grades increased, the percentage of "D" and "F" grades also increased indicating that agencies could not fully complete all audit requirements (Figure 14). CSRM expects audit compliance grades will recover as more agencies use the tools afforded them, including audit centralized services, audit standards, and templates.

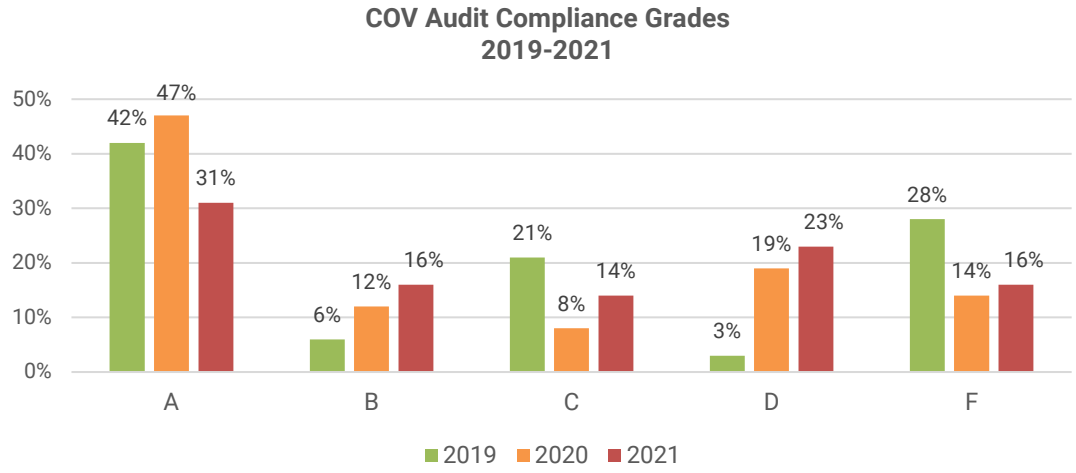


Figure 14: Audit Compliance Grades

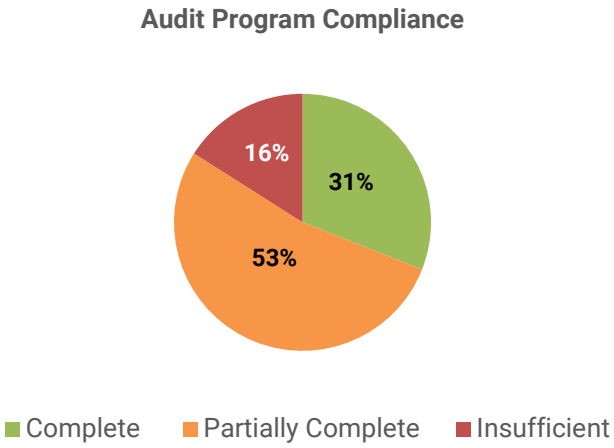
Key security audit compliance metrics and analysis

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

Overall agency IT security audit program compliance decreased. IT security audits provide an independent assessment of each agency's sensitive IT applications. These audits help agencies ensure that the appropriate security controls are implemented in their agency applications and infrastructure. Commonwealth IT security audit requirements include:

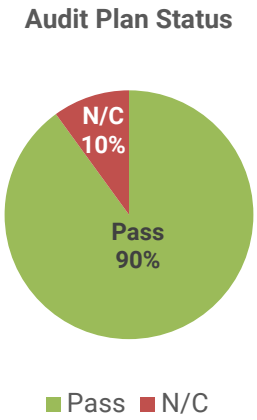
- creating an annual IT security audit plan
- performing IT security audits on sensitive systems triennially
- updating the status of corrective action plans for IT security findings discovered during the audits.

Audit program compliance has decreased from the prior year, with 31% of agencies having implemented a comprehensive audit program in 2021. This decrease is mainly attributed to agencies not performing IT security audits on sensitive systems due to resource constraints caused by the pandemic. CSRM anticipates audit program compliance will improve for agencies as auditing resources become more reliably available.



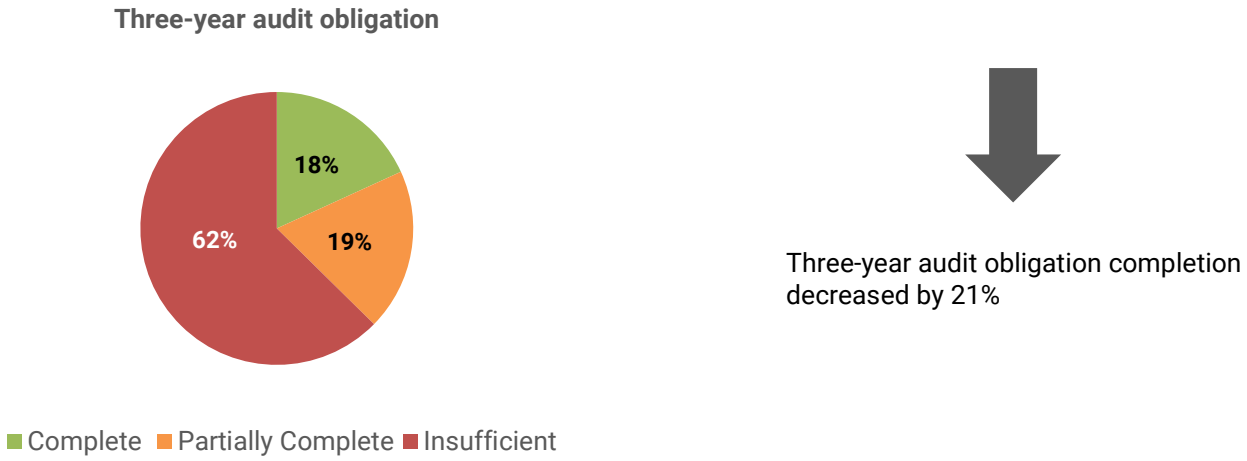
Audit program compliance decreased by 16 percent

Most agencies submit their IT security audit plans as required. IT security audit plans demonstrate the agencies' intentions to complete the audits of their sensitive information systems triennially. In 2021, 90% of agencies submitted an IT security audit plan. These scores have remained the same for the last four years. Most agencies are submitting IT security audit plans timely. However, there are still a few agencies that have failed to meet this requirement. CSRM will work with those agencies to ensure they understand this requirement and share resources that are available to complete the IT security audit plan.

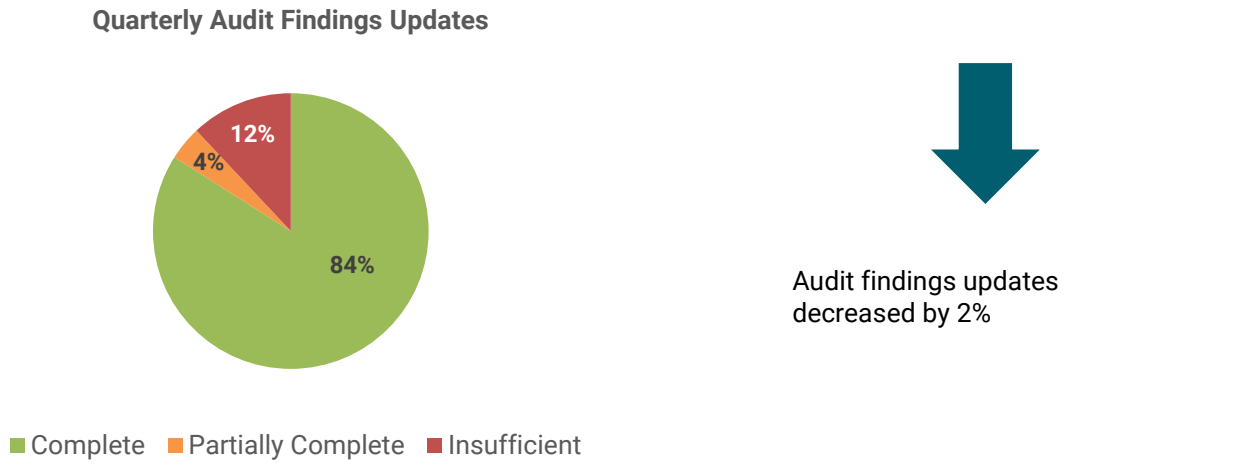


IT security audit plan status remained the same

Agency three-year audit obligation metrics declined. Of the agencies that have established an audit plan, 18% have fulfilled their obligation to audit every sensitive system at least once every three years, a decrease of 21% from last year. CSRM anticipates this metric will recuperate as agencies concentrate on getting sensitive systems audited on a three-year basis.



Most agencies that perform IT security audits provide the required quarterly updates to the findings. Our analysis found that 84% of agencies that submitted audit findings provided the required quarterly IT security audit updates. In addition, the percentage of agencies that had insufficient quarterly updates increased by 4% from the prior year. CSRM will work with agencies to report their progress toward closing the findings and prioritize their resources to address the most significant findings first.



Audit Findings Analysis

Although fewer audits were conducted in calendar 2021 than in the previous year, agencies reported 468 new audit findings in 2021, compared to 402 new audit findings reported in 2020. Remediation of audit findings is also at a higher pace in 2021. As of the end of calendar year 2021, there were still over 1,600 audit findings in need of remediation (Figure 18).

CSRM requires agencies to file an exception for any audit findings exceeding 90 days. Agencies must be able to provide a business or technical justification for the delay while also demonstrating they have implemented adequate mitigating controls until the issue can be resolved.

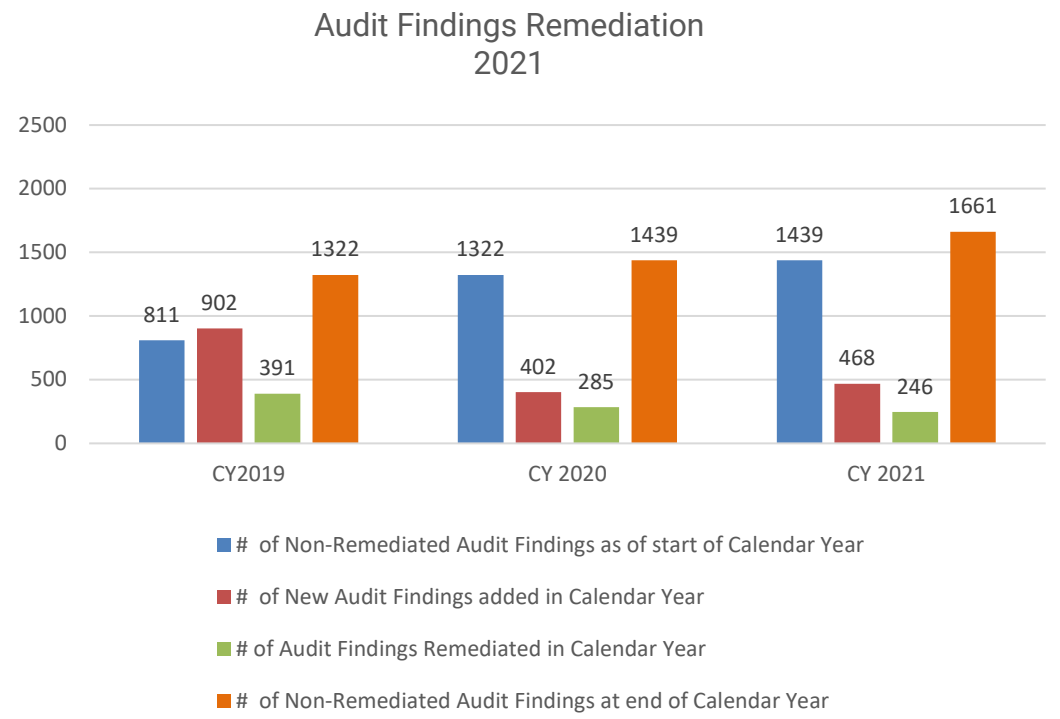


Figure 15: Audit Finding Remediation

Audit findings are not addressed timely. CSRM analyzed the average number of days to it took to close audit findings in 2021. On average, the turnaround time to resolve and close an audit finding was 495 days. This is a slight improvement over the 2020 figure of 528 days. The average number of days to close findings associated with critical security controls, identified by the Center for Internet Security (CIS) to protect against known attack vectors has decreased from 553 days to 475 days (Figure 19).

We recommend agencies dedicate additional resources to address the issues identified in audit and risk findings to ensure audit and risk findings are resolved in a timelier manner. Agencies should continue to prioritize and remediate findings by criticality, first addressing the findings in any areas associated with critical controls.

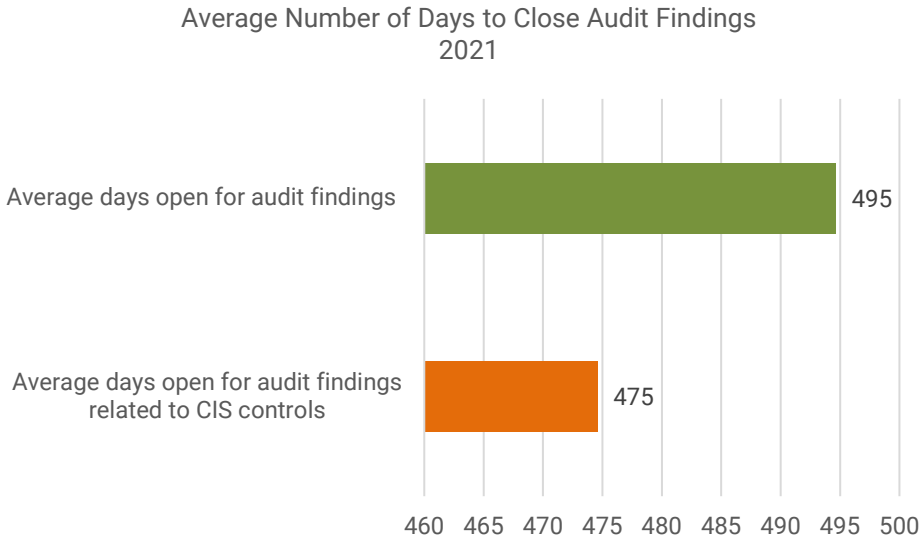


Figure 16: Closing Audit Findings

CSRM analyzed IT security audit findings by security control family. Commonwealth security standards address 17 information security control families or groupings of similar IT security controls designed to support secure and resilient IT systems (Figure 20). Based on an analysis of the IT audit findings for the Commonwealth, the top IT security control families identified by audits are:

- Access control family (18%)
- Audit & accountability family (10%)
- Configuration management family (8%)

CSRM uses these results to provide agency training, develop further security guidance and offer tools for the agencies to address the control gaps in these areas.

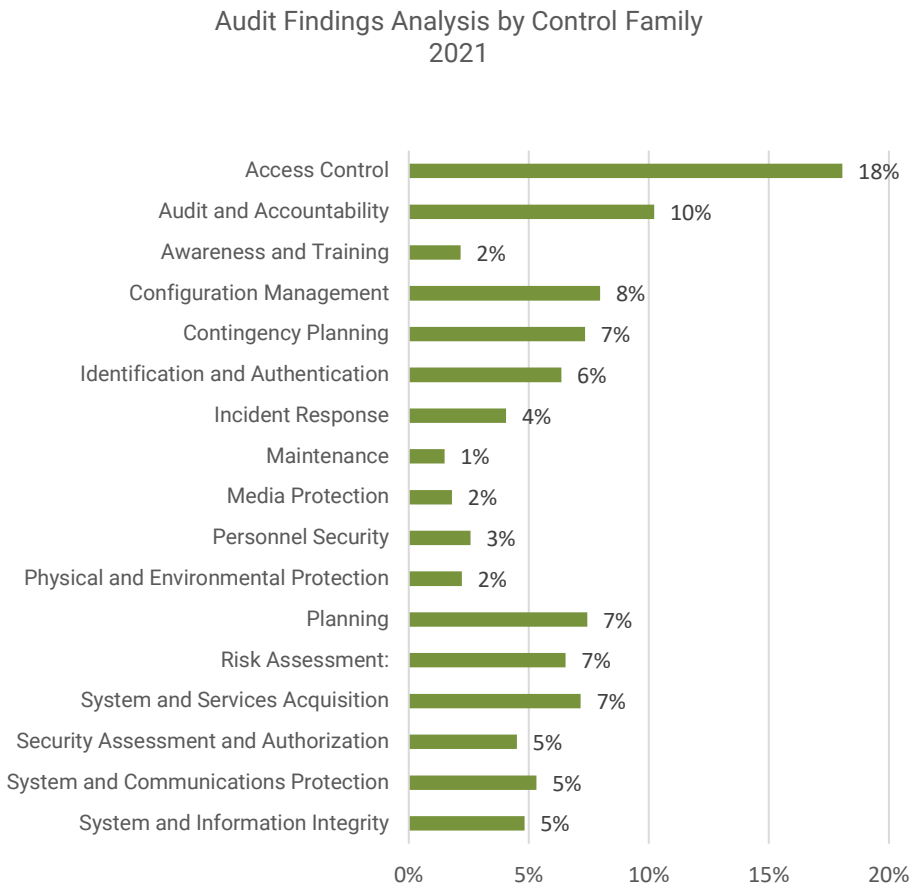


Figure 17: Audit Findings by Control Family

Commonwealth IT Risk Management Program

Risk compliance report card

The risk compliance grades reflect the varying levels of risk management programs at the agencies. The grade is based on an agency's submission of:

- an IT risk assessment plan,
- quarterly updates to their risk assessment findings,
- completion of required IT risk assessments,
- whether the ISO is certified and whether the ISO reports to the agency head,
- the completion of the agency Business Impact Analysis,
- the certification of agency applications and
- the submission of quarterly IDS reports.

The agencies are graded using a ten-point letter grade system. The percentage of agencies with "A" and "B" grades decreased in 2021. There was a 5% increase in agencies with "C" grades and a 5% increase in "D" grades, but a 1% decrease in "F" grades (Figure 21). This risk metric was mainly impacted by agencies not being able to fulfil their 3-year risk assessment obligations. CSRM anticipates risk program compliance grades will get better as agencies focus on completing IT risk assessments on sensitive systems and providing quarterly updates on the corrective actions taken to address risk assessment findings.

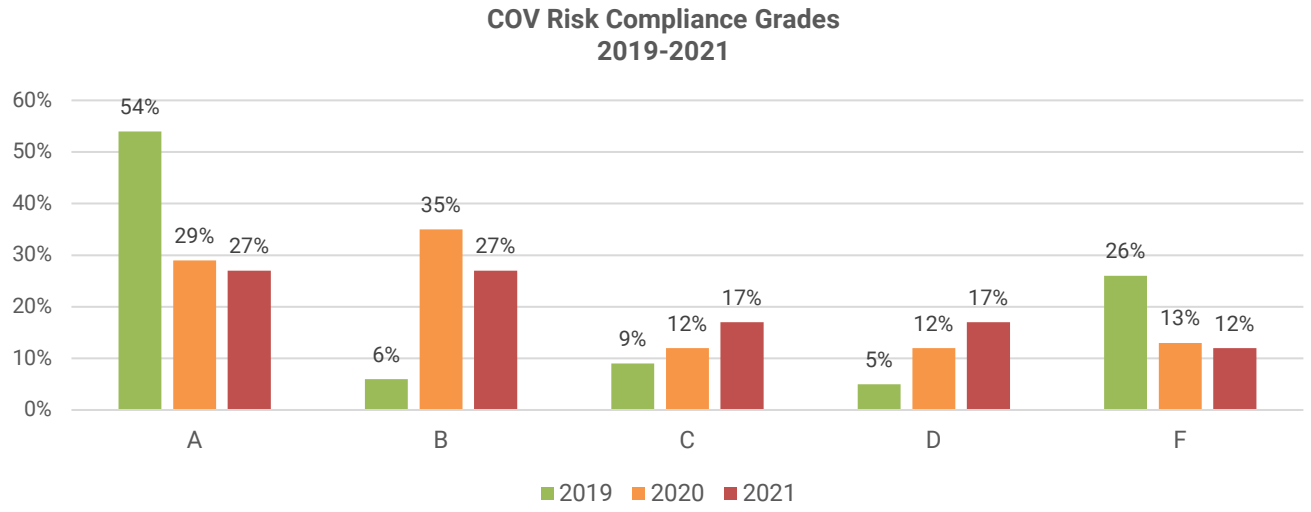
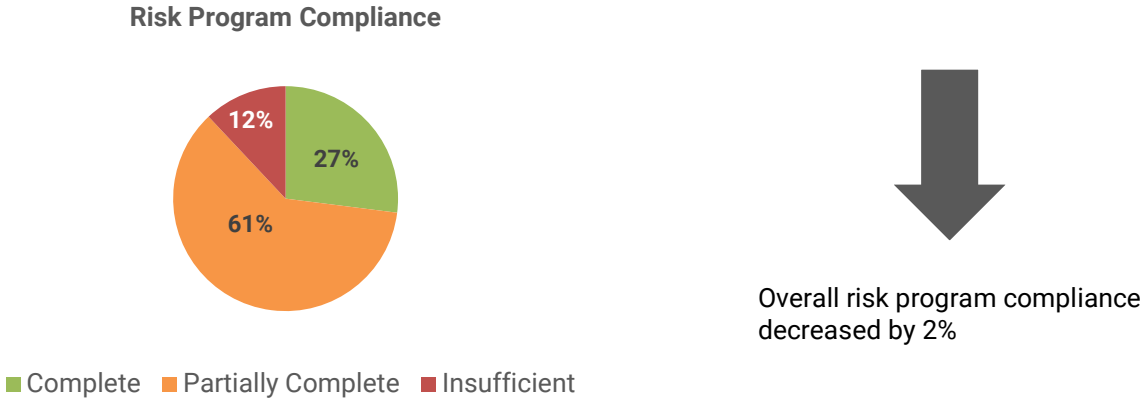


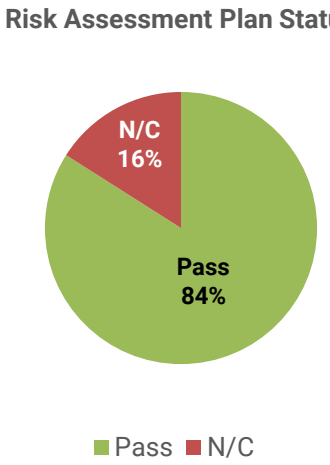
Figure 18: Risk Compliance Grades

Key security risk compliance metrics and analysis

Risk management program compliance slightly declines. Risk management activities experienced a slight downturn during 2021. The overall risk program compliance decreased by 2% from the previous year. Agencies not completing risk assessments triennially contributed to the decrease. CSRM recommends agencies place more emphasis on implementing comprehensive risk management programs by providing additional attention to risk assessments and business impact analysis and dedicating the necessary resources to their IT risk management programs.

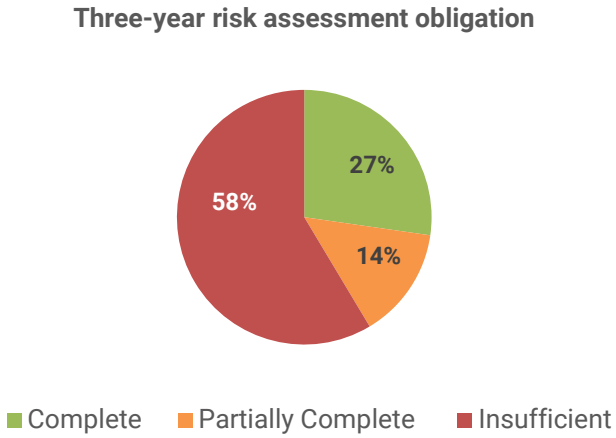


Most agencies submit risk assessment plans as required. Agencies must submit a risk assessment plan on an annual basis identifying their plan to complete risk assessments on sensitive systems. Risk assessment plan submissions experienced a 2% decrease in 2021.



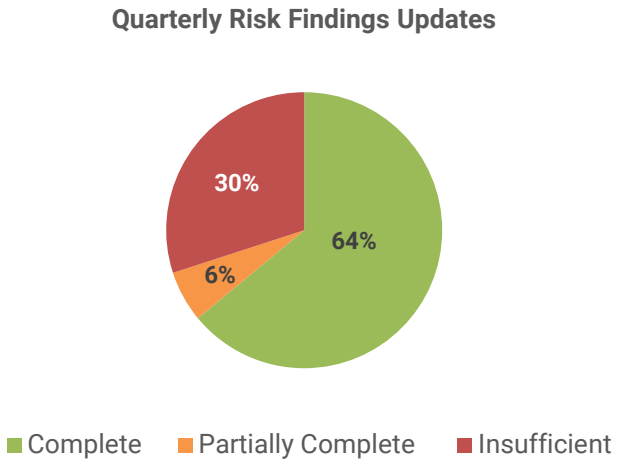
Risk assessment plan submissions decreased by 2%

Three-year risk assessment obligation declines. Risk assessments are central to ensuring agencies are monitoring and mitigating critical risks. This metric details agencies' completion of risk assessments for sensitive systems at least once every three years. Only 27% of agencies have fulfilled their obligation to complete a risk assessment of every sensitive system at least once every three years. This is a decrease of 18% from last year. To improve compliance with this requirement, CSRM will increase communication to agencies and offer additional training on risk assessment processes.



hree-year risk assessment bligation decreased by 18%

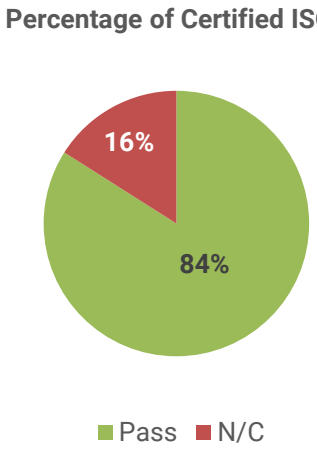
Only 64% of agencies that perform risk assessments provide the required quarterly updates to the findings. Our analysis found that 30% of agencies did not submit required quarterly risk updates for open risk findings and 6% submitted only partial updates. CSRM will continue to encourage agencies to report their progress toward closing risk findings and prioritize their resources to address the most significant risk findings first.



The percentage of agency ISOs (Information Security Officers) that are certified has declined slightly since last year. 84% of ISOs are certified in 2021, compared to 86% in 2020. 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 has the minimum baseline knowledge of Commonwealth information security requirements. Agencies that do not have a certified ISO consistently have lower audit compliance and risk compliance grades. The following agencies did not have certified ISOs at the conclusion of 2021:

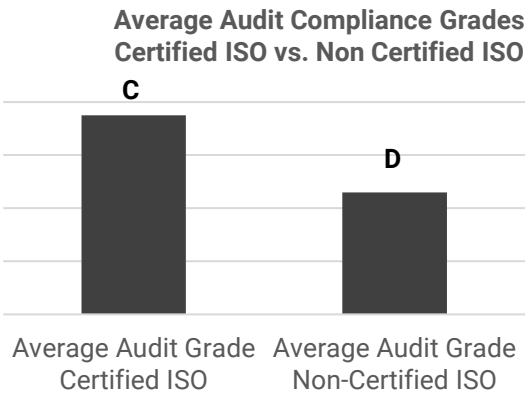
- Gunston Hall
- Indigent Defense Commission
- Jamestown-Yorktown Foundation
- New College Institute
- Science Museum of Virginia
- Southwest Virginia Higher Education Center
- Tobacco Region Revitalization Commission
- Virginia Commission for the Arts
- Virginia Foundation for Healthy Youth
- Virginia Innovation Partnership Corporation
- Virginia State University

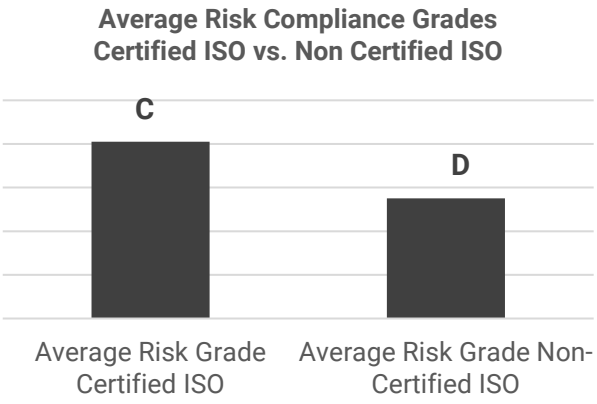
CSRM recommends these agencies commit to recruiting, hiring, and training ISO staff to initiate improvements in their agencies' IT security posture. CSRM is monitoring compliance with this metric and using it as criteria for each agency's risk compliance score.



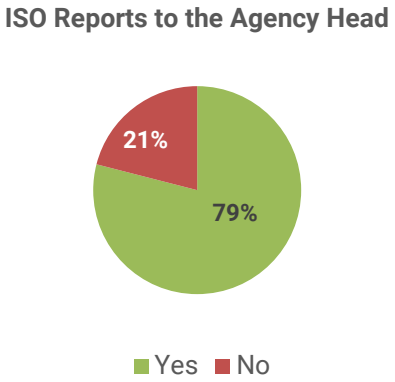
The percentage of ISOs that are certified decreased by 2%

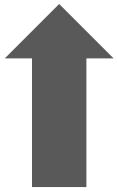
In addition, there is a correlation between ISO certification and overall compliance as summarized in the charts below.





The majority of agency ISOs report to their agency head as required. 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. Most agencies (79%) have met this requirement, a 5% improvement from last year. While we recognize each agency has its own unique organization, CSRM recommends agencies take the necessary steps to ensure that the ISO reports directly to the agency head to confirm that information security has the needed emphasis and support in every agency in the Commonwealth.



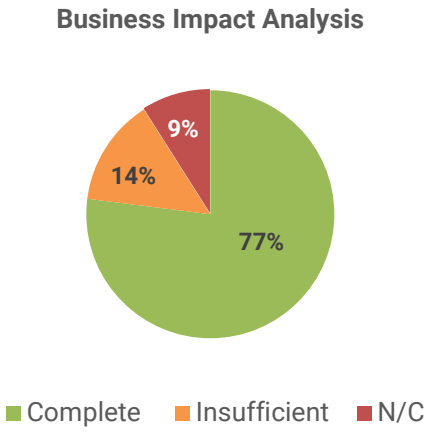


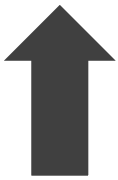
ISOs that report to their agency head increased by 5%

The following ISOs were not reporting to agency heads or do not have approved security exceptions to the requirement.

- Department of Conservation and Recreation
- Department of Fire Programs
- Department of Forestry
- Department of Military Affairs
- Department of Planning and Budget
- Department of Wildlife Resources
- Jamestown-Yorktown Foundation
- Office of Attorney General
- Southern Virginia Higher Education Center
- Southwest Virginia Higher Education Center
- Virginia Department of Emergency Management
- Virginia Department of Health
- Virginia Department of Transportation
- Virginia Economic Development Partnership
- New College Institute

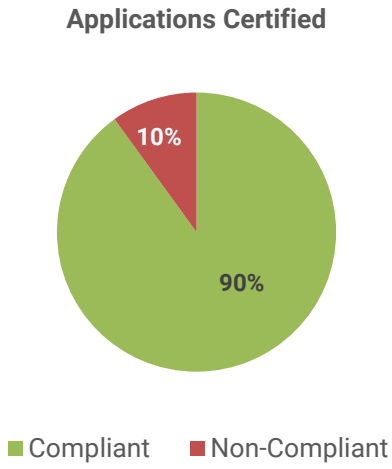
Business Impact Analysis (BIA) metrics increased. The information documented in BIAs are a primary input to data and application sensitivity, risk assessments, contingency plans, and system security plans. The percentage of completed BIAs increased 7% from the previous year. This indicated that agencies have improved in this area. This improvement was achieved by increased attention on addressing this key metric.





BIA completion increased by 7%

The majority of agencies have all their applications certified. Our analysis found that 90% of agencies had all their applications certified in 2021. Certifying applications shows an agency's intent to make sure all information regarding the applications is complete. This includes associating each application with a business process, data set and a device. Additionally, there can be no conflicts in sensitivity ratings between applications, business processes and devices.



Risk Assessment Findings Analysis

Agency risk assessments generate findings which require quarterly updates. In 2021, there were 496 new risk assessment findings compared to 381 new findings created in the previous year. However, analysis indicates that remediation of risk findings dropped significantly. 343 findings were remediated in 2020, but only 214 in 2021. As of the end of calendar year 2021, there were still 2162 risk findings requiring remediation (Figure 22).

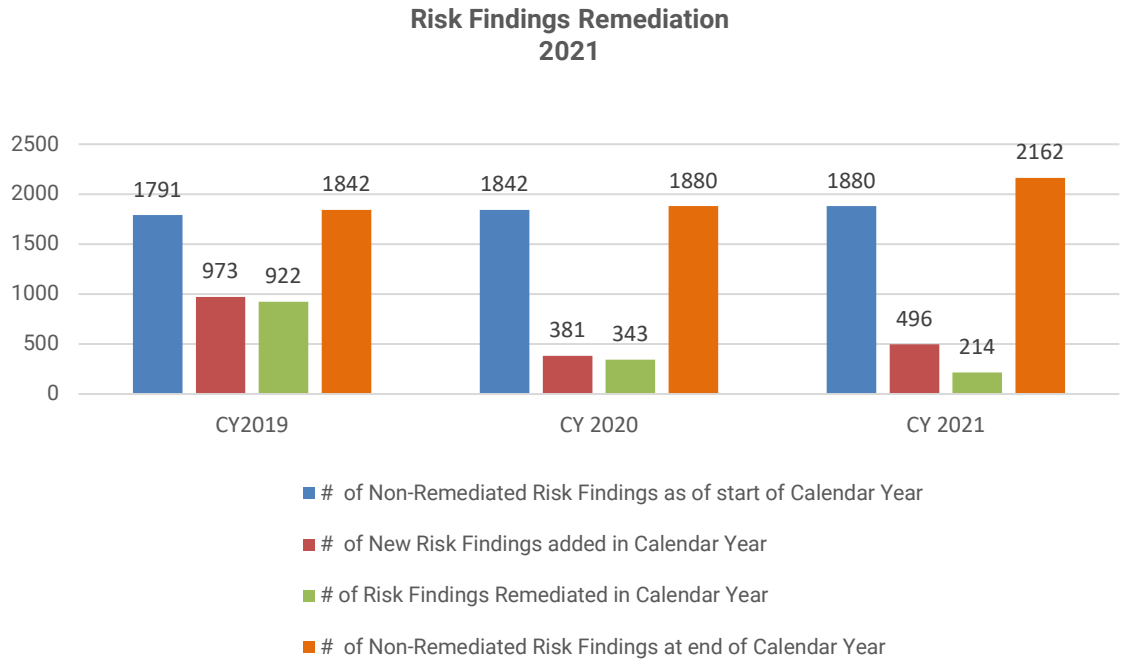


Figure 19: Risk Findings Remediation

Risk findings are not quickly addressed. CSRM analyzed the average number of days to it took to close risk assessment findings in 2021. Closed risk assessment findings were open an average of 382 days before being resolved and closed (Figure 20). The average number of days to close findings associated with CIS controls, key controls that protect against attacks from known attack vectors, were open an average of 433 days. While risk findings were closed more quickly than audit findings, improvement is still needed.

CSRM recommends agencies dedicate additional resources to address the issues identified in audit and risk findings to ensure audit and risk findings are resolved in a timelier manner. CSRM requires agencies to file an exception for any risk findings exceeding 90 days. Agencies should continue to prioritize and remediate findings by criticality, first addressing the findings in any areas associated with critical controls.

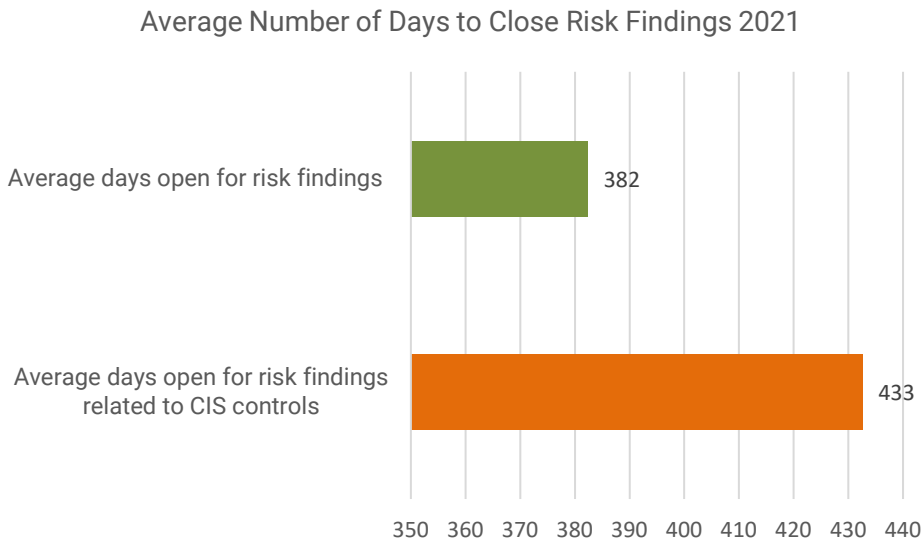


Figure 20: Closing Risk Findings

CSRM analyzed risk findings, which are the result of risk assessments performed by the agencies to identify potential threats to the confidentiality, integrity, and availability of an IT system. The results are organized by IT security control family (Figure 21). The top three security families that had the most IT risk findings were:

- Access control family (21%)
- Audit and accountability family (8%)
- System and services acquisition family (8%)

Poor access controls create an increased risk that agencies are exposed to unauthorized access of data, fraud, or disruption of IT services. VITA is working with the administration regarding implementing an identity access management (IAM) solution for the Commonwealth that will address this issue. IAM will create an automated framework for policies and technologies to ensure that users are properly authorized and have appropriate access to technology resources.

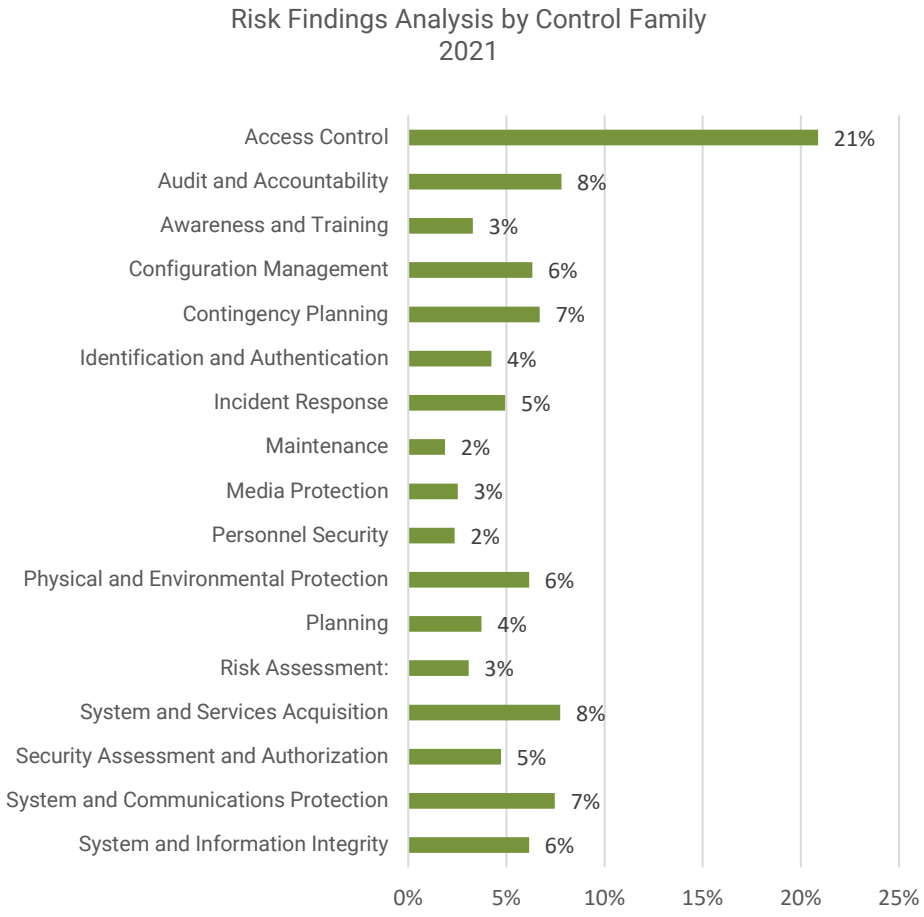


Figure 21: Risk Findings by Control Family

Commonwealth Centralized Security Services

To enhance agency IT security programs, CSRM offers a shared centralized service. These services include IT security auditing, ISO (Information Security Officer) support, and web application vulnerability scanning programs. IT security auditing and ISO support services are optional programs that agencies can acquire based on their security 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 improve information security and compliance in the Commonwealth.

Centralized IT security audit services

In the past, many agencies did not perform required IT security audits because they did not have their own IT auditing departments or did not have funds to hire outside auditing resources. The centralized IT auditing service assists these agencies with documenting their IT security audit plans, conducting IT security audits, and supporting agency efforts to create and submit corrective action plans to address the issues found during audits. Currently, 34 agencies have elected to use the shared centralized audit service to perform IT security audits. The average audit score for agencies that have centralized audit services is a B (80%), a 7% decrease from 2020 (Figure 14).

Despite the decrease in the overall audit score, agencies utilizing centralized audit services are outperforming agencies that are not using the service by 16%. Auditing is a valuable tool that detects issues and helps agencies strengthen their overall security posture.

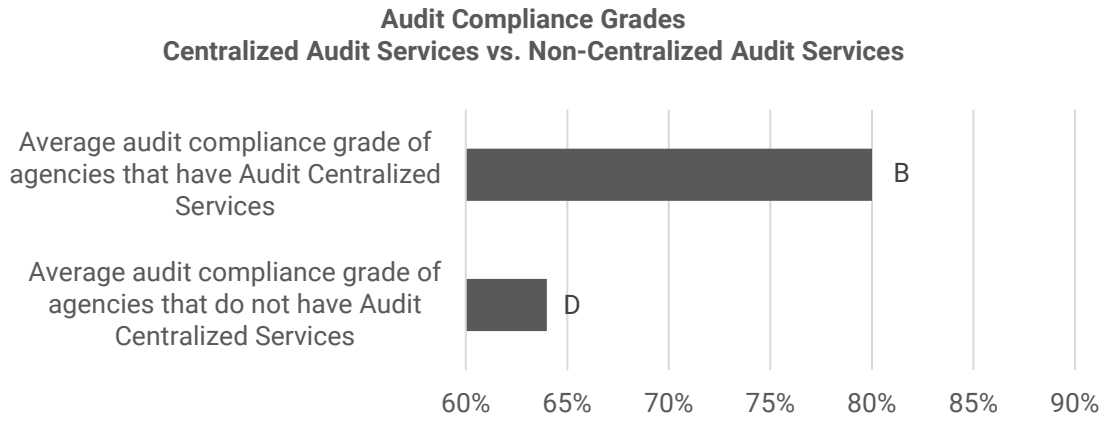


Figure 22: Audit Compliance Grades Comparison

Centralized ISO Services

The centralized ISO service currently supports 36 customer agencies. This service 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 score for agencies utilizing ISO centralized services is a B (80%), a 7% decrease from 2020. The average risk score for agencies not utilizing ISO centralized services is a C (75%), a 1% decrease from 2020 (Figure 15). Agencies utilizing ISO centralized services are outperforming the average risk score for agencies not utilizing ISO centralized services by 5%. Despite the decrease in the risk score for agencies utilizing ISO centralized services, ISO centralized services anticipates improvements in risk compliance.

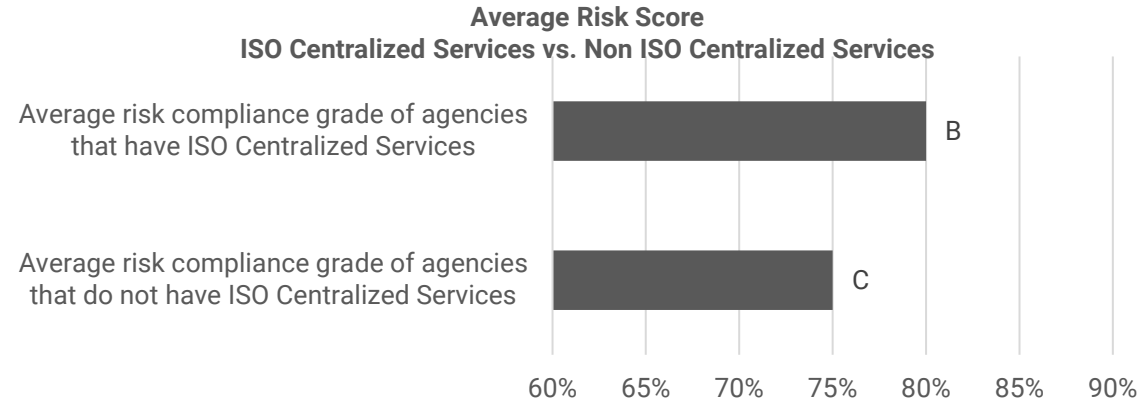


Figure 23: Risk Score Compliance Grades Comparison

Web application vulnerability scanning program

The web application vulnerability scanning program provides automated scans of Commonwealth public facing websites to identify potential security weaknesses that the agencies can address to prevent attacks. CSRM performs over 6,000 scans of public sites and private sensitive sites each year.

In 2020, VITA updated requirements in the IT Risk Management Standard regarding vulnerability scans. Agencies are now required to remediate vulnerabilities that are rated critical or high within 30-days for publicly facing systems and within 90-days for systems hosted on the agency's internal network in accordance with an organizational assessment of risk. CSRM anticipates this requirement will further ensure that significant vulnerabilities are addressed timely to protect Commonwealth data.

In 2021, there was over 6000 active findings, of which 4,169 were still open from previous years. As the chart below shows, each year agencies are falling behind with remediating findings. In tracking findings since the inception of the program, the closure rate hit an all-time low of 5% and an outstanding rate of 95% (Figure 24).

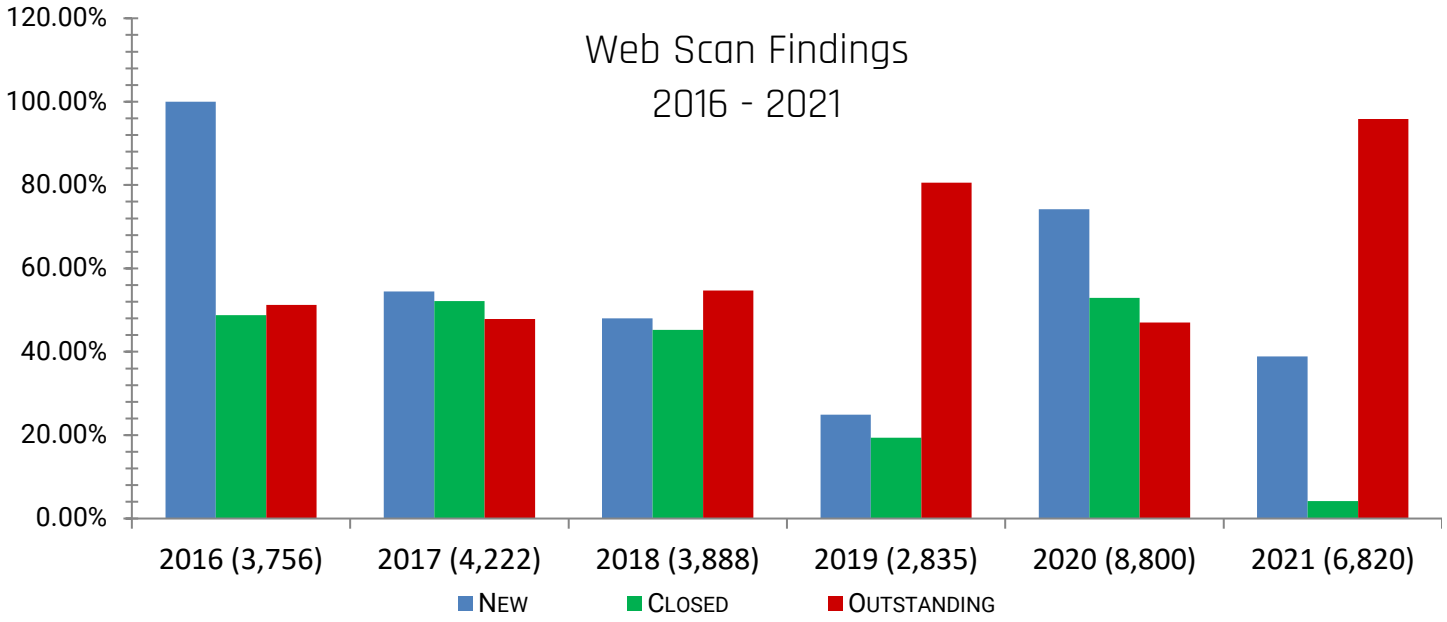


Figure 24: Web Scan Vulnerabilities

Nationwide Cyber Security Review

Annually, the Commonwealth participates in the **National Cyber Security Review (NCSR)** sponsored by the MS-ISAC. The NCSR is a self-assessment survey aligned within the **NIST cybersecurity framework (CSF)** to evaluate an agency's cybersecurity posture. The survey is distributed to government agencies in all states, localities, tribal nations, and US territories. Nationally the survey has a very high participation rate, and the cumulated results are reported bi-annually to the US Congress.

The NCSR provides significant insight into IT security practices at each agency by identifying gaps in performance areas that allow us to benchmark year-to-year progress. In addition, it gives a way to measure and compare the Commonwealth against other peer survey participants across the nation.

Each agency participating in the survey, ranked their compliance for five core cybersecurity functions: *identify, protect, detect, respond, and recover*.

> ***Identify*:** The activities measured for this function are key for an agency's understanding of their internal culture, infrastructure, and risk tolerance.
>
> ***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.
>
> ***Detect*:** The quicker an agency can 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 organization's ability to identify incidents.
>
> ***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.
>
> ***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.

Using the NCSR measurements, each agency evaluates itself on several activities that support each core function. The scale is heavily policy focused and goes from a low score of one (activity is not performed, i.e., no processes, policies or technologies are in place) to a high score of seven (activity is optimized, i.e., policies and procedures are formally documented, implemented, tested, and continuously monitored for effectiveness). NCSR recommends a *minimum* compliance level score of five.

NSCR Scoring		
Score	**The recommended minimum 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.
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.

The survey requires agencies to evaluate their processes and controls using the scoring described in the table above. On average, participating Commonwealth agencies rank themselves close to the recommended minimum level score (of five) in all core cybersecurity functions. In addition, Commonwealth agencies assessed themselves slightly above the national average of all peer states. The average score for all five of the measured functions for the Commonwealth was 5.25 in 2020 and decreased slightly to 5.15 in 2021. The average score for all five functions for other participating peer states in the national survey was 4.88 (in 2020, which is the most recently available data).

Commonwealth results declined slightly from 2020 to 2021. Self-assessment scores for all COV agencies were slightly lower in 2021 compared to the 2020 scores. This could be due to the increase in the number of participating Commonwealth agencies. For the agencies that participated, the "Protect" function is consistently rated as most

developed function (at 5.52 in 2020; 5.6 in 2021). The "Recover" function is the least developed function (at 5.04 in 2020), but the "Respond" function was rated slightly lower in the most recent survey (4.96 in 2021) (Figure 25). Commonwealth agency results exceeded the recommended minimum level score of 5 for all measured functions except the Respond function which was just a below 5. A score of 5 means the agency believes that "Implementation in process" for the measured function. Almost all Commonwealth agencies have reported they are usually in the scoring range of 5.

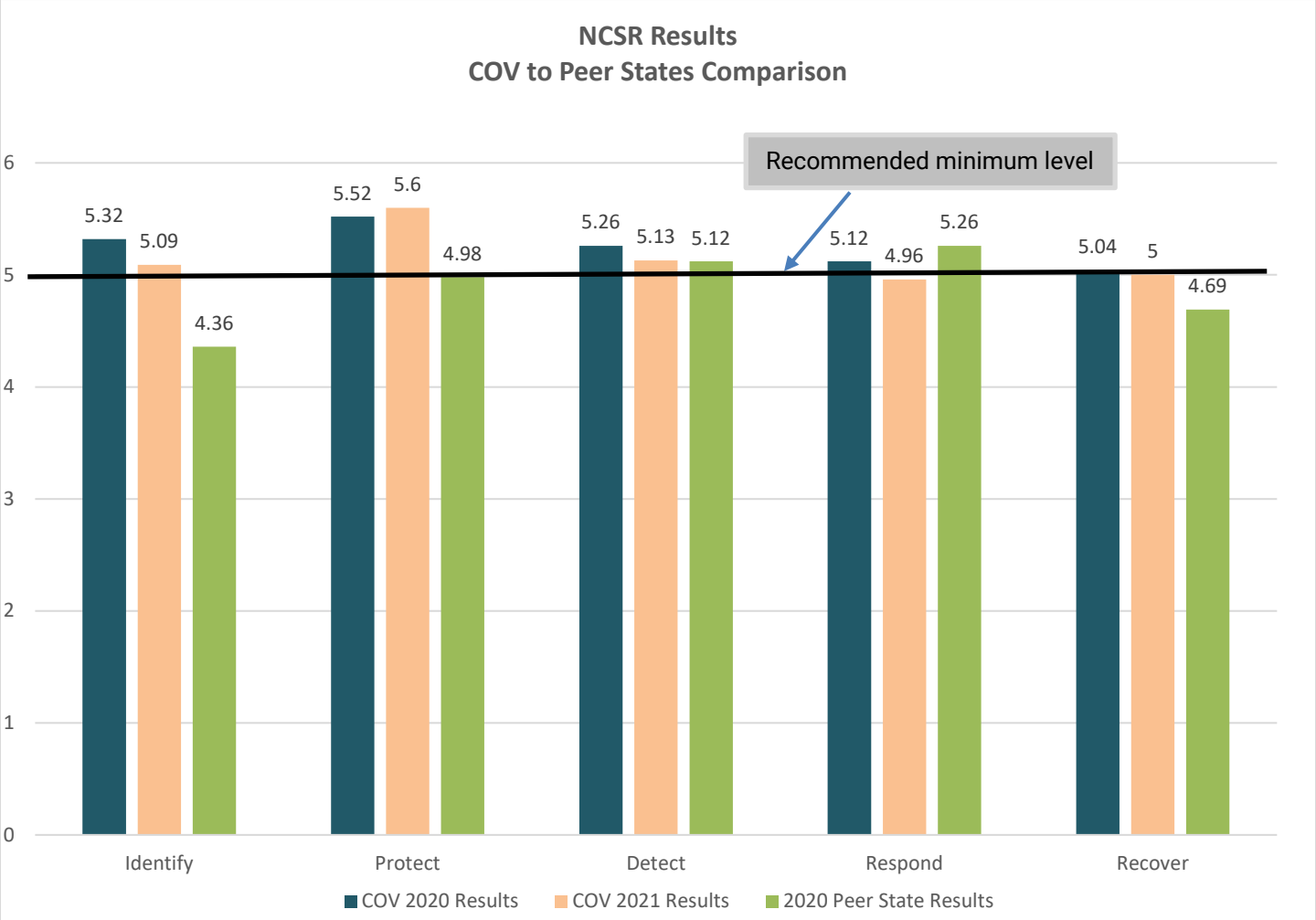


Figure 25: NCSR COV to Peer States Comparison

Over the last three years of tracking NCSR results for Commonwealth agencies we have experienced an overall average score of 5.06, slightly above the recommended minimally acceptable score (Figure 26).

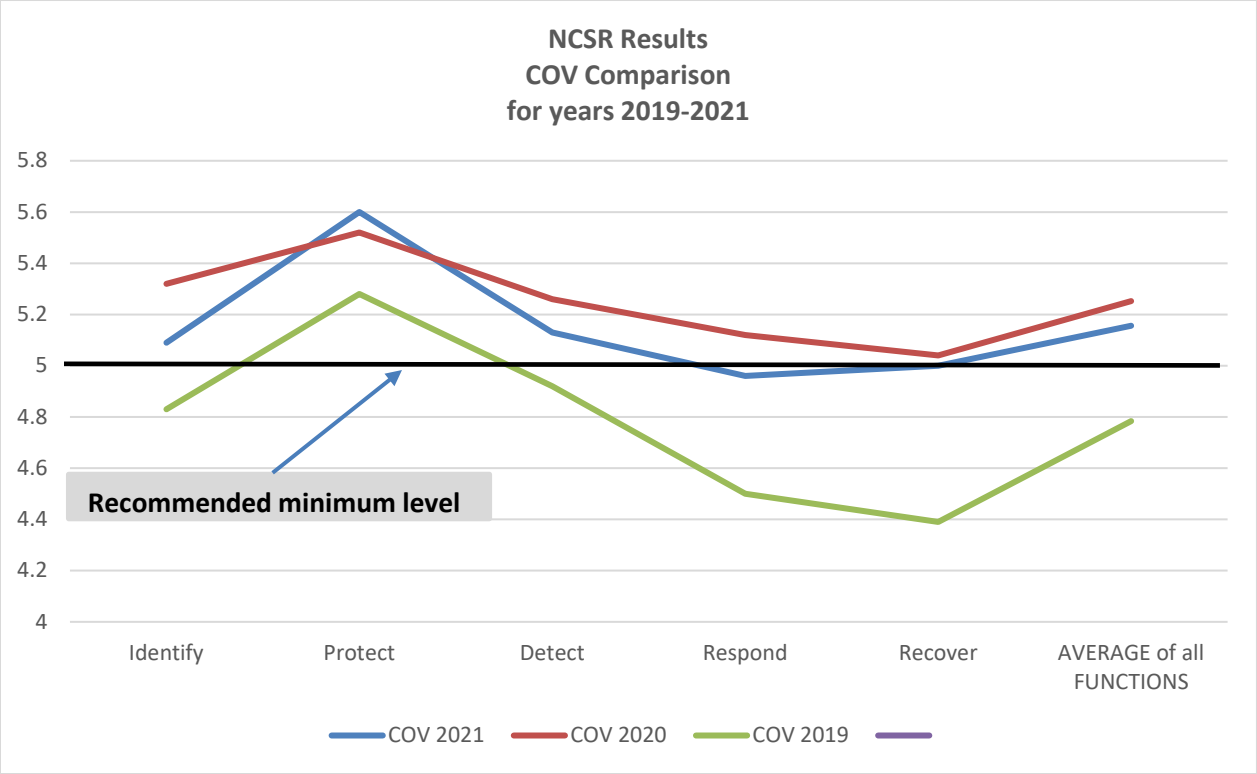


Figure 26: NCSR COV by Year

The chart below (Figure 27) shows the distribution of scoring for all 50 states in the US. Overall, 23 of 50 states (46% in total) scored at or above the recommended minimum level of five (5). The remaining 27 states (54%) scored below the recommended level of five (5). The average score for all Commonwealth agencies of is 5.2 (Implementation in process), putting the Commonwealth at the approximate scoring level of 18 other states.

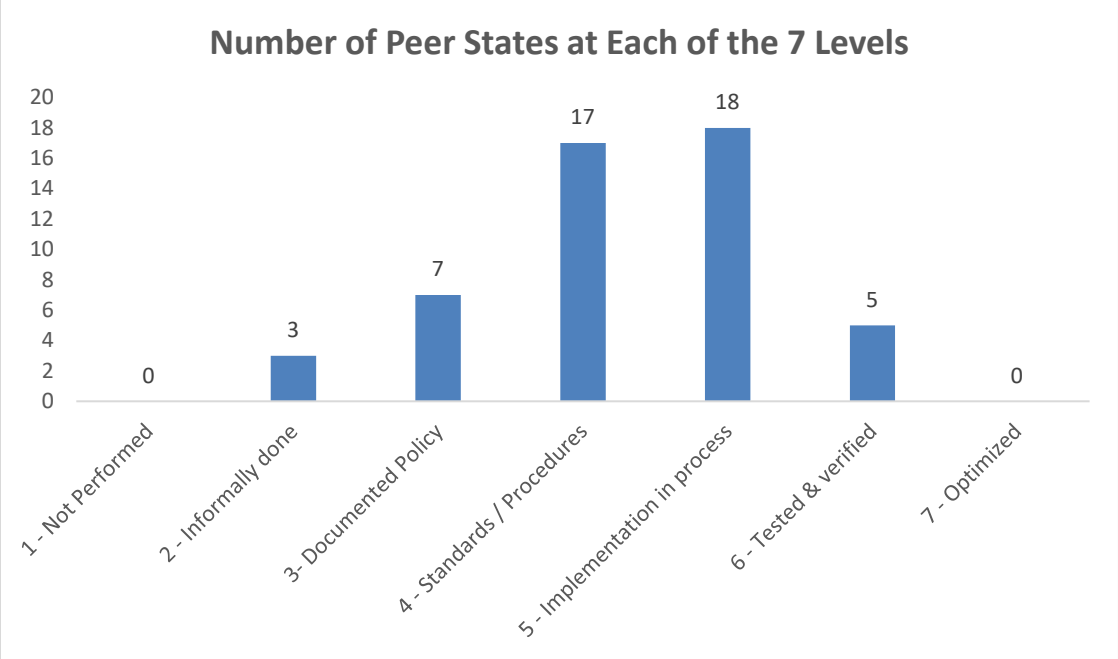


Figure 27: Peer States Level Distribution

Commonwealth agencies compared well with their peer state agencies. MS-ISAC grouped all nationally participating agencies into peer group subsectors by government service/business function. CSRM combined COV agencies into

similar subsector groups to compare. The results demonstrate that Commonwealth subsectors self-reported levels slightly higher on average than our peer state subsectors. Commonwealth agencies in most sub-sectors rated themselves the higher compared to their peers (Figure 28).

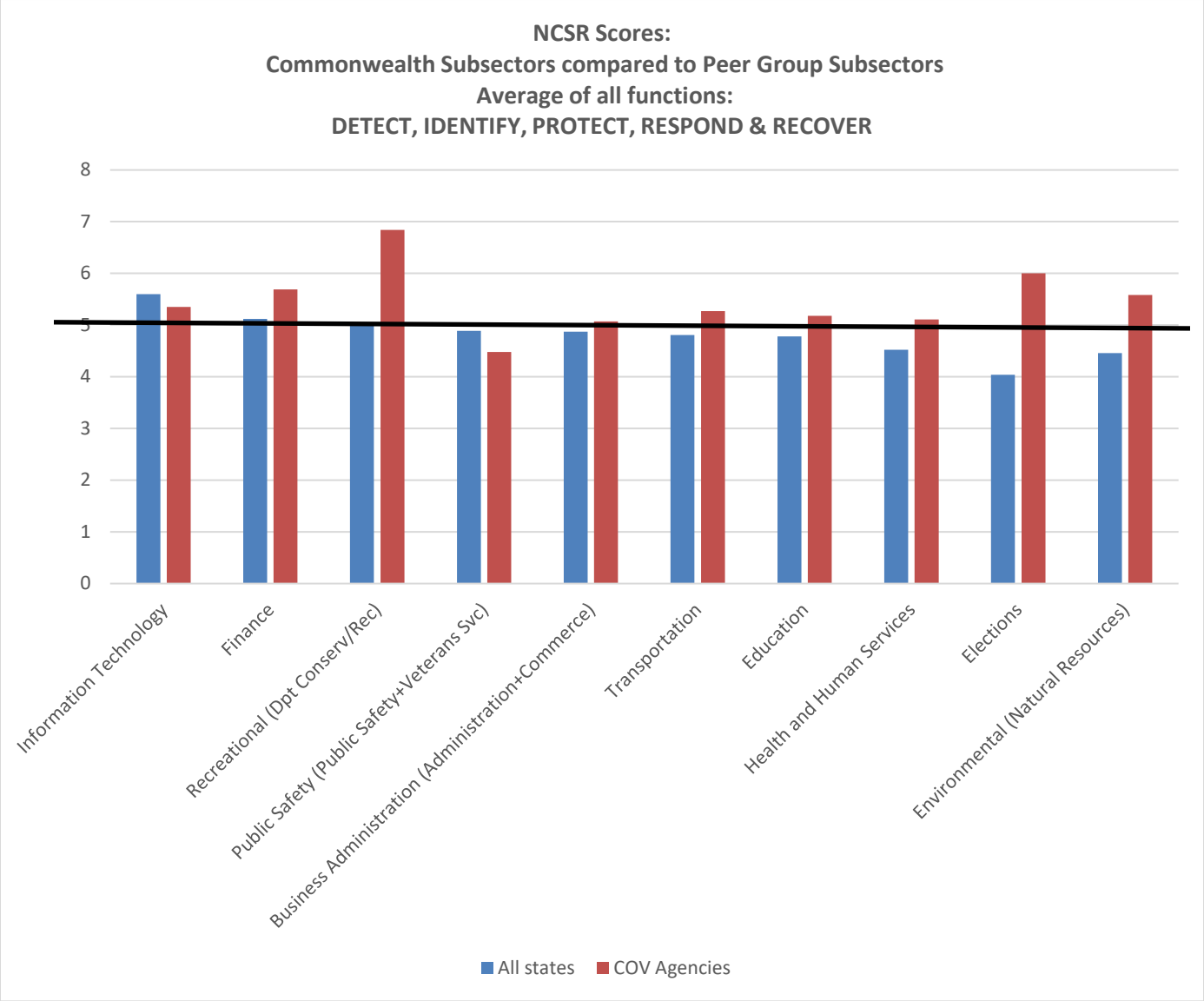


Figure 28: NCSR Scores for COV to Peer Group Subsectors

Commonwealth secretariats are showing overall improvement. Analysis of all NCSR self-assessments by Commonwealth secretariats shows that eleven secretariats are rating themselves higher than the minimum recommended level of five (implementation in process). Two of those secretariats are nearly at or above level six (tested and verified). Nine other secretariats are performing in the level five range (implementation in process).

NCSR analysis by secretariat

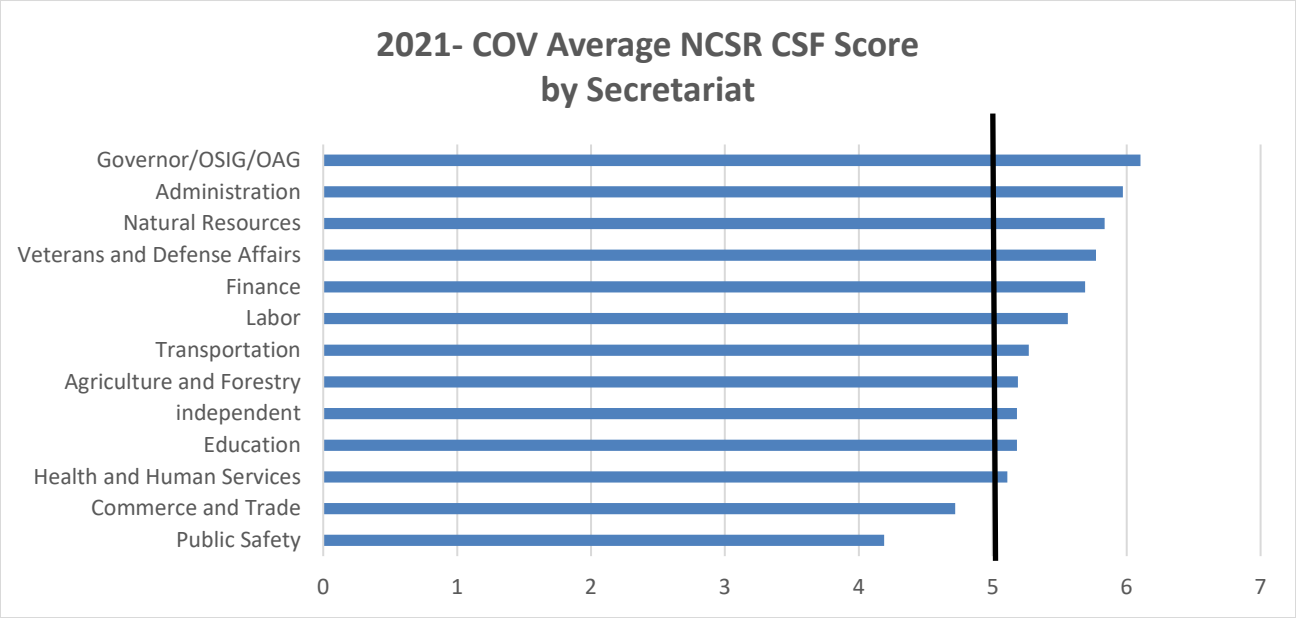


Figure 29: NCSR Scores by Secretariat

Cybersecurity framework – analysis by function

Identify

The activities under the "Identify" functional area are key for an agency's understanding of their current internal culture, infrastructure, and risk tolerance. Underdeveloped 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.

There are several categories in the Identify function:

"Asset Management" is the data, personnel, devices, system, and facilities that enable the organization to achieve business purposes. Assets must be identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

The "Business Environment" category is related to how the organization's missions, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

"Governance" is related to the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

"Risk Assessment" describes how the organization understands the cybersecurity risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

"Risk Management Strategy", the least developed category in the identify function, describes how the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. This may indicate that additional resources to assist with formal risk management assessments could be beneficial to Commonwealth agencies.

Lastly, "Supply Chain Risk Management" relates to how the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support supply chain decisions.

In 2019, Commonwealth agencies scored an average of 4.86 for the categories in the Identity function. Identify function category scores improved to 5.31 in 2020 and then declined in 2021 to 5.08 (Figure 30).

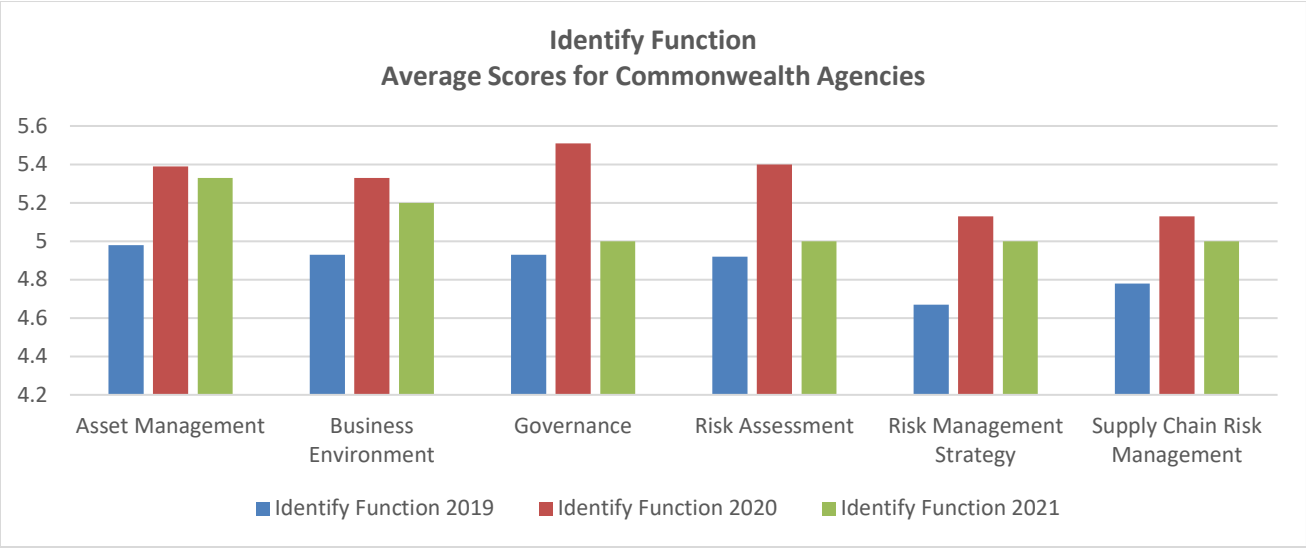


Figure 30: Identify Function Scores

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.

The Categories in the Protect function are:

- "Access Control" describes how access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- "Awareness and Training" designates how the organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security related duties and responsibilities.
- "Data Security," the highest scoring category for the Commonwealth in the Protect function, refers to the idea that information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- "Information Protection Processes and Procedures" describes how the security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
- "Maintenance" is related to the maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
- "Protective technology," which 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, is the lowest scoring category in the protect function. This indicates that agencies may need more guidance regarding best practices for ensuring that technical security solutions are managed correctly.

Average scoring for Commonwealth agencies in the overall Protect function metric showed a slight improvement from 5.31 in 2019 to 5.51 in 2020 and to 5.6 in 2021 (Figure 31).

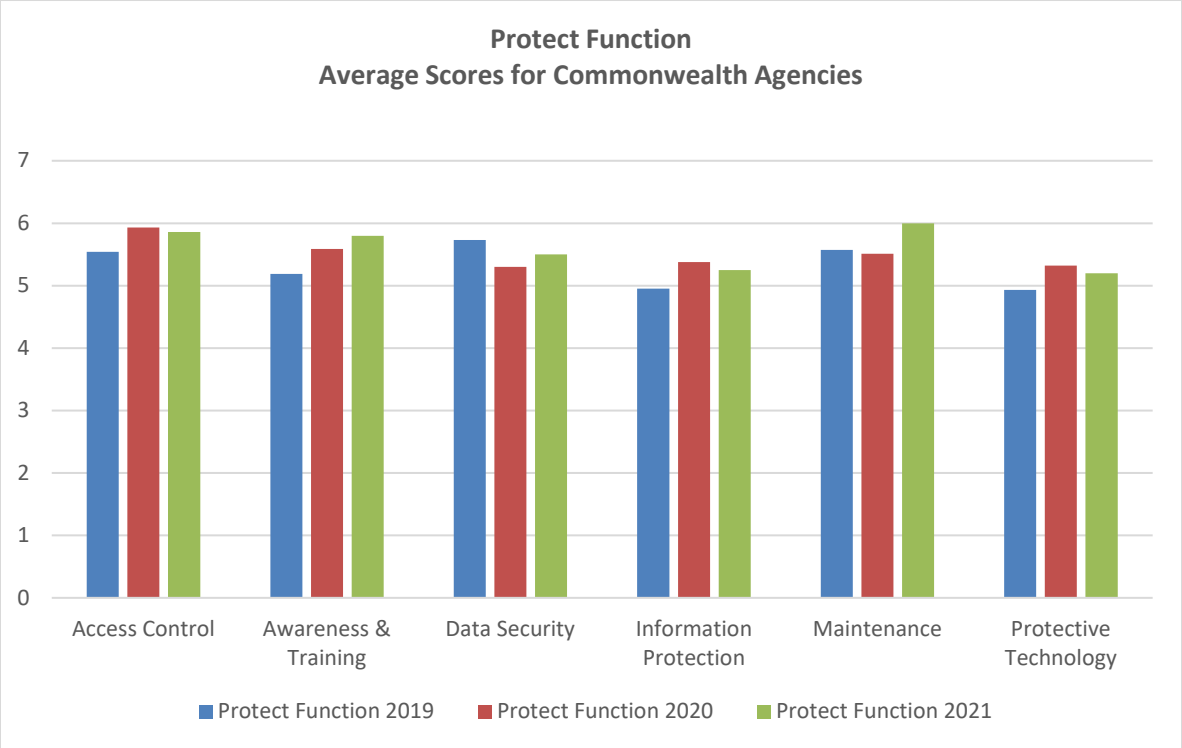


Figure 31: Protect Function Scores

Detect

Activities contained with the detect function are related to the agency's ability to identify incidents. Rapidly detecting a cybersecurity incident puts an agency in the best position to remediate the issue and mitigate the consequences of the incident. The importance of this control should not be underestimated because of the growing and overwhelming number of logs and events that agencies handle. The sheer volume of logged information makes it difficult to analyze and identify indicators of an occurrence in a timely manner. Agencies must dedicate adequate resources in terms of tools and personnel to monitor logs efficiently and effectively.

Within the Detect function, are the following categories:

- "Anomalies and Events" measures capabilities related to detecting anomalous activity and understanding the potential impact of events that are detected.
- "Continuous Monitoring" measures the capability to monitor systems and assets to identify cybersecurity events and verify the effectiveness of protective measures.
- "Detection Processes" and procedures are maintained and tested to ensure timely and adequate awareness of unusual events.

Measurements in the Detect function have decreased slightly moving from 2020 to 2021 (Figure 32).

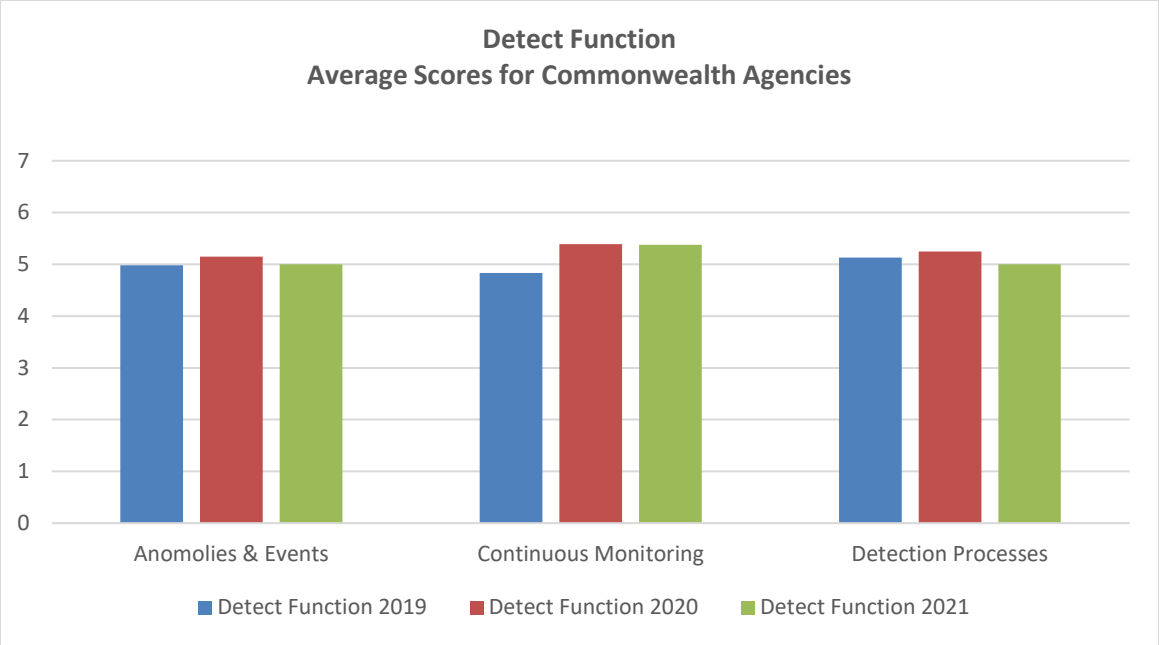


Figure 32: Detect Function Scores

Respond

An agency can affect the magnitude of the impact of an incident if the agency can respond effectively and efficiently when an incident occurs. 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.

Categories in the Respond function are:

- The "Analysis" category is conducted to ensure adequate response to support recovery activities.
- The "Communications" category involves communication activities that are coordinated with internal/external stakeholders.
- "Improvements" describes organizational response activities that can be improved by coordinating lessons learned.
- "Mitigation" describes the activities performed to prevent the expansion of an event, mitigate its effects, and eradicate the incident.
- "Response Planning" are the various procedures that are executed and maintained, to ensure timely response to detected security events.

Commonwealth agencies have usually scored themselves the lowest on the Respond function in the last few NCSR surveys. The average Commonwealth score in 2019 was only 4.6. In 2020, the average score went up to 5.12, but in 2021, it then dropped below 5 again to 4.96 (Figure 33). CSRM recommends that agencies allocate more time to develop effective communication response plans related to incidents. In addition, agencies should develop policies to properly document and analyze lessons learned following incidents and incident response exercises. Finally, response strategies should be updated, if necessary, following incidents and exercises.

.

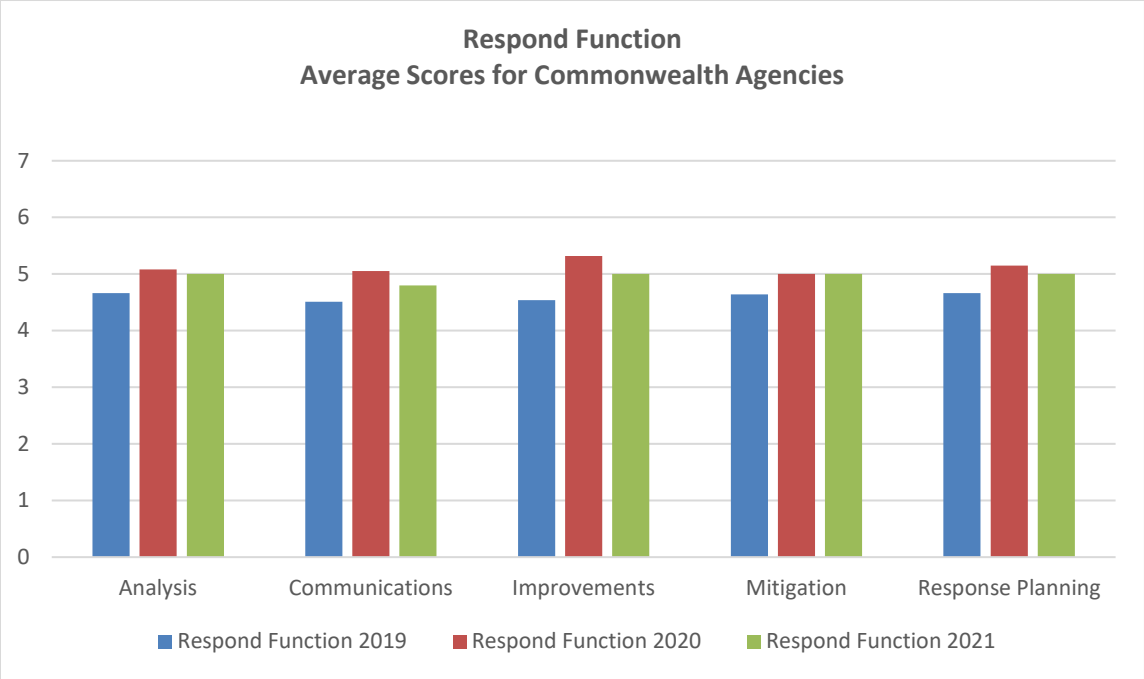


Figure 33: Respond Function Scores

Recover

The recover function pertains to an agency's ability to return to its baseline after an incident has occurred. These 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.

The Recover function is comprised of these categories:

- The "Communications" category relates to coordination with internal and external parties during a security event.
- "Improvements" describes the processes related to incorporating lessons learned from handling IT security incidents into improving recovery planning and processes.
- "Recovery Planning" describes processes and procedures that are executed to ensure timely restoration of systems affected by cybersecurity events.

Commonwealth agencies improved slightly in this function. Average score in 2019 was 4.47. It was 5.03 in 2020, and 5.00 in 2021 (Figure 34). So, most agencies are reporting that implementation is in process for all three categories of the Recover function.

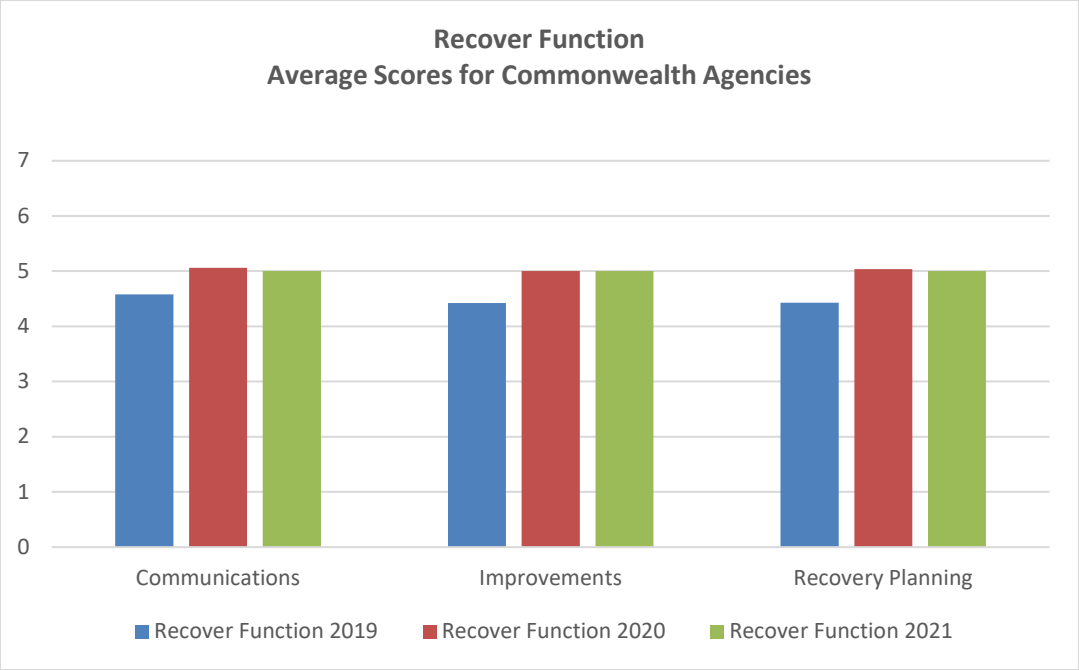


Figure 34: Recovery Function Scores

NCSR survey demographic analysis

Commonwealth agencies were surveyed as to the number of full-time equivalent (FTE) personnel who were on staff (Figure 35).

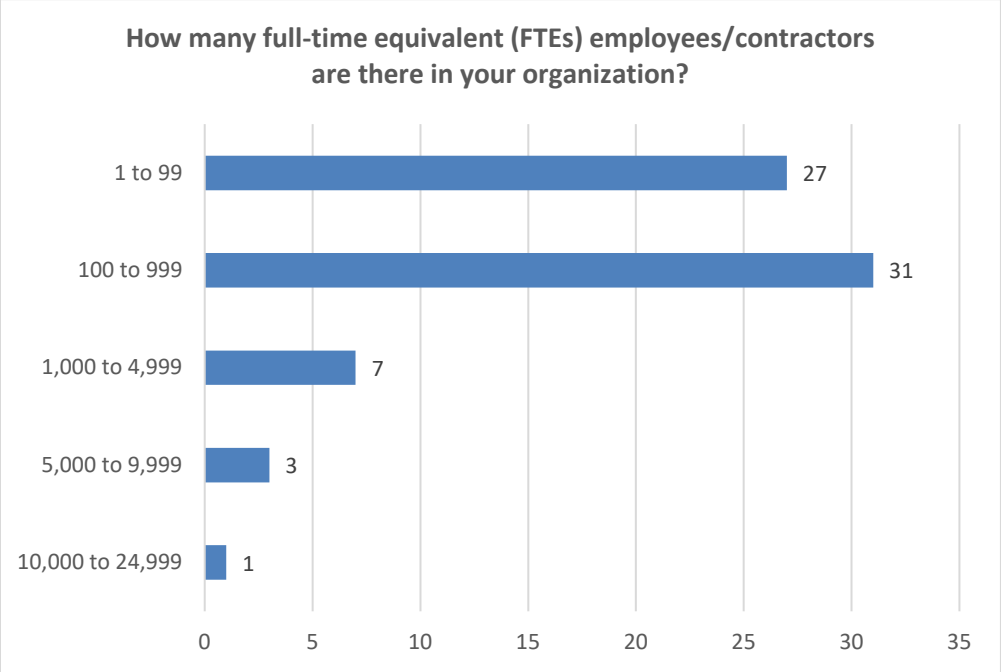


Figure 35: Demographic: # FTE

Agencies with fewer than 1000 full-time equivalents averaged 5.38 on the NCSR. Larger agencies with over 1000 FTEs averaged 4.37 (Figure 36).

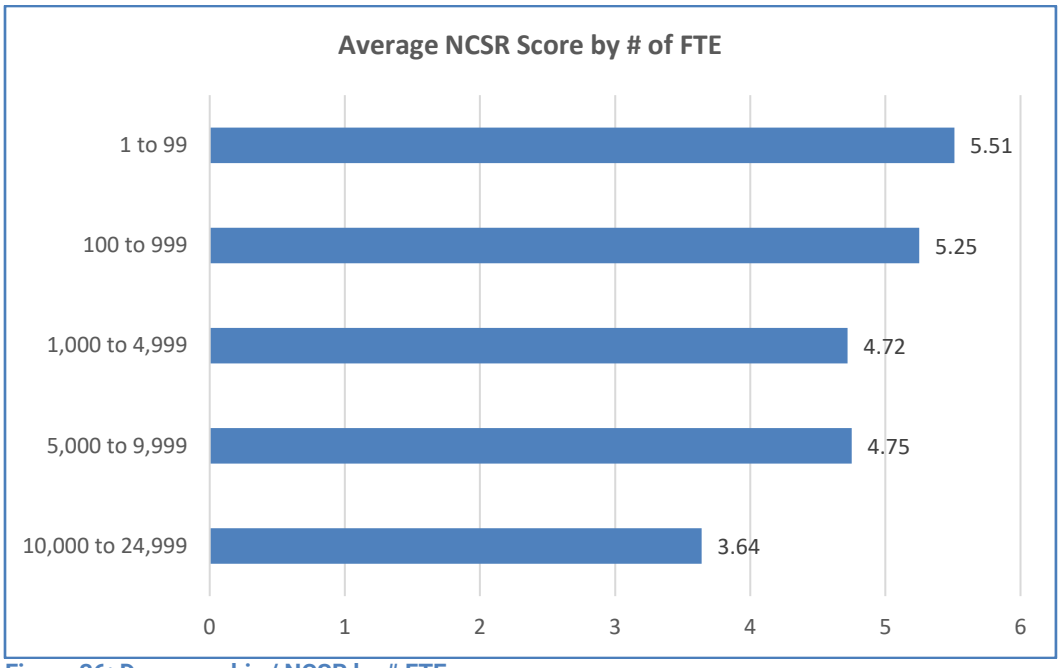


Figure 36: Demographic / NCSR by # FTE

Agencies were also surveyed as to the number of full-time employees whose primary job responsibility is in information technology. The majority of agencies reported that they have less than 24 employees working in the IT area (Figure 37).

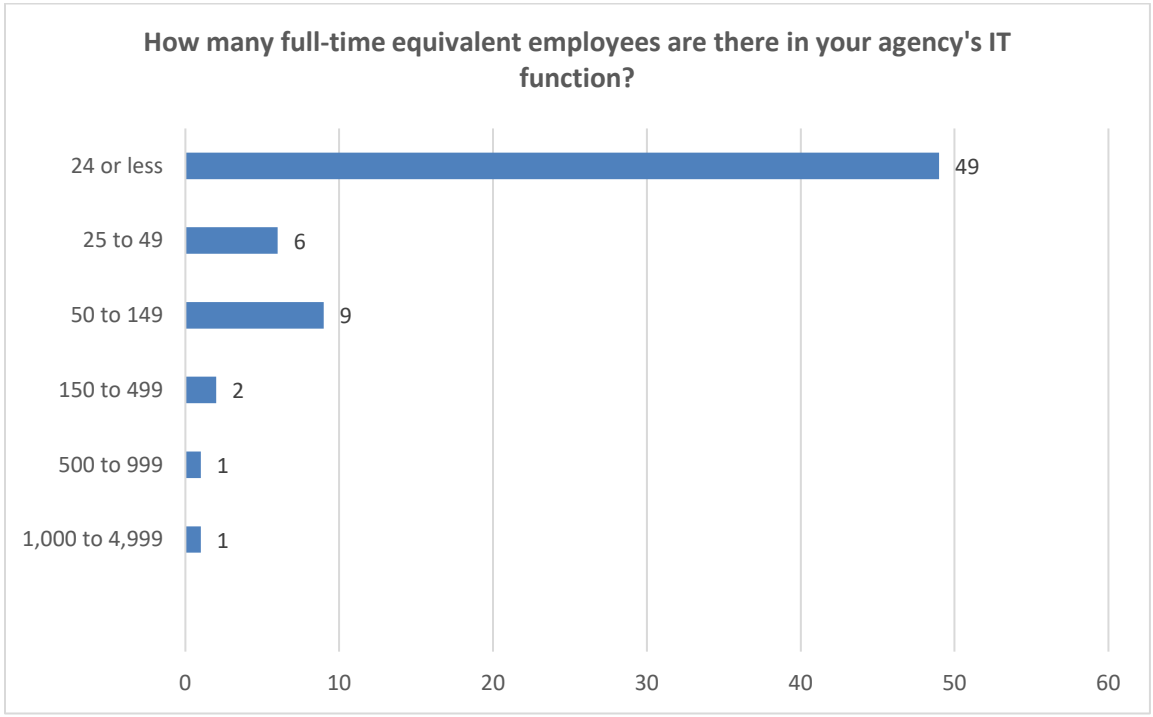


Figure 37: Demographic: # of FTE in Info Technology

We then calculated the average NCSR score based on the number of IT employees reported by Commonwealth agencies. Agencies with fewer than 50 full-time equivalents working in IT averaged 5.23 on the NCSR. Agencies with 50 or over FTEs in IT averaged 5.04 (Figure 38).

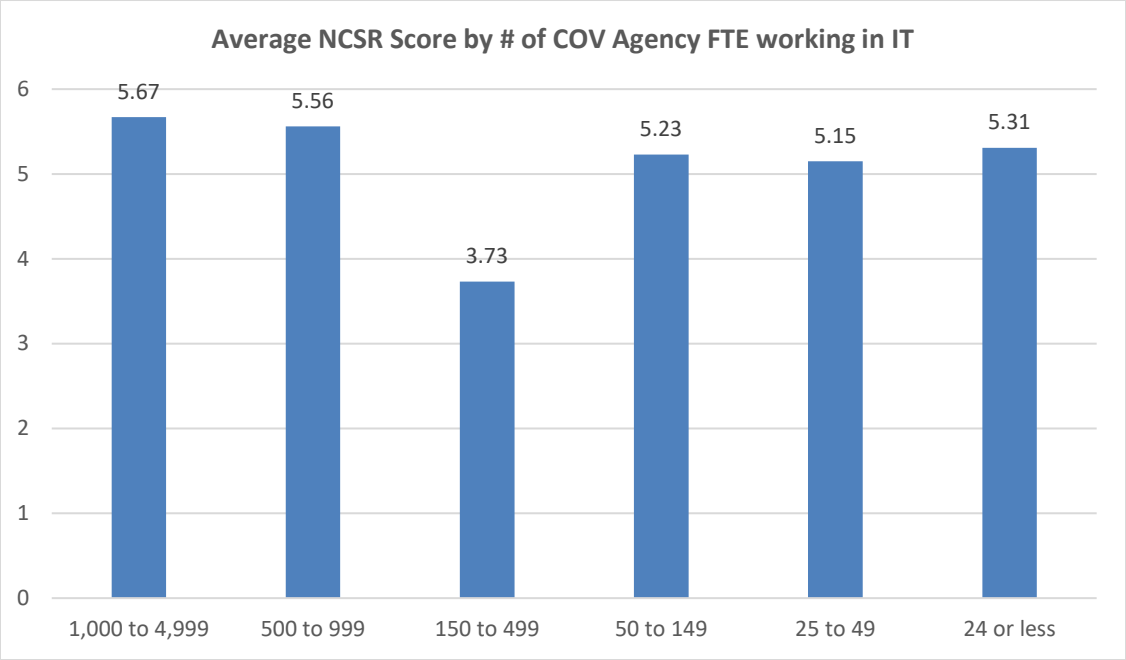


Figure 38: Demographic: NCSR Scores by #FTE in IT

Finally, agencies were asked how many of their employees have IT security related duties. The majority of agencies indicated that there are fewer than five people working with IT security duties (Figure 39).

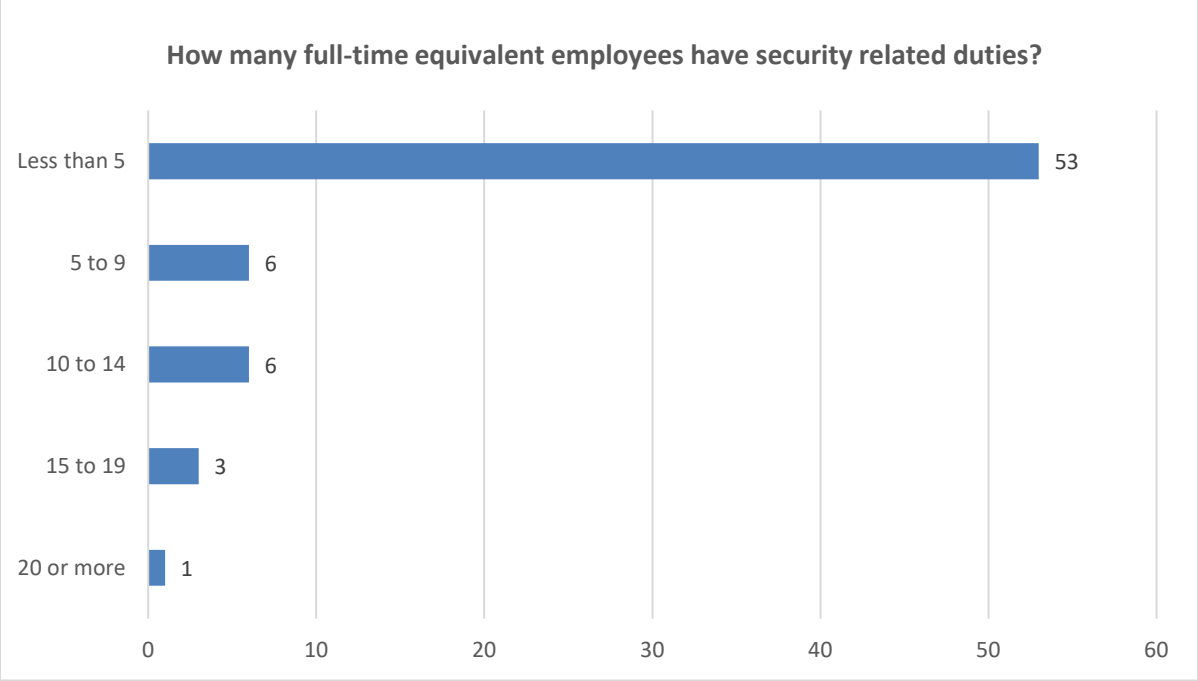


Figure 39: Demographic: # FTE in IT Security

We then reviewed the NCSR scores based on the number of employees working with IT security roles. Agencies with fewer than 5 employees working full-time in IT security scored 5.35 on the NCSR. Agencies with 5 or more employees working in IT security scored an average of 4.71 on the NCSR (Figure 40). No agencies reported that they had zero employees with IT security related duties.

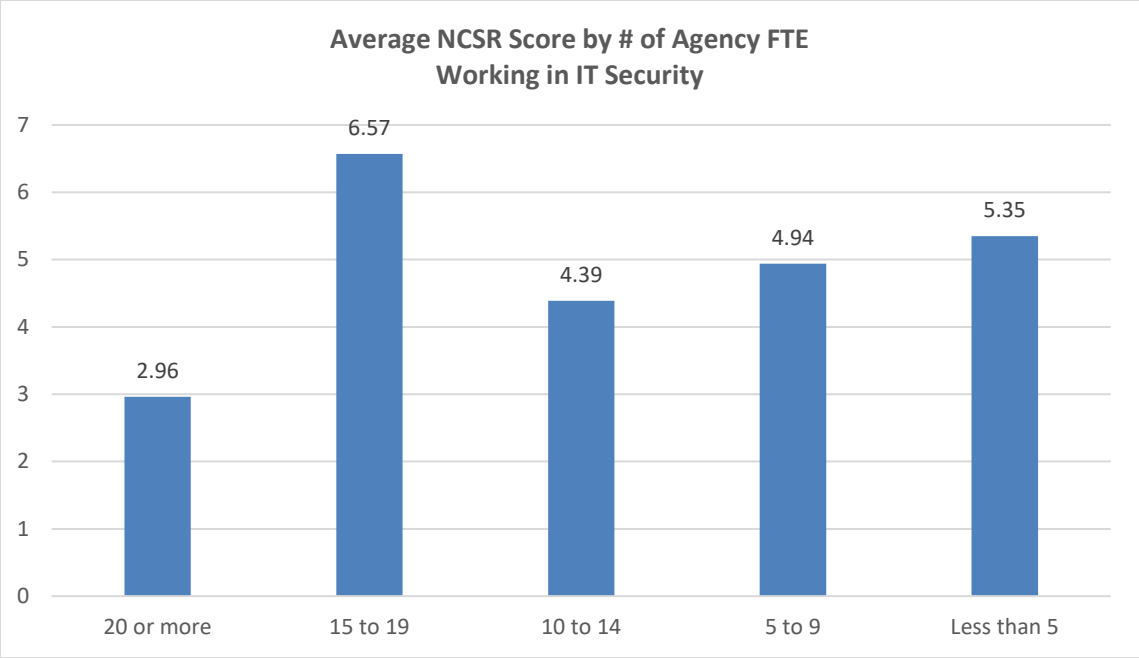


Figure 40: Demographic: NCSR Scores by #FTE in IT Security

Staffing totals key takeaways

- Smaller Commonwealth agencies with less than 1,000 total employees scored 10% higher than larger Commonwealth agencies on the NCSR.
- Agencies with 50 or more full-time persons working in IT scored essentially the same on the NCSR as agencies employing fewer than 50 people in IT.
- Interestingly, agencies with 20 or more employees with IT security roles scored the lowest on the NCSR survey.

Top five security concerns

Commonwealth agencies participating in the NCSR survey were asked to identify their top five IT security concerns. This year, as for the last few years, the top concern by far was a “Lack of Sufficient Funding”. 71% of all responses included “Lack of Sufficient Funding” as a top five concern. Figure 41 shows the five top concerns.

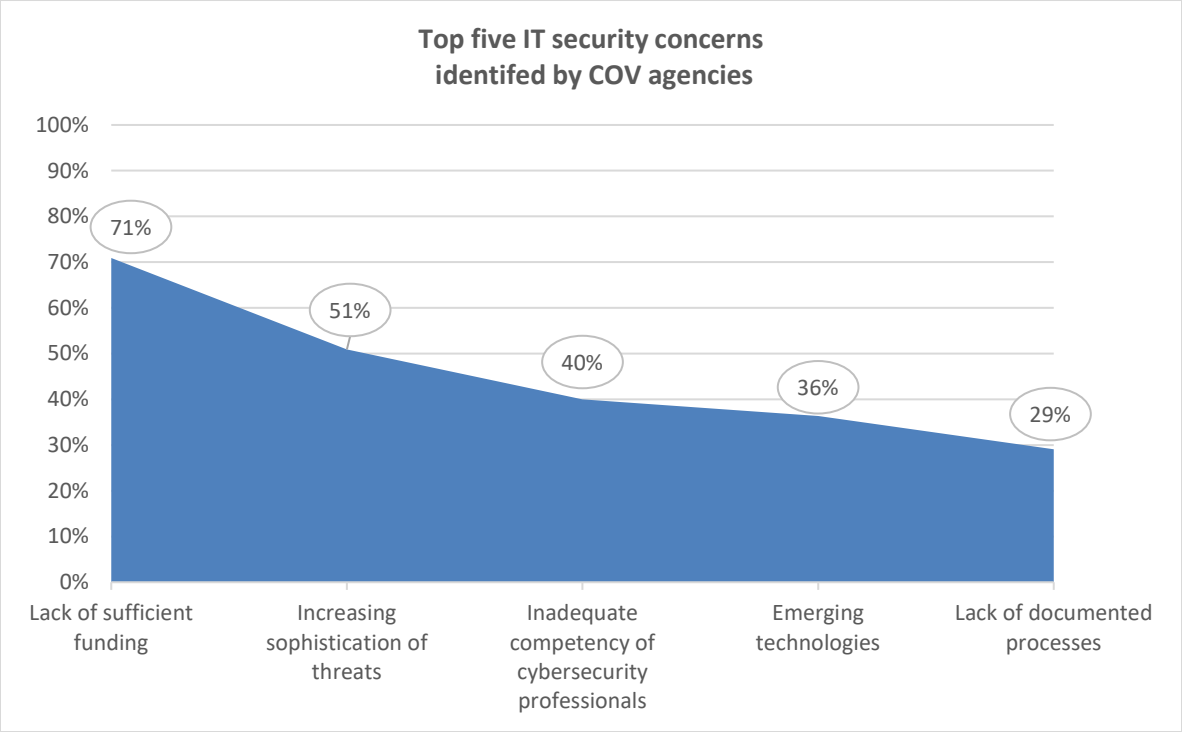


Figure 41: Top Five Security Concerns

NCSR Policy-Related Questions

The NCSR survey requires that each agency evaluate itself as it relates to over 100 questions in various IT security areas. Several policy-specific activities that support the core cybersecurity functions were analyzed to determine if the self-assessments identified any strengths or weaknesses.

Agencies rated themselves in the NCSR as to their progress in implementing *organizational cybersecurity policies*. An organizational cybersecurity policy is a key component in assuring that an agency's cybersecurity culture, infrastructure and risk tolerance has been documented and understood by its employees and contractors. More than half of the agencies indicated in their self-assessments that their organizational cybersecurity policy was either "optimized" (26%) or "tested and verified" (23%). Only 1% of agencies indicated that this was "Not performed" (Figure 42).

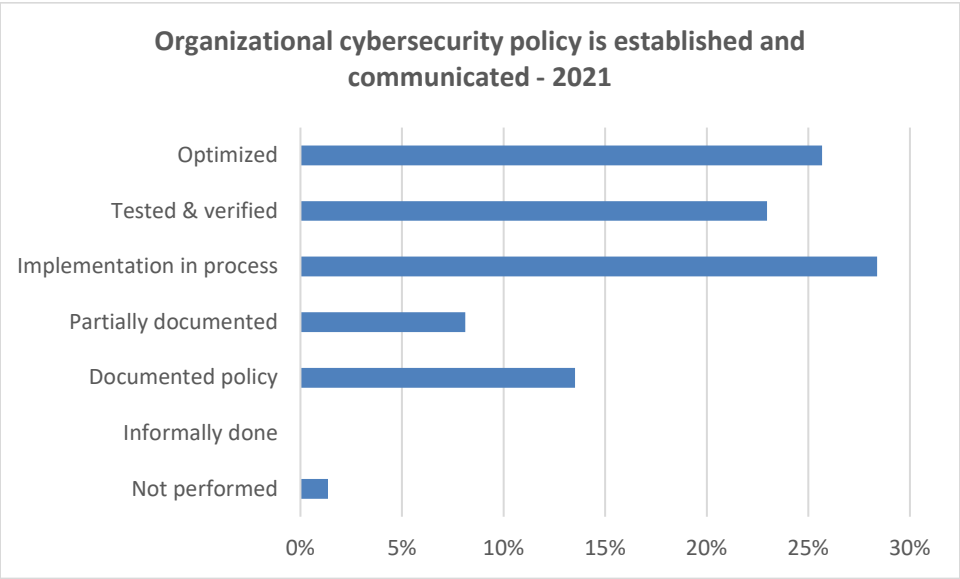


Figure 42: Organizational Cybersecurity Policy

Managing legal and regulatory requirements is important to assure that agencies are complying with all federal and state laws and other requirements. Overall, agencies scored themselves as performing very well in this area: 24% of the agencies considered themselves "optimized," and an additional 28% believe this area has been "tested and verified" (Figure 43).

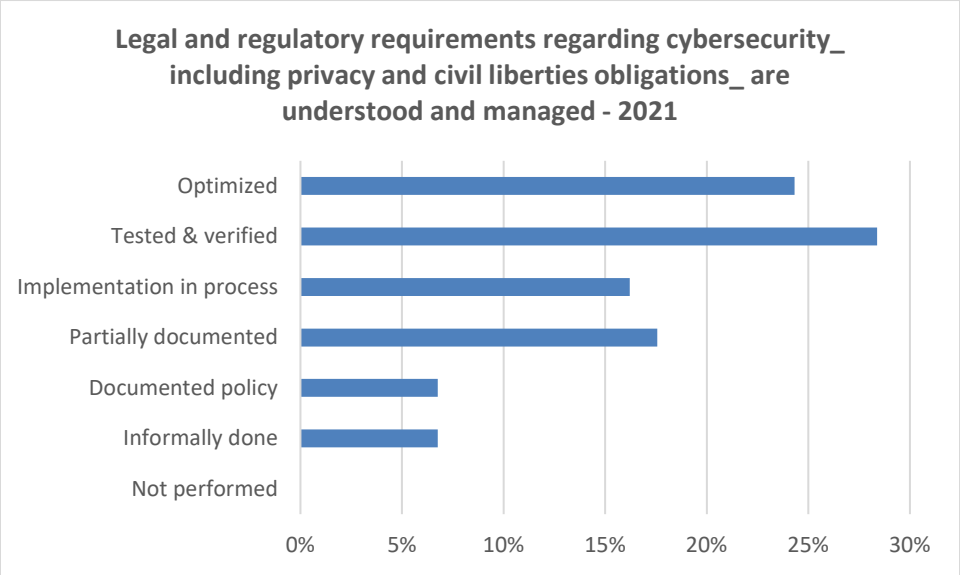


Figure 43: Legal & Regulatory Requirements

Policies for governance and risk management processes address cybersecurity risks so that any potential issues or gaps in performance are promptly identified and corrected. Overall, agencies scored themselves as performing well in this area (14% optimized and 21% tested and verified). In addition, 21% indicate that these processes are currently being implemented (Figure 44).

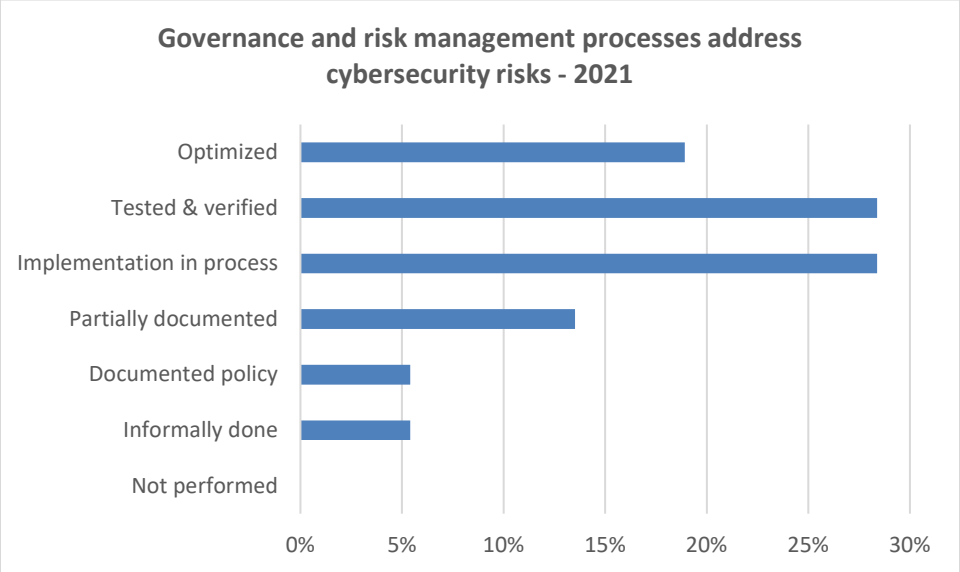


Figure 44: Governance and Risk Management

Summary of NCSR survey results

The NCSR evaluates cybersecurity progress as it relates to the Cyber Security Framework. In the Commonwealth, this information is used to benchmark between agencies, secretariats, and peer states. It also helps to identify strengths and opportunities for improvement. The federal government also uses this information for anonymous summary reporting to Congress providing a broad picture of the cybersecurity implementation across the country.

CSRM intends to address the concerns identified in the NCSR assessments in order of priority. Some of the immediate issues that were identified in this assessment were lack of sufficient funding to support IT security and lack of progress in the respond and recover functions. CSRM continues to champion the efforts to provide necessary funding for Commonwealth IT security programs. In addition, CSRM will continue to provide tools, templates and training to agencies that support all the cybersecurity framework functions and to strengthen the security for Commonwealth information.

Appendix I - 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 current security audit plan

Risk assessment plan status
Pass - Documents received as scheduled
N/C - Missing risk assessment plan

Three-year risk assessment obligation completed
X% - The percentage of risk assessment work completed as measured against the agency's sensitive systems over the past three years
N/A - Not applicable as the agency had no risk assessments due
N/C - The agency head has not submitted risk assessment 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
N/C – the data provided is incomplete, and there is an active application without any business processes
X% – The percentage of business processes that have been submitted and approved within the last 365 days

IDS (intrusion detection system) quarterly reports
Pass - Documents received as scheduled
N/C - Reports were not received

Applications Certified
Compliant – Agency application inventory is compliant for completeness
Non-Compliant – Agency application inventory is incomplete

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 Head

Agency Name	Agency Secretariat	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding Updates Received	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Current Year Percentage of Risk Finding Updates Received	BIA Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	ISO Centralized Services	Audit Centralized Services
Board of Accountancy	Finance	Pass	50%	100%	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Commonwealths Attorneys Services Council	Public Safety	Pass	N/A	N/A	Pass	N/A	N/A	100%	Pass	Compliant	Pass	Yes	No	No
Compensation Board	Administration	Pass	83%	100%	Pass	0%	100%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Department for Aging and Rehabilitative Services	Health and Human Resources	Pass	82%	100%	N/C	N/C	0%	0%	Pass	Compliant	Pass	Yes	No	No
Department for the Deaf and Hard of Hearing	Health and Human Resources	Pass	100%	N/A	N/C	N/C	0%	0%	Pass	Compliant	Pass	Yes	No	Yes
Department of Accounts	Finance	Pass	0%	N/A	Pass	42%	N/A	12%	Pass	Compliant	Pass	Yes	No	Yes
Department of Aviation	Transportation	Pass	75%	100.00%	Pass	100%	0%	100%	Pass	Compliant	Pass	Yes	No	No
Department of Behavioral Health and Development Services	Health and Human Resources	Pass	8%	91.66%	Pass	0%	80.95%	100%	Pass	Compliant	Pass	Yes	No	No
Department of Conservation and Recreation	Natural Resources	Pass	50%	100%	Pass	100%	100%	94%	Pass	Compliant	Pass	No	Yes	No

Agency Name	Agency Secretariat	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding Updates Received	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Current Year Percentage of Risk Finding Updates Received	BIA Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	ISO Centralized Services	Audit Centralized Services
Department of Corrections	Public Safety	Pass	50%	100%	Pass	65%	N/A	100%	Pass	Compliant	Pass	Yes	No	No
Department of Criminal Justice Services	Public Safety	Pass	71%	100%	Pass	57%	87.39%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Department of Education	Education	Pass	41%	100.00%	Pass	80%	N/A	100%	Pass	Compliant	Pass	Yes	No	Yes
Department of Elections	Administration	Pass	100%	N/A	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	Yes	No
Department of Environmental Quality	Natural Resources	Pass	53%	99.48%	Pass	100%	0%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Department of Fire Programs	Public Safety	N/C	N/C	75%	Pass	0%	N/A	100%	Pass	Compliant	Pass	No	No	No
Department of Forensic Science	Public Safety	Pass	100%	N/A	Pass	100%	100%	0%	Pass	Compliant	Pass	Yes	No	Yes
Department of Forestry	Agriculture & Forestry	Pass	75%	6.58%	Pass	25%	21.88%	100%	Pass	Compliant	Pass	No	Yes	Yes
Department of General Services	Administration	Pass	72%	100%	Pass	89%	100.00%	100%	Pass	Compliant	Pass	Yes	No	No
Department of Health Professions	Health and Human Resources	Pass	100%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Department of Historic Resources	Natural Resources	Pass	100%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	No	Yes

Agency Name	Agency Secretariat	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding Updates Received	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Current Year Percentage of Risk Finding Updates Received	BIA Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	ISO Centralized Services	Audit Centralized Services
Department of Housing and Community Development	Commerce and Trade	Pass	100%	N/A	Pass	40%	25%	100%	Pass	Compliant	Pass	Yes	No	Yes
Department of Human Resource Management	Administration	Pass	83%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Department of Juvenile Justice	Public Safety	Pass	0%	N/A	Pass	0%	N/A	N/C	Pass	Partial	Pass	Yes	Yes	Yes
Department of Labor and Industry	Commerce and Trade	Pass	38%	100%	Pass	88%	100.00%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Department of Medical Assistance Services	Health and Human Resources	Pass	57%	100%	Pass	N/C	34.29%	100%	Pass	Compliant	Pass	Yes	No	No
Department of Military Affairs	Veterans and Defense Affairs	Pass	0%	N/A	Pass	0%	N/A	0%	Pass	Compliant	Pass	No	No	No
Department of Motor Vehicles	Transportation	Pass	40%	96.30%	Pass	100%	77.29%	100%	Pass	Compliant	Pass	Yes	No	No
Department of Planning and Budget	Finance	Pass	0%	N/A	Pass	83%	41.56%	100%	Pass	Compliant	Pass	Yes	Yes	Yes

Agency Name	Agency Secretariat	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding Updates Received	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Current Year Percentage of Risk Finding Updates Received	BIA Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	ISO Centralized Services	Audit Centralized Services
Department of Professional and Occupational Regulation	Commerce and Trade	Pass	0%	N/A	N/C	N/C	46.67%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Department of Rail and Public Transportation	Transportation	Pass	80%	100%	Pass	N/C	0%	100%	Pass	Compliant	Pass	Yes	No	Yes
Department of Small Business and Supplier Diversity	Commerce and Trade	Pass	0%	N/A	N/C	100%	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Department of Social Services	Health and Human Resources	Pass	20%	0%	Pass	53%	0%	100%	Pass	Compliant	Pass	Yes	No	No
Department of Taxation	Finance	Pass	29%	16.76%	Pass	90%	16.53%	N/C	Pass	Non-Compliant	Pass	Yes	No	No
Department of Treasury	Finance	Pass	24%	0%	Pass	N/C	0%	100%	Pass	Compliant	Pass	Yes	No	No
Department of Veterans Services	Veterans and Defense Affairs	Pass	0%	N/A	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes	Yes	No
Department of Wildlife Resources	Natural Resources	Pass	31%	100%	Pass	0%	N/A	100%	Pass	Compliant	Pass	No	Yes	No
Frontier Culture Museum of Virginia	Education	Pass	0%	100%	Pass	0%	100%	100%	Pass	Compliant	Pass	Yes	Yes	No

Agency Name	Agency Secretariat	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding Updates Received	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Current Year Percentage of Risk Finding Updates Received	BIA Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	ISO Centralized Services	Audit Centralized Services
Gunston Hall	Education	Pass	0%	N/A	Pass	N/C	0%	100%	Pass	Compliant	N/C	Yes	Yes	No
Indigent Defense Commission	Independent	Pass	25%	75%	Pass	0%	75%	100%	Fail	Compliant	N/C	Yes	Yes	Yes
Jamestown-Yorktown Foundation	Education	Pass	50%	100%	Pass	10%	100%	100%	Pass	Compliant	N/C	No	No	Yes
Library of Virginia	Education	Pass	10%	N/A	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes	No	No
Marine Resources Commission	Natural Resources	Pass	67%	100.00%	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Motor Vehicle Dealer Board	Transportation	Pass	50%	100%	N/C	N/C	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes
New College Institute	Education	N/C	N/C	N/A	N/C	N/C	N/A	0%	Fail	Non-Compliant	N/C	No	No	No
Norfolk State University	Education	Pass	28%	80.90%	Pass	24%	0%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Office for Children's Services	Health and Human Resources	Pass	75%	100%	Pass	75%	44.23	100%	Pass	Compliant	Pass	Yes	No	Yes
Office of Attorney General	Executive	Pass	N/C	0%	N/C	N/C	N/A	100%	Pass	Non-Compliant	Pass	No	Yes	No
Office of State Inspector General	Executive	Pass	100%	100%	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes	No	No

Agency Name	Agency Secretariat	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding Updates Received	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Current Year Percentage of Risk Finding Updates Received	BIA Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	ISO Centralized Services	Audit Centralized Services
Office of the Governor	Executive	N/C	N/C	N/A	Pass	100%	0%	N/C	Pass	Compliant	Pass	Yes	Yes	No
Richard Bland College	Education	Pass	71%	41.30%	N/C	N/C	N/A	100%	Fail	Compliant	Pass	Yes	No	No
Science Museum of Virginia	Education	Pass	0%	N/A	Pass	60%	0%	100%	Pass	Compliant	N/C	Yes	Yes	No
Southern Virginia Higher Education Center	Education	Pass	N/A	N/A	Pass	N/A	N/A	100%	Pass	Compliant	Pass	No	Yes	No
Southwest Virginia Higher Education Center	Education	N/C	N/C	N/A	N/C	N/C	N/A	0%	Fail	Non-Compliant	N/C	No	No	No
State Corporation Commission	Independent	Pass	92%	100%	Pass	N/C	N/A	100%	Pass	Compliant	Pass	Yes	No	No
State Council of Higher Education for Virginia	Education	Pass	0%	0%	Pass	N/C	0%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
State Lottery Department	Independent	Pass	84%	N/A	Pass	54%	N/A	100%	Pass	Compliant	Pass	Yes	No	No
Tobacco Region Revitalization Commission	Commerce and Trade	Pass	0%	N/A	Pass	0%	N/A	100%	Pass	Compliant	N/C	Yes	No	No
Virginia College Savings Plan	Independent	Pass	88%	100%	Pass	67%	N/A	100%	Pass	Non-Compliant	Pass	Yes	No	No

Agency Name	Agency Secretariat	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding Updates Received	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Current Year Percentage of Risk Finding Updates Received	BIA Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	ISO Centralized Services	Audit Centralized Services
Virginia Commission for the Arts	Education	N/C	N/C	N/A	Pass	0%	N/A	100%	Pass	Compliant	N/C	Yes	Yes	No
Virginia Department of Agriculture and Consumer Services	Agriculture & Forestry	Pass	95%	100%	Pass	0%	0%	100%	Pass	Compliant	Pass	Yes	No	No
Virginia Department of Emergency Management	Public Safety	N/C	N/C	N/A	N/C	N/C	N/A	N/C	Pass	Compliant	N/C	No	Yes	No
Virginia Department of Health	Health and Human Resources	Pass	31%	97.74%	Pass	79%	100%	100%	Pass	Compliant	Pass	No	No	No
Virginia Department of Transportation	Transportation	Pass	67%	94.81%	Pass	100%	0%	100%	Pass	Compliant	Pass	No	No	No
Virginia Economic Development Partnership	Commerce and Trade	N/C	N/C	N/A	N/C	N/C	N/A	N/C	Fail	Non-Compliant	Pass	No	No	No
Virginia Employment Commission	Commerce and Trade	Pass	65%	44.60%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	No	No
Virginia Energy (Formerly DMME)	Commerce and Trade	Pass	50%	N/A	Pass	N/C	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes

Agency Name	Agency Secretariat	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding Updates Received	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Current Year Percentage of Risk Finding Updates Received	BIA Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	ISO Centralized Services	Audit Centralized Services
Virginia Foundation for Healthy Youth	Health and Human Resources	Pass	0%	N/A	Pass	50%	N/A	N/C	Pass	Non-Compliant	N/C	Yes	No	No
Virginia Information Technologies Agency	Administration	Pass	20%	100%	Pass	0%	51.43%	97%	Pass	Compliant	Pass	Yes	Yes	Yes
Virginia Innovation Partnership Corporation (Formerly CIT)	Commerce and Trade	Pass	0%	N/A%	Pass	N/C	N/A	0%	Pass	Compliant	N/C	Yes	No	No
Virginia Museum of Fine Arts	Education	Pass	100%	N/A	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes	No	Yes
Virginia Museum of Natural History	Education	Pass	0%	0%	N/C	N/C	0%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Virginia Racing Commission	Agriculture & Forestry	Pass	20%	100%	Pass	80%	100%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Virginia Retirement System	Independent	Pass	100%	100.00%	Pass	39%	63.68%	100%	Pass	Compliant	Pass	Yes	No	No
Virginia State Police	Public Safety	Pass	60%	100%	Pass	2%	100%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Virginia State University	Education	Pass	46%	100.00%	Pass	85%	100%	0%	Pass	Compliant	N/C	Yes	Yes	Yes

Agency Name	Agency Secretariat	Audit Plan Status	3 Year Audit Obligation	Current Year Percentage of Audit Finding Updates Received	Risk Assessment Plan Status	3 Year Risk Assessment Obligation	Current Year Percentage of Risk Finding Updates Received	BIA Status	IDS Quarterly Reports	Applications Certified	ISO Certification Status	ISO Reports to Agency Head	ISO Centralized Services	Audit Centralized Services
Virginia Workers Compensation Commission	Independent	Pass	100%	100%	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes	No	Yes

*Approved exception on file

Appendix II – Cybersecurity framework results – Detail

National Cybersecurity Review (NCSR) Results

NCSR Level Legend
7 – Optimized
6 – Tested and verified
5 – Implementation in process
4 – Partially documented standards and/or procedures
3 – Documented policy
2 - Informally performed
1 - Not performed
* Recommended level is 5 or higher

Agency	Identify	Detect	Protect	Respond	Recover	Average
Board of Accountancy	6.07	5.50	5.90	5.75	5.83	5.81
Virginia Innovation Partnership Corporation (Formerly CIT)	4.97	4.17	5.21	2.31	2.00	3.73
Commission for the Arts						
Commonwealth of Virginia (overall)	5.10	5.17	5.51	4.94	5.00	5.14
Commonwealth's Attorneys' Services Council	7.00	7.00	7.00	6.63	7.00	6.93
Compensation Board	3.62	5.67	3.62	3.38	2.33	3.72
Department for Aging and Rehabilitative Services	2.97	3.94	4.72	2.19	2.00	3.16
Department for the Deaf and Hard of Hearing	2.97	3.94	4.72	2.19	2.00	3.16
Department of Accounts	6.52	6.44	6.64	6.44	6.00	6.41
Department of Agriculture and Consumer Services	6.86	6.89	6.67	7.00	6.67	6.82
Department of Aviation	5.72	6.00	6.00	6.00	6.00	5.94
Department of Behavioral Health and Development Services	5.52	5.94	5.49	5.94	6.00	5.78
Department of Conservation and Recreation	5.69	5.89	5.87	5.75	5.17	5.67
Department of Corrections	5.28	5.06	5.87	5.63	5.50	5.47
Department of Criminal Justice Services	4.03	5.72	5.49	3.56	2.33	4.23
Department of Education	6.21	3.00	6.18	2.69	1.50	3.91
Department of Elections	3.17	3.72	4.28	3.69	4.00	3.77
Department of Emergency Management	3.21	3.28	3.54	2.38	2.50	2.98
Department of Environmental Quality	4.59	3.72	5.18	4.13	4.50	4.42
Department of Fire Programs	3.52	2.50	3.87	2.38	2.00	2.85
Department of Forensic Science	5.00	5.00	5.03	5.00	5.00	5.01
Department of Forestry	5.21	3.56	4.90	3.44	2.00	3.82
Department of Game and Inland Fisheries	5.83	5.94	5.56	4.63	5.67	5.53
Department of General Services	6.03	5.33	5.97	5.56	5.17	5.61
Department of Health Professions	6.00	5.94	5.95	5.94	6.00	5.97
Department of Historic Resources	7.00	7.00	7.00	7.00	7.00	7.00
Department of Housing and Community Development	5.86	5.56	5.92	5.75	5.83	5.78
Department of Human Resource Management	6.24	5.94	6.21	6.00	6.00	6.08
Department of Juvenile Justice	4.00	4.00	4.00	4.00	4.00	4.00
Department of Labor and Industry	5.34	6.44	5.10	5.69	5.50	5.62
Department of Medical Assistance Services	3.17	3.83	4.64	3.38	3.50	3.70

Department of Military Affairs	5.76	5.78	6.00	5.88	5.33	5.75
Virginia Energy (Formerly DMME)	4.72	5.00	5.00	4.88	5.00	4.92
Department of Motor Vehicles	6.45	6.44	6.36	6.69	7.00	6.59
Department of Planning and Budget	5.72	6.00	5.77	6.00	5.67	5.83
Department of Professional and Occupational Regulation	3.62	3.33	4.23	3.25	4.67	3.82
Department of Rail and Public Transportation	7.00	7.00	7.00	7.00	7.00	7.00
Department of Small Business and Supplier Diversity	7.00	6.00	6.03	5.94	6.00	6.19
Department of Social Services	3.00	4.06	3.64	3.13	3.33	3.43
Department of Taxation	3.86	4.00	4.03	3.63	4.83	4.07
Department of Treasury	6.52	6.39	6.41	6.00	5.83	6.23
Department of Veterans Services	3.28	2.56	3.97	2.31	1.67	2.76
Department of Wildlife Resources	5.59	5.89	5.69	4.50	5.67	5.47
Virginia Economic Development Partnership						
Frontier Culture Museum of Virginia	5.00	5.44	5.31	5.31	5.00	5.21
Gunston Hall	5.90	5.94	5.90	5.81	6.00	5.91
Indigent Defense Commission	6.00	5.94	5.92	5.88	5.83	5.92
Jamestown-Yorktown Foundation	4.31	4.06	4.82	2.25	3.83	3.85
Library of Virginia	6.69	6.00	6.38	6.31	6.00	6.28
Marine Resources Commission	5.03	5.72	5.46	5.19	4.67	5.21
Motor Vehicle Dealer Board	3.52	4.67	4.33	2.75	2.83	3.62
New College Institute	4.00		5.64			
Norfolk State University	3.59	2.83	4.64	2.13	2.67	3.17
Office of Children's Services	5.76	6.56	6.69	6.88	6.50	6.48
Office of State Inspector General	7.00	6.17	6.87	6.19	7.00	6.65
Office of the Attorney General	5.86	6.00	5.85	5.94	6.00	5.93
Office of the Governor	5.97	5.89	5.87	5.75	6.00	5.90
Science Museum of Virginia	5.79	6.00	5.87	6.00	6.00	5.93
Southern Virginia Higher Education Center	2.86	3.94	4.67	2.19	2.00	3.13
Southwest Virginia Higher Education Center	5.79	6.00	5.85	5.94	6.00	5.92
State Corporation Commission	4.17	5.67	4.28	5.63	6.00	5.15
State Council of Higher Education for Virginia	5.28	7.00	5.69	5.00	5.00	5.59
State Lottery Department	4.03	4.89	5.46	4.88	4.67	4.79
Tobacco Region Revitalization Commission						
Virginia Department of Health	5.76	5.67	5.38	5.06	5.00	5.37
Virginia Department of Transportation	4.07	4.06	4.28	3.88	3.67	3.99
Virginia Employment Commission	5.14	4.67	5.26	4.75	5.50	5.06
Virginia Foundation for Healthy Youth	5.03	5.67	5.69	6.19	5.33	5.58
Virginia Information Technologies Agency	6.34	6.33	6.28	6.88	6.50	6.47
Virginia Museum of Fine Arts	7.00	7.00	7.00	7.00	7.00	7.00
Virginia Museum of Natural History	5.62	5.50	5.00	5.75	6.00	5.57
Virginia Racing Commission	5.41	5.50	5.59	5.38	5.00	5.38
Virginia Retirement System	6.69	6.94	6.87	6.56	6.83	6.78
Virginia School for the Deaf and Blind	4.00	4.00	4.00	4.00	4.00	4.00
Virginia State Police	5.52	4.33	5.26	5.25	6.00	5.27

Virginia State University	6.69	7.00	6.85	6.94	7.00	6.89
Virginia Workers Compensation Commission	7.00	6.78	7.00	6.94	7.00	6.94