VIRGINIA IT AGENCY

2020 COMMONWEALTH OF VIRGINIA INFORMATION SECURITY REPORT

Commonwealth Security and Risk Management

Prepared and Published by:

Virginia Information Technologies Agency

Connecting – Protecting - Innovating

Comments on the
2020 Commonwealth of Virginia Information Security Report
are welcome.
Suggestions may be conveyed electronically to CommonwealthSecurity@vita.virginia.gov

Please submit written correspondence to:

Chief Information Officer of the Commonwealth
Virginia Information Technologies Agency
Commonwealth Enterprise Solutions Center
11751 Meadowville Lane
Chester, VA 23836
cio@vita.virginia.gov

VIRGINIA IT AGENCY

Executive summary **4**

2020 Annual Information Security Report **7**

Commonwealth threat management program **7**

Incident trends by category 12

Cyber intelligence from Commonwealth partners 15

Security investigations by category 16

CSRM centralized services **17**

Centralized IT security audit services 17

Centralized ISO Services 18

Web application vulnerability scanning program 18

Commonwealth information security governance program **19**

Statute requires compliance monitoring 19

Commonwealth Information Security Officers Advisory Group 20

Commonwealth Information Security Council 20

Risk Management Committee 21

Commonwealth IT audit compliance program **21**

Audit compliance report card 21

Key Commonwealth security audit compliance metrics and analysis 22

Audit Findings by Calendar Year Analysis 24

Commonwealth IT risk management program **26**

Risk compliance report card 26

IT risk management program monitoring 27

Nationwide Cyber Security Review **33**

National Cyber Security Review Analysis 33

Appendix I -Agency Compliance Report Card **47**

Appendix II - Agency Information Security Data Points **53**

Appendix III - Cybersecurity framework results - Detail **60**

Executive summary

This 2020 Commonwealth of Virginia (COV) Information Security Report is the 11th annual report by the chief information officer (CIO) of the Commonwealth to the governor and the General Assembly. As directed by § 2.2-2009(B)(1) of the *Code of Virginia*, the CIO is required to identify annually those agencies that have not implemented acceptable policies, procedures and standards to control unauthorized uses, intrusions or other security threats. In accordance with § 2.2-2009(B)(1), the scope of this report is limited to sixty-six executive branch agencies, six independent agencies, and three Level I institutions of higher education. This report does not address compliance for 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 follows a baseline created by CSRM in 2008 to assess the strength of agency information technology (IT) security programs that are established to protect Commonwealth data and systems. A listing of the agencies that were assessed and their security compliance and cybersecurity framework assessment metrics are found in the appendices of this document.

CSRM implemented a new quantitative cyber risk analysis model 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.

VITA CSRM facilitates the COV IT Risk Management Committee. The IT Risk Management Committee focuses on the VITA infrastructure program and security risks facing the Commonwealth. The committee is comprised of VITA personnel and stakeholders from Commonwealth state agencies. The committee identifies, tracks, and prioritizes identified risks. Risk alerts are issued by the committee to ensure critical risks are escalated for quick remediation. The committee also recommends changes to standards, policies, and procedures to address the critical risks facing the Commonwealth.

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 model that VITA has adopted, CSRM plays an integral role in identifying cybersecurity risks and tracking them until they are resolved.

VITA CSRM leverages the enterprise cloud oversight service (ECOS) to minimize risk and ensure cloud-based service providers are able to meet Commonwealth IT security requirements. As agencies continue to move toward cloud services, CSRM has established a security review process for third-party systems and services. This supports agencies to ensure the applications in the cloud are secure, dependable and resilient. ECOS is a service specifically created for establishing contract terms and oversight of third-party vendors offering software as a service (SaaS) applications.

VITA CSRM monitors findings identified through IT audits and IT risk assessments. 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 create an increased risk that agencies will be exposed to unauthorized access of data, fraud or disruption of IT services. To address this issue, VITA has made a budget request for resources to implement an identity access management (IAM) solution for the Commonwealth. IAM will create an automated framework for policies and technologies to ensure that users are properly authorized and have appropriate access to technology resources.

Agencies with information security officers reporting to agency heads have better compliance scores with CSRM cybersecurity metrics. Commonwealth security standards require agency information security officers (ISOs) to report to their agency head. This requirement intends to prevent conflicts of interest and to ensure ISOs have the appropriate level of independence to advise the agency head of the risk they assume. Analysis shows that 74% of Commonwealth ISOs report to their agency head. This is an improvement from only 55% of agencies having implemented this requirement last year. In addition, ISO independence correlates to higher scores with CSRM IT security metrics. Agencies where the ISO reports to the agency head score an average risk grade of B, while agencies where the ISO does not report to the agency head score lower and have an average risk grade of D. Agencies should continue to take the necessary steps to implement this change in their organizational structure to prevent conflicts of interest between security and operations and ensure agency ISOs have the proper authority to manage security within their agencies.

Attackers continue to threaten Virginia colleges and universities. CSRM threat management works with the Multi-State Information Sharing & Analysis Center (MS-ISAC) to share threat information with Commonwealth agencies. Based on this analysis, higher education comprised the majority of the security investigations (55%), more than COV agencies, local governments, and the public schools combined. Furthermore, 90% of the investigations related to compromised accounts, 29% of the malware infection investigations, and 46% of the software vulnerabilities investigations were related to institutions of higher education.

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 without being subject to any centralized oversight authority related to IT security. However, CSRM has long recommended and continues to recommend that higher education institutions be subject to IT security oversight similar to executive branch agencies.

CSRM provided IT security support for elections in the Commonwealth. Safe and secure elections are a top priority for the Commonwealth. To ensure the integrity of elections, CSRM performed a comprehensive security review of all systems and infrastructure supporting Virginia elections. CSRM partnered with the Department of Elections to develop security standards and regulations. In addition, CSRM provided monitoring of local county and city policies and procedures. CSRM also established a cybersecurity command center to handle any issues that occur during the election process. CSRM will continue to partner with the Department of Elections to provide support for upcoming elections.

Ransomware attacks continue to be a threat. During 2020, at least six Virginia public school systems were victims of ransomware. Fairfax County was one of the first Commonwealth public schools victimized by the "Maze" ransomware. Nationally, more than 63 U.S. school districts and colleges were impacted by ransomware in 2020. Recent data shows that one of the Commonwealth's public body cyber insurers responded to 50 incidents ranging from publicly exploited vulnerable software to full ransomware incidents. The average cost of cleaning up a ransomware incident was $150,000, with one reaching as much as $300,000.

Overall agency audit and risk program metrics were consistent with the prior year. Compliance metrics for audit and risk scores have remained consistent for the last few years, and have not improved significantly. CSRM will encourage eligible agencies to use centralized ISO and audit services to achieve compliance. CSRM also reviews audit and risk compliance as a part of the IT strategic planning process. Agencies with poor compliance scores could find their IT strategic plans rejected or approval delayed.

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 528 days to close and findings from risk assessments averaged 398 days. 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. Agencies should prioritize and remediate findings according to the severity of the potential impact and the likelihood of occurrence.

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. Agencies that used the centralized audit service achieved an average audit compliance grade of B. This is higher than the average agency audit grade of C for non-audit services agencies. Agencies using the ISO risk management services received an average risk compliance grade of A. In comparison, non-ISO service agencies had an average risk compliance grade of C. Use of audit and ISO services has helped agencies that lacked resources comply with security requirements and improve their audit and risk grades.

In addition, CSRM's vulnerability scanning service continues to provide vulnerability scanning and assists agencies in reducing the number and impact of vulnerabilities. CSRM anticipates further improvements in compliance and security as agencies utilize the centralized services. Since the scanning service was started, 10,722 vulnerabilities have been identified and almost 90% of these vulnerabilities have been corrected.

CSRM collaborated with other agencies and IT suppliers to conduct the annual Commonwealth cybersecurity preparedness exercise. The event brought agencies and suppliers together to test the awareness, effectiveness, and efficiency of their incident response tools and processes. The exercise focused on the planning and execution aspects of cyber response plans, to include objectives, scenarios, reporting and assessment procedures, network architecture, tools, and lessons learned from utilizing the scenarios outlined during the exercise. CSRM saw significant improvement in this year's exercise from the previous year and will look to continue building on the success of this exercise to improve on the Commonwealth's ability to respond to IT security incidents.

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. Survey results indicated that agencies on average have a maturity level identified as "partially documented standards and/or procedures" in the five cybersecurity areas assessed. While comparatively, this level of maturity is slightly better than the national average, it is below the Commonwealth's target of "optimized".

The average agency score for each area improved in 2020 from the prior year. According to NCSR, the recommended minimum maturity level is set at a score of five or "implementation in process". A maturity level of "implementation in process" indicates that the organization has formally documented their policies, standards and processes and is in the process of implementation. Commonwealth agencies reported that they reached this level for nearly every function, on average. CSRM will continue to work with agencies to improve their maturity to the next level of "tested and verified." A maturity level of "tested and verified" indicates that the organization has not only formally documented its policies, standards and procedures but also indicates that implementation of those policies, standards and procedures is routinely tested and verified.

2020 Annual Information Security Report

The 2020 Annual Security Report for the Commonwealth of Virginia report includes an analysis of the Commonwealth threat management program, new services offered, the Commonwealth information security governance program and the Commonwealth risk management program.

Commonwealth threat management program

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

During 2020, the Commonwealth of Virginia continued to be a target for cyberattacks. The Commonwealth experienced over 66 million attack attempts on the network and blocked 50,099 pieces of malware. Despite many layers of protection, the Commonwealth still experienced 188 successful IT security incidents.

Thirty-four percent of all incidents were the result of successful malware attacks. As the largest category of incidents, malware is a constant threat to Commonwealth devices and data. Malware programs are designed to infect targeted computers in order to damage systems or provide unauthorized access to sensitive data. Cybercriminals often develop malware to exploit known vulnerabilities in a system. Systems are most vulnerable to these types of attacks when they are running unpatched and/or end-of-life software or hardware. Once an application has been declared to be end-of-life, the vendor no longer provides security updates for known vulnerabilities.

Multiple attack vectors can be used to carry out cyberattacks. A primary avenue of attack used against the Commonwealth is phishing emails containing malicious attachments. In order to protect systems from this attack vector, email is actively scanned and potentially malicious content is blocked. In addition, employee security awareness training emphasizes phishing recognition and reporting.

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

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

Most malware attacks are financially motivated. In the U.S., malware called "Trojans" were the most prevalent type of malware in 2020. Some Trojan attacks are used to steal information while others were used as a mechanism to secure a ransom from the entity. In a 2020 report from the MS-ISAC, six of the top ten malware infections were Trojans. Commonwealth entities experienced Trojan attacks resulting in 62 incidents. A Trojan known as "Emotet" was most prevalent with 10 of the 62 infections. "Emotet" is typically used to steal information or to install additional malware on a device. When malware is installed, more vulnerabilities will

develop in the layers of protection around the device. Once a device is vulnerable, the attacker can install ransomware on the device in an attempt to encrypt the data and collect a fee.

In a ransomware attack, the malware encrypts the victim's data, making it unusable until it is decrypted. The ransomware then displays a note on the screen requesting payment for the decryption key. This payment is normally requested in cryptocurrency so that the payment cannot be traced. However, if the entity pays the ransom, there is no guarantee that the key will be provided or that it will actually decrypt the data. The best protection from ransomware is to have a good clean backup of the data so that the device can be wiped and the data restored.

Ransomware attacks targeted Commonwealth governments and schools. Fairfax County was one of the first Commonwealth public schools victimized by the "Maze" ransomware. In addition, at least six Virginia public school systems were victims of ransomware during 2020. Nationally, more than 63 U.S. school districts and colleges were impacted by ransomware in 2020. Recent data shows that one of the Commonwealth's public body cyber insurers responded to 50 incidents ranging from publicly exploited vulnerable software to full ransomware incidents. The average cost of cleaning up a ransomware incident was $150,000 with one reaching as much as $300,000.

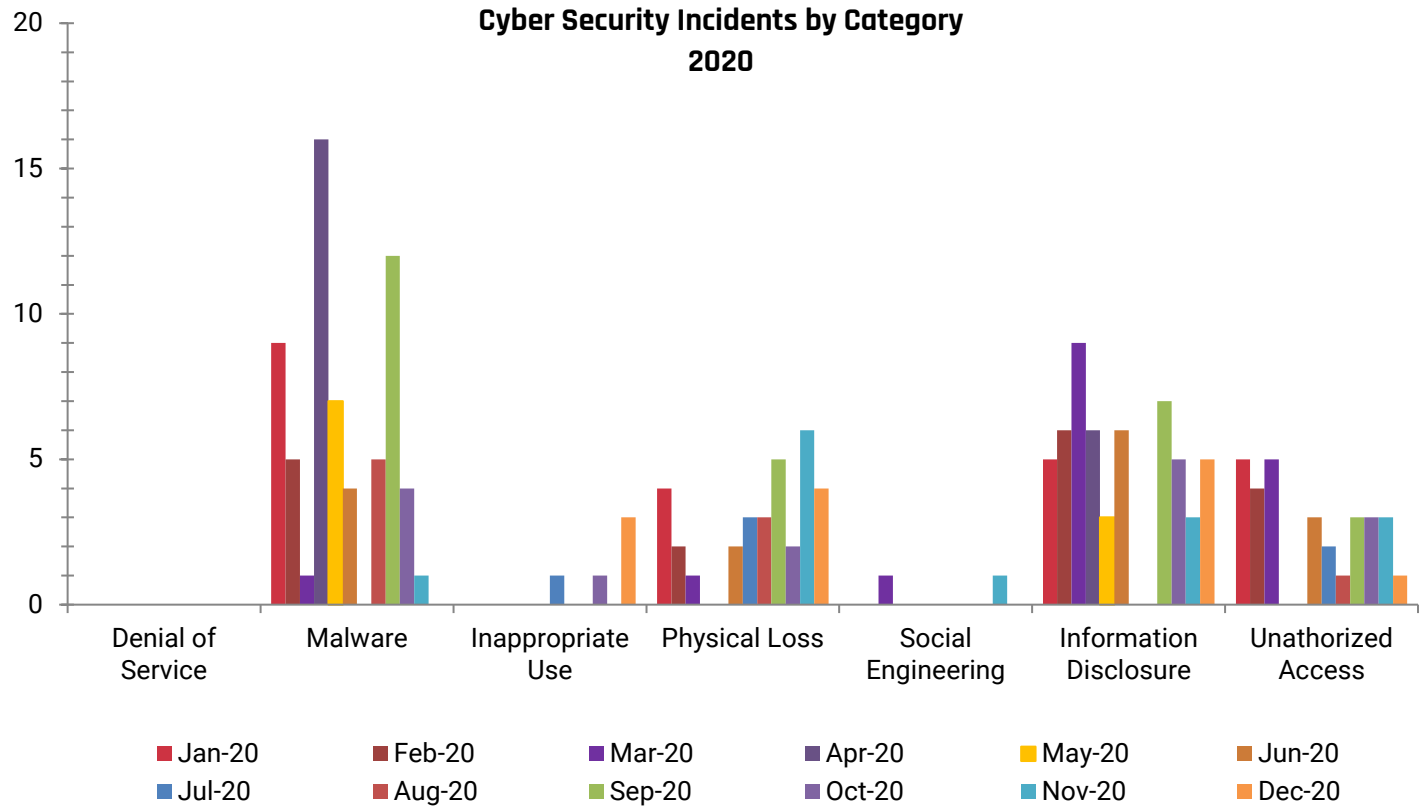
Most of these attacks are due to problems with an organization's cyber hygiene or a user falling victim to a phishing attack. CSRM expects these attacks to continue until the targets are able to adequately address their cyber hygiene deficiencies and better educate users.

It is Commonwealth Security's recommendation that agencies should not pay the ransom requested in a ransomware attack. Preventative measures combined with strong recovery methods are the best tools against ransomware. Commonwealth Security, through its governance and training programs, has developed guidelines, best practices and recommendations to prevent ransomware attacks (https://www.vita.virginia.gov/media/vitavirginiagov/resources/pdf/Ransomware-Study-Report.pdf).

CSRM recommends best practices to combat malware. Commonwealth Security has implemented many layers of protection to reduce the risk of malware infections. However, best practices still need to be followed by both agencies and users:

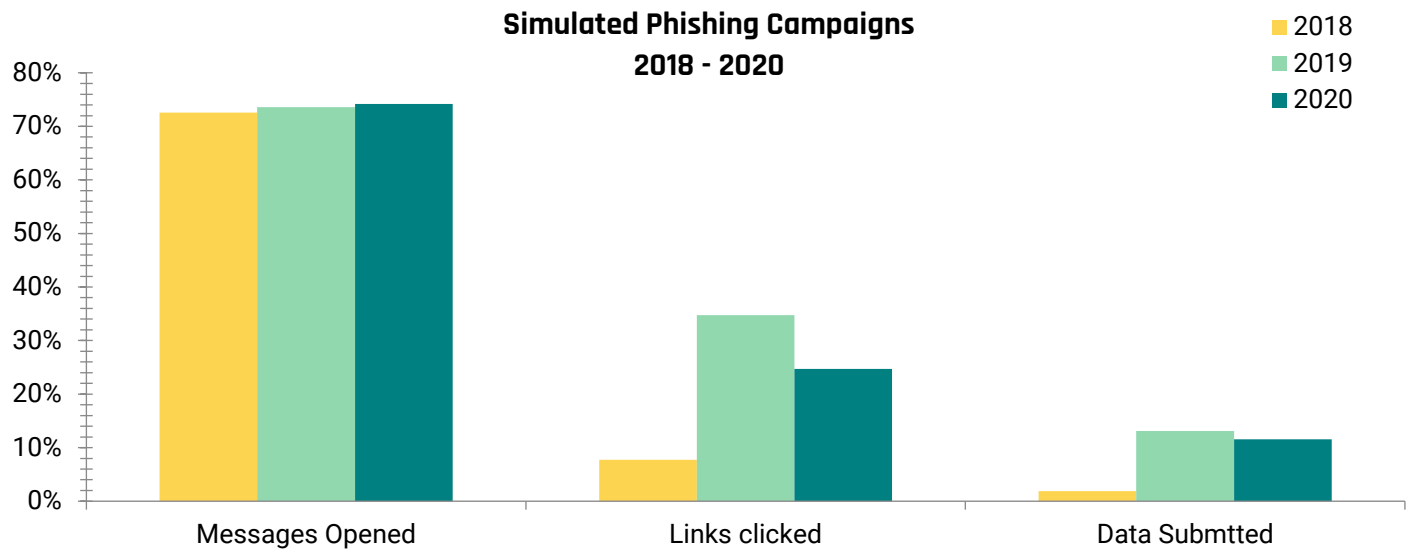
- All systems must be protected with the necessary security technology
- All systems need to be patched and/or upgraded to supported versions of software
- All systems need to be continually scanned for vulnerabilities and issues promptly remediated
- Users need to be given ongoing security awareness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

Information disclosure was the second largest category of incidents for 2020. Information disclosure incidents continued to be a threat. These incidents typically occur due to user errors. Users send unencrypted emails containing sensitive data, misfile physical documents and inadvertently mail sensitive information to the wrong recipient. Although multifactor authentication can mitigate the problem with exposed credentials, it still does not resolve the human error issues with data disclosure. An increased emphasis on improving security awareness training will help to protect both Commonwealth employees and data. Information disclosure incidents accounted for 29% of all incidents experienced during 2020.



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.

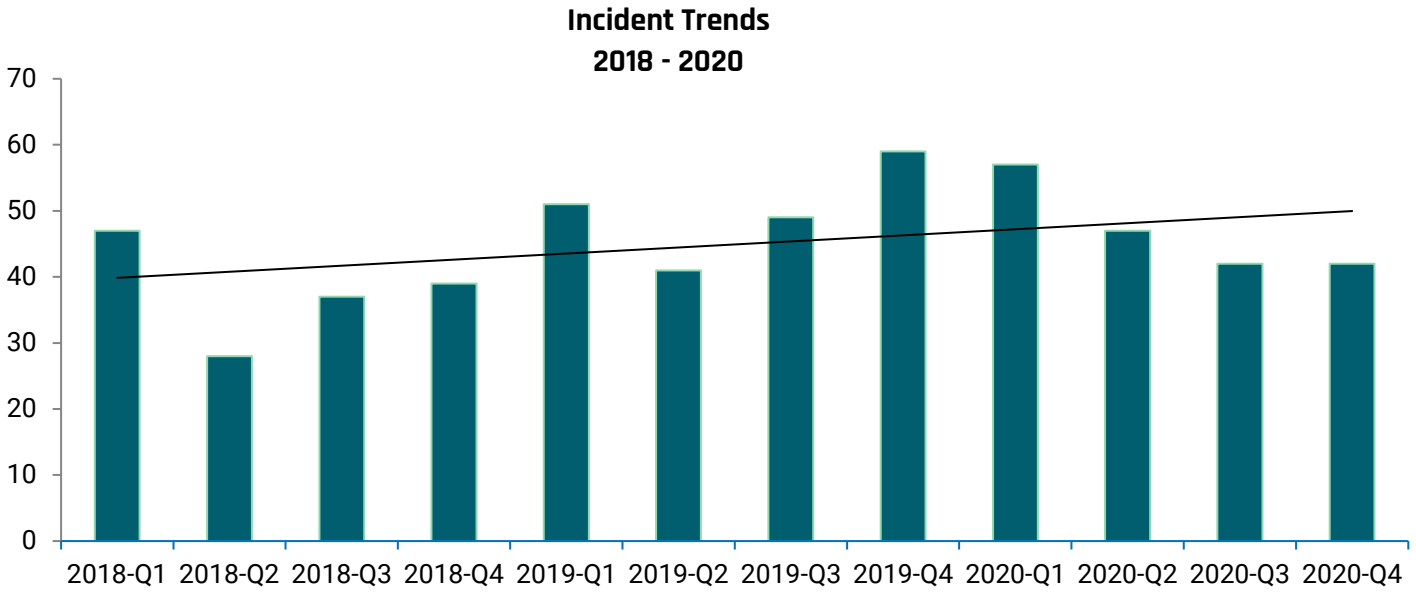
During 2020, CSRM provided simulated phishing training to selected COV employees. Of the employees targeted in the phishing exercise, 74% of the employees opened the phishing message, 25% clicked on the link in the message and 12% submitted their credentials. The chart below shows a comparison of the results over the past three years (2018 to 2020).



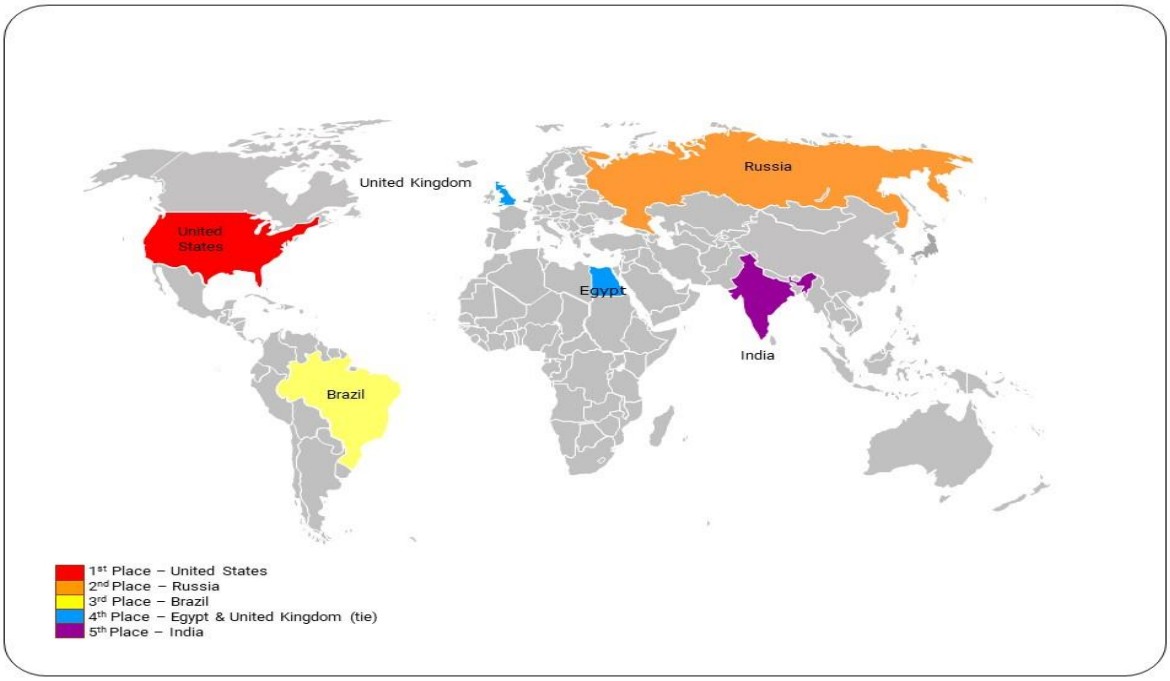
While the 2020 sample size is similar to 2018, the results show that 12% of users exposed their credentials in 2020, about a 10% increase over 2018. This demonstrates the need for continuous security awareness training. VITA has been vested with additional authority in the Code of Virginia to establish minimum IT security awareness training requirements for all employees. A new IT security training standard, effective in 2021, now requires that all agencies must meet a minimum established training baseline for their employees.

In addition, this new baseline emphasizes enhanced training for employees to recognize phishing attacks and to respond appropriately. To this end, CSRM's CSIRT will implement a new software platform designed to conduct large-scale simulated phishing campaigns. With this new software platform, every agency and every employee in the Commonwealth could be targeted in simulated phishing exercises. The software platform will allow the CSIRT to identify agencies and employees that require additional training. CSRM expects to significantly increase the number of agencies and employees that it is able to provide phishing training for in 2021.

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 have been implemented and additional layers of protection have been added. However, attackers continue to develop new tactics to compromise systems and incident trends have been steadily rising. CSRM is constantly investigating new security controls and additional practices to protect the environment from compromise.

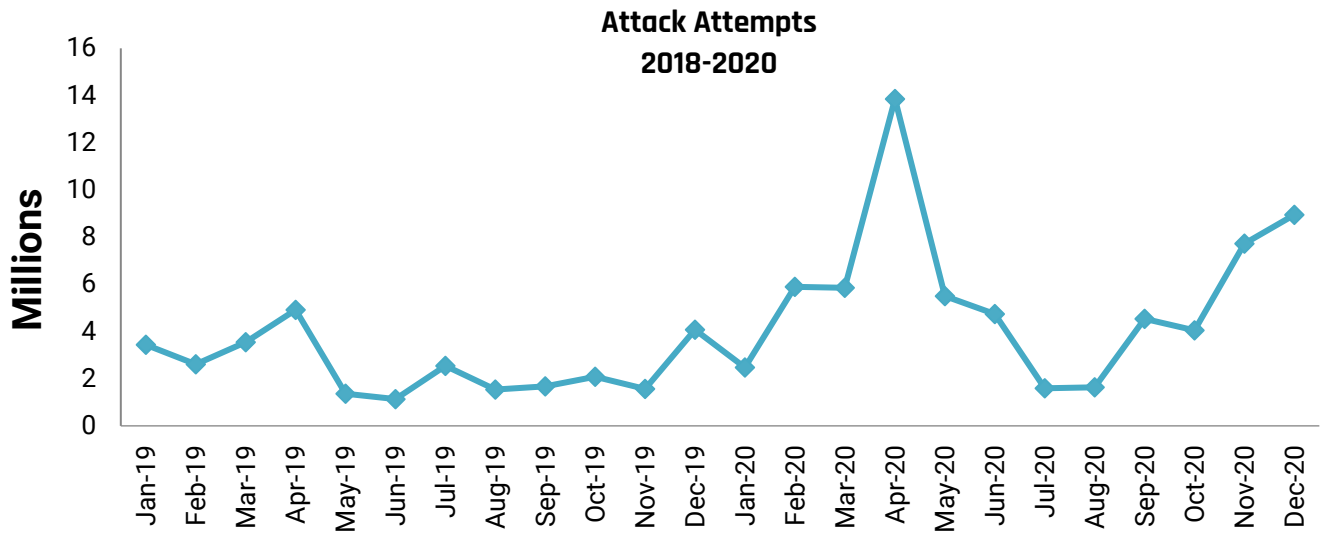


The origins of the attacks on the Commonwealth's network are monitored and tracked. CSRM receives threat intelligence information from multiple sources. This information is incorporated into the security monitoring systems that protect the Commonwealth's data from attack. In correlating this information with our intelligence partners, we are able to proactively block attacks from the points of origin before systems are compromised. During the past year, the top five countries where attacks against the Commonwealth originated were the United States, Russia, Brazil, Egypt and United Kingdom (tied for 4th place) and India. It is important to remember that attack origination does not define attack attribution.



Attack attempts are persistent. During 2020, over 66 million attack attempts were detected against Commonwealth systems. This is a rate of 2.12 attacks every second. The spikes in attack attempts are indicative of new types of attack traffic being observed. When an alert is triggered, the traffic is examined to determine whether it is malicious or authorized. Systems are adjusted to prevent the malicious attack

attempts from penetrating the COV network. Alerts for known authorized traffic are tuned out to reduce false positives. The drop in attack attempts following a spike is due to the tuning of the systems.

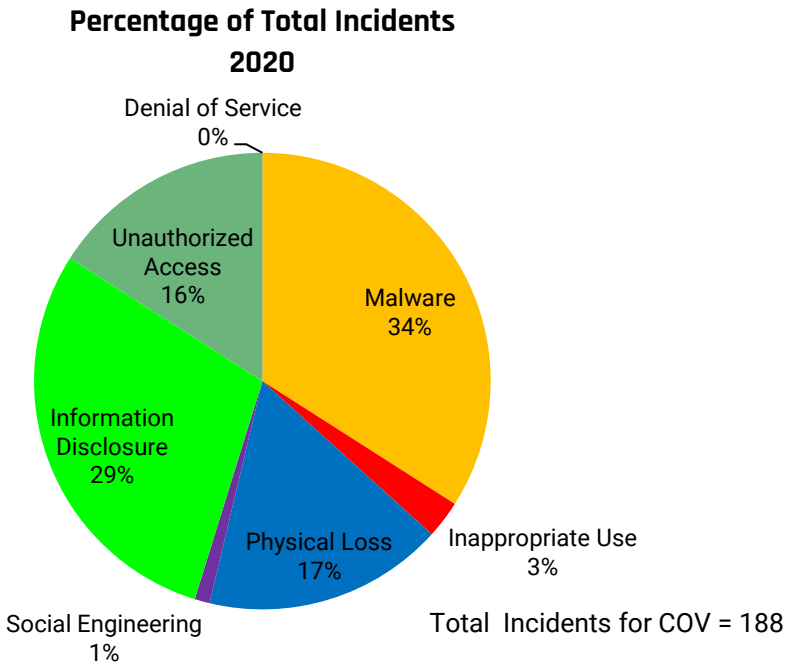


Incident trends by category

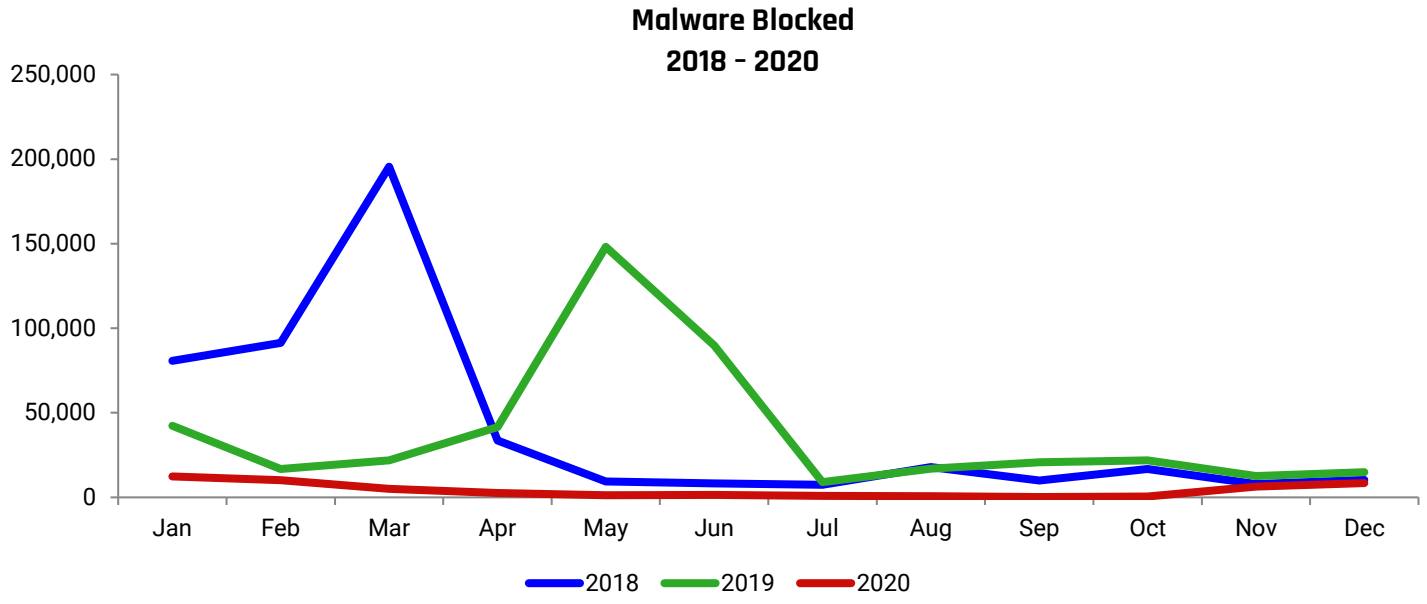
Reported security incidents are analyzed and grouped into one of the following categories described below:

- **Denial of service** - Loss of availability of a COV service due to malicious activity
- **Inappropriate usage** - Misuse of COV resources
- **Information disclosure** – COV data was exposed to recipients that did not have a need to know this data. COV systems were not accessed as part of the disclosure.
- **Malware** - Execution of malicious code such as viruses, Trojans, ransomware, spyware and key loggers
- **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

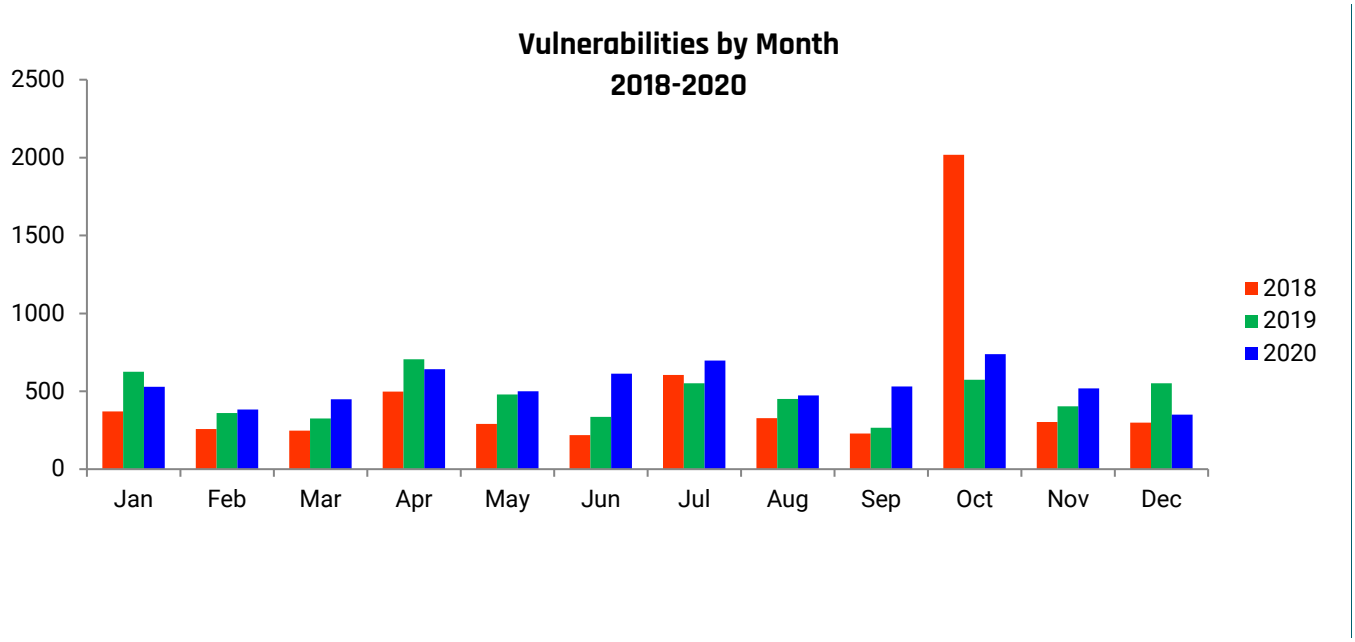
During 2020, malware was the top category for security incidents. Information disclosure was the second most frequent incident type, followed by physical loss, unauthorized access, inappropriate use and social engineering. The COV environment did not experience any denial of service (DOS) attacks during 2020.



Malware is blocked. The Commonwealth has multiple layers of protection against malware infections occurring on COV devices. During 2020, these layers of protection blocked approximately 50,099 pieces of malware. Even with multiple layers of protection, the Commonwealth still experienced 64 successful malware infections.



Vulnerability tracking is in place. As part of tracking threats to the Commonwealth, CSRM monitors Commonwealth systems for newly discovered vulnerabilities and incorporates them into a weekly advisory. This advisory is distributed to localities, state agencies and higher education institutions. In 2020, the advisory identified 6,425 vulnerabilities that could affect Commonwealth systems. This is a 14% increase over 2019. ISOs can use this information to ensure that critical vulnerabilities are being patched in compliance with security standards.

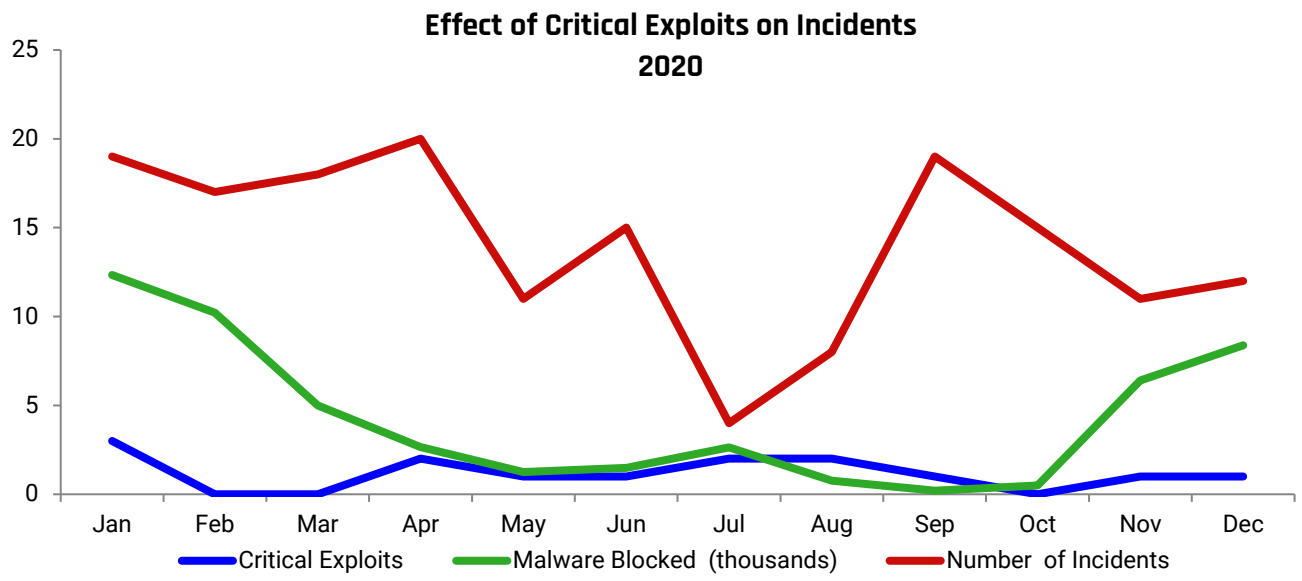


Critical exploits in the wild decreased by 92% from the previous year. Zero day vulnerabilities are newly discovered vulnerabilities that do not have patches available. These vulnerabilities are prime targets for attackers. Attackers develop exploit code using these vulnerabilities to install malware on a device before the manufacturer can provide an update or patches can be applied. As attackers publish the exploit code in the wild, these zero day vulnerabilities pose an increased risk to the environment.

During 2020, the total number of critical exploits tracked by CSRM decreased from 181 to only 14, a 92% decrease. As more and more data has been collected about the systems and technologies that are in use throughout the Commonwealth, security analysts have been able to fine-tune vulnerability reporting to focus on the products that are being used. This tuning resulted in a decrease in the number of critical vulnerabilities being tracked.

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.

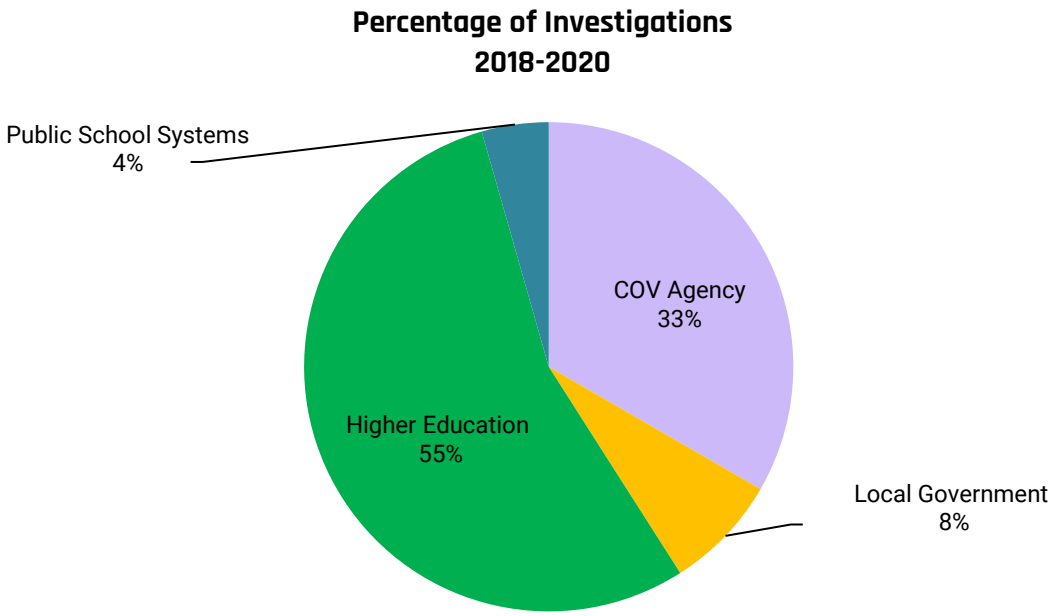
CSIRT analyzes each incident to determine the root cause and uses the information to strengthen protections to mitigate the risk of future attack. However, critical exploits still remain a risk, particularly zero day exploits for which no patch or fix is available.



Cyber intelligence from Commonwealth partners

The information received from Commonwealth partners includes data involving state and local governments, higher education and public schools 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 2020, the Commonwealth experienced 1,780 alerts resulting in 246 investigations. This was a 47% decrease in the number of investigations and an 89% decrease in the number of alerts. There were fewer alerts in 2020 compared to 2019 because of the spike in alerts caused by one significant breach in 2019 mainly experienced by higher education institutions (MyFitnessPal).

The following chart shows the percentage of investigations by type of entity.



Cyberattacks against Virginia's higher education systems and users continue. During 2020, higher education continued to be the most targeted group of public sector institutions in Virginia. This is due to the more open environment, financial opportunities, wealth of personal identifiable information and valuable confidential research found in most higher education institutions. Institutes of higher education had 583 vulnerabilities, 141 compromised accounts, 89 malware infections and 3 cyberattacks reported by Commonwealth partners. Attackers are looking to exploit the vulnerabilities in higher education systems to gain control of systems, to perform reconnaissance to be used in future attacks, to deliver malware to/from the infected devices and to compromise the confidentiality, integrity, availability of systems and data.

Most higher education institutions in Virginia are governed by the *Restructured Higher Education Financial and Administrative Operations Act of 2005.* This act gives them operational autonomy over their information technology without being subjected to any centralized oversight authority related to IT security by VITA. However, CSRM recommends that higher education institutions be subject to IT security oversight similar to the oversight that is provided to executive branch agencies.

The below table summarizes the data received from the MS-ISAC during 2020. MS-ISAC is an organization that is comprised of state government, local government and tribal territories. They monitor the intelligence community and the internet for attacks against their members. As this data only contained alerts that were identified by the MS-ISAC, the potential of additional data loss is possible.

Security investigations by category

	Higher education	Local government	Public school systems	COV agencies
Accounts compromised	90%	4%	3%	3%
Malware infections	29%	0%	0%	71%
Cyberattacks	9%	0%	0%	91%
Software vulnerabilities	46%	24%	6%	24%
Other miscellaneous attacks	0%	0%	0%	100%
***Potential loss associated with records exposed**	$92,208	$19,776	$9,605	$36,480

*Potential loss associated with records exposed assumes records were exposed. Costs were calculated using the per capita cost by industry of a data breach as determined in the Ponemon Institute's *Cost of a Data Breach Study: Global Analysis* report.

CSRM provided 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, 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 performed a comprehensive security review to ensure the systems and infrastructure supporting the elections were secure. In partnership with the Department of Elections, CSRM electronically scanned all election systems for security vulnerabilities. In addition, a cybersecurity command center was established in order to handle any issues occurring on Election Day. CSRM also worked with the 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 to partner with the Department of Elections to provide support for upcoming elections.

CSRM coordinates an annual Cybersecurity Tabletop Exercise. In the midst of the COVID-19 pandemic, SAIC as the Multisourcing Services Integrator (MSI), in cooperation with the Virginia Information Technologies Agency (VITA), hosted the second Cybersecurity Tabletop Exercise, performed on an enterprise level, in the Commonwealth of Virginia. The 2020 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 that 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 that areas of improvement could be addressed.

Significant conclusions from the exercise were:

- 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. It is clear that 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.

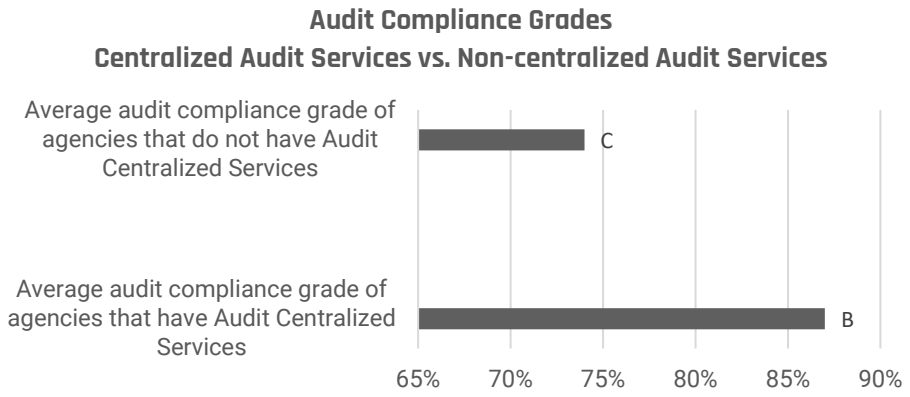
CSRM centralized services

To supplement agency IT security programs, CSRM offers a shared centralized services. These services include IT security auditing, ISO 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 enhance information security and compliance in the Commonwealth.

Centralized IT security audit services

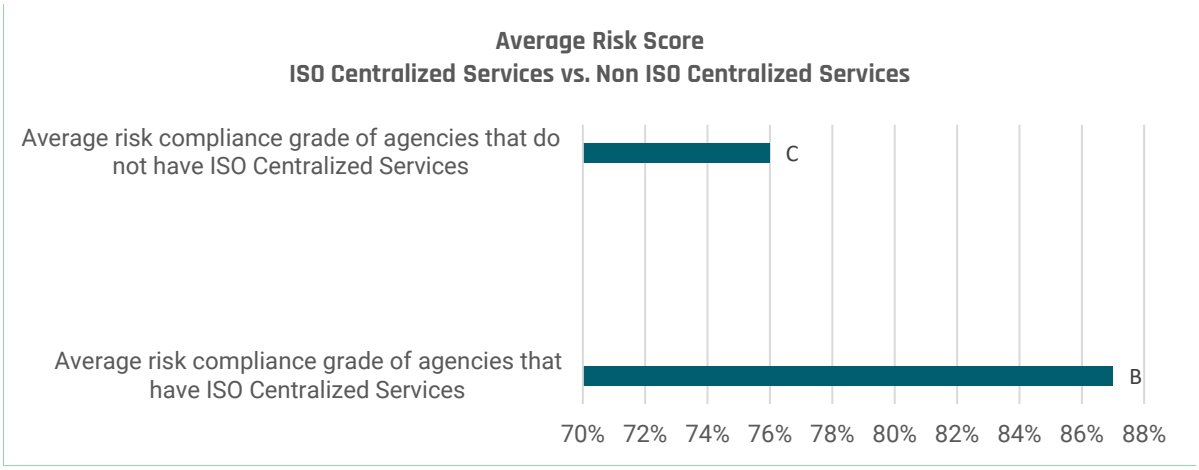
In the past, many agencies did not perform required IT security audits because they did not have their own IT auditing departments or otherwise did not have funds to hire outside auditing resources. The centralized IT auditing service assists these agencies with documenting their IT security audit plans, conducting IT security audits, and supporting agency efforts to create and submit corrective action plans to address the issues found during audits. Currently 32 agencies have elected to use the shared centralized audit service to perform IT security audits. The average audit score for agencies that have audit centralized services is a B (87%); a 3% increase from 2019. Agencies utilizing audit centralized services are outperforming non-audit centralized services agencies by 13%, demonstrating the benefits of using the service. Auditing is a valuable tool that

identifies issues and helps agencies strengthen their overall security posture, and the Commonwealth as a whole.



Centralized ISO Services

The centralized ISO service currently supports 32 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 (87%); a 4% decrease from 2019, taking them from an A to a B. The average risk score for agencies not utilizing ISO centralized services is a C (76%); a 5% increase from 2019. Agencies utilizing ISO centralized services are outperforming the average risk score for agencies not utilizing ISO centralized services by 11%, indicating that ISO service agencies have supported Commonwealth efforts towards compliance. ISO centralized services anticipates additional improvements in risk compliance.

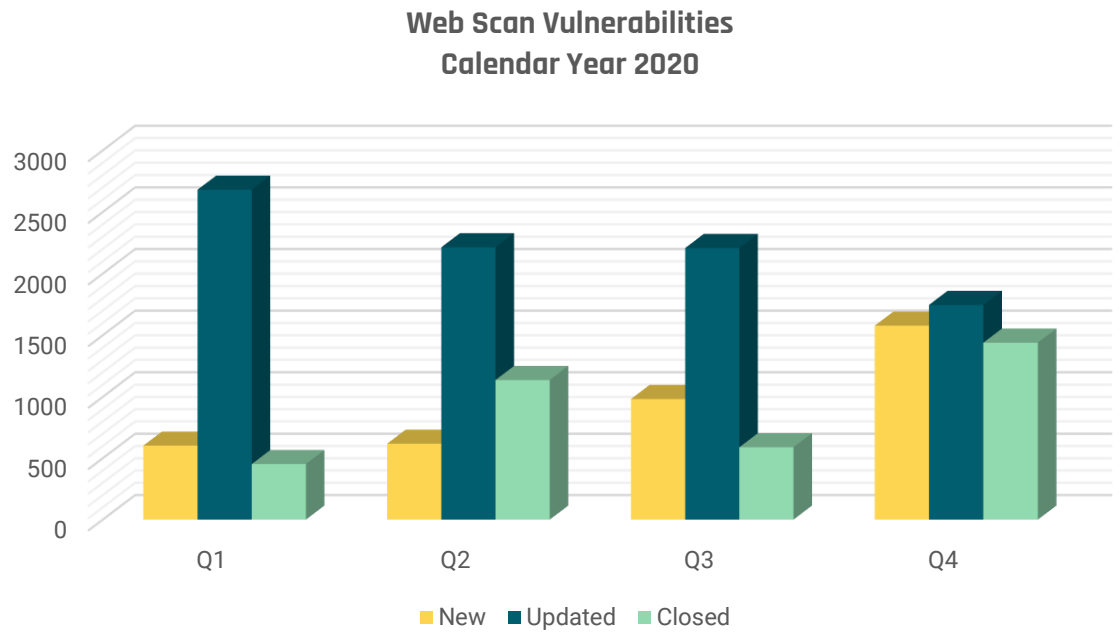


Web application vulnerability scanning program

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 scans over 6,000 public sites (targets) every quarter. Since the scanning service began, over 10,000 vulnerabilities have been identified and more than 90% of these vulnerabilities have been corrected.

Additionally, CSRM scans private sensitive sites with operating system level scans and application level sites for sensitive applications.

The detection rate for new alerts increased over the year. An increase in new alerts indicates that there is a need for ongoing remediation efforts. Updated alerts (repeat scan findings) declined in the last year. A decrease in repeat findings indicates that agencies are fixing the issues that are identified in the vulnerability scans.



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

VITA also updated requirements in the IT Risk Management Standard regarding vulnerability scans in 2020. A Agencies are required to remediate "vulnerabilities that are rated critical, high, or otherwise identified by CSRM, 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 that this requirement will further ensure that significant vulnerabilities are addressed quickly to protect Commonwealth information.

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

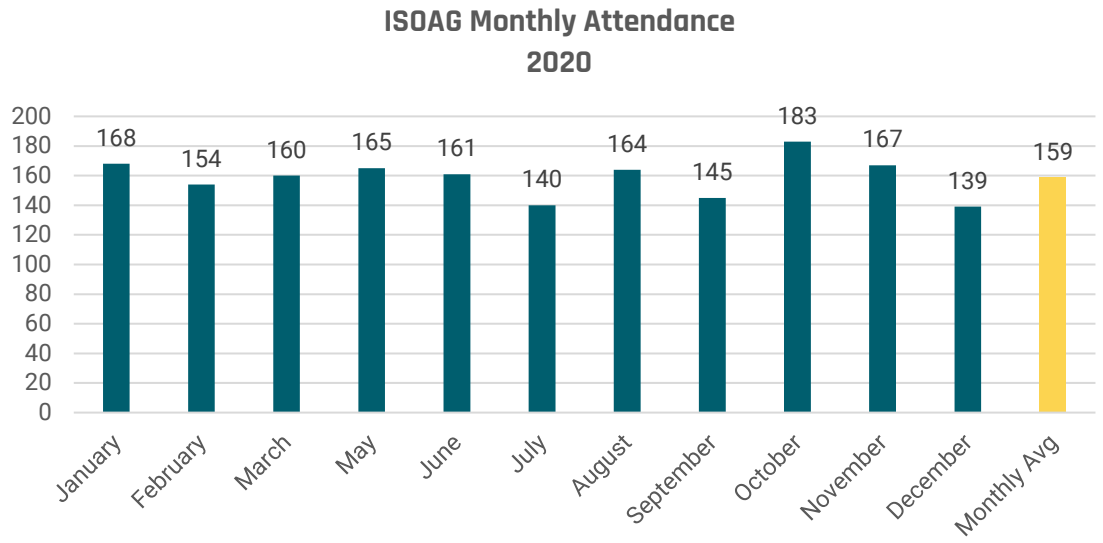
Per §2.2-2009 (B.1) of the Code of Virginia, the CIO is required to report "*the results of security audits, the extent to which security policy, standards, and guidelines have been adopted by executive branch and independent agencies, and a list of those executive branch agencies and independent agencies 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 maturity that provides additional insight into agency programs and will enable the Commonwealth to improve security endeavors.

Commonwealth Information Security Officers Advisory Group

The Information Security Officers Advisory Group (ISOAG) is a dynamic group of information security professionals, open to all state and local government personnel. The group's goal is to improve the security posture of the Commonwealth through the exchange of IT security knowledge. Every year, CSRM conducts monthly meetings with knowledgeable speakers from government and private sector organizations to share their information security expertise at no cost to attendees. The monthly average attendance for 2020 was 159 attendees per meeting. This was an increase of 13% from the monthly average attendance from 2019.

Meeting attendance allows members to earn continuing professional education credits (CPE), a requirement necessary for security professionals to maintain their security certifications and memberships in global security organizations. It also provides an opportunity to share best practices, allow feedback on proposed policy changes and receive information concerning local training opportunities. Meeting presentation materials are posted to the VITA website as an additional resource to the group. Due to the pandemic in 2020, the ISOAG meetings with the exception of January, February and March were conducted via web meetings. CSRM anticipates using web meetings for the foreseeable future to provide security training for agency and local security professionals in the Commonwealth. Below is a chart that displays the ISOAG monthly attendance from 2020.



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 IS Council recommends strategic direction for information security and privacy initiatives in the Commonwealth. 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.

In addition to reviewing proposed changes to security policies and standards, in 2020 the IS Council contributed to the ransomware attack preparedness study in response to new Virginia statutory requirements. This resulted in a comprehensive report that analyzed the risk ransomware posed to the Commonwealth and

provided recommendations and best practices to prevent these attacks. 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 engage 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 helped the Department of Treasury determine how much cyber liability insurance is needed in the event a system is breached or incapacitated. It also allows 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 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. Potential impacts of each risk are discussed and possible mitigating controls. The committee documents these risks and reports risk alerts to escalate risks and issues that may have a significant impact on the enterprise or customer agencies, as necessary. As a result, VITA and the associated service providers have 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. This supports agencies to make sure the applications in the cloud are secure, dependable and resilient. ECOS (Enterprise Cloud Oversight Service) 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 the provider's applications running 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 by the agencies.

Commonwealth IT audit compliance program

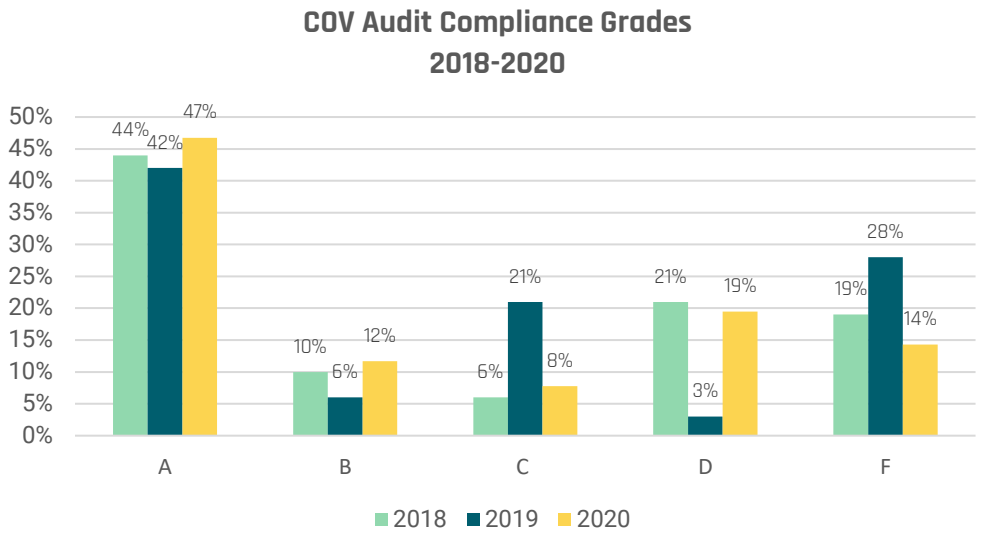
The Commonwealth IT audit compliance program includes review and oversight of the agencies' IT auditing activities, including submission of audit plans, completed audits and corrective actions. The completion of these items are used to determine the agencies' overall audit program score.

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

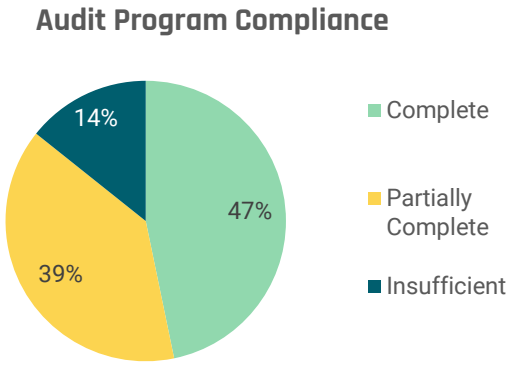
quarterly updates to their IT security audit findings, and completion of required IT security audits. The compliance grades provide a familiar measurement tool to reflect the degree to which agencies are completing their necessary IT security audit requirements. In addition, the compliance grades clearly identify agency IT audit strengths and opportunities for improvement.

Overall, agency audit programs compliance has improved from the previous year, with more agencies earning "A" and "B" grades. While the percentage of "D" grades increased, the percentage of "F" grades decreased. CSRM anticipates that audit compliance will continue to improve as agencies use the tools afforded them, including audit centralized services, audit standards, and templates.



Key Commonwealth security audit compliance metrics and analysis

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



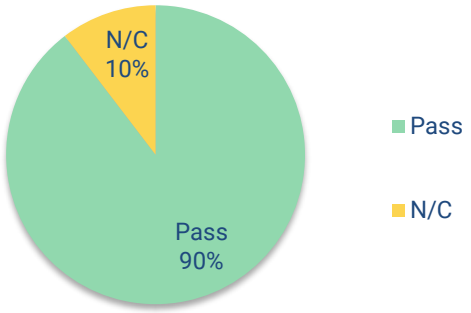
Audit program compliance increased by 5 percent

Overall agency IT security audit program compliance increased. 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, and updating the status of corrective action plans for IT security findings discovered during the audits. Audit program compliance has increased from the prior year, with 47% of agencies having implemented a comprehensive audit program in 2020. This increase can be attributed to the improvements in submitting quarterly remediation updates. CSRM anticipate audit program compliance will improve as agencies understand the importance of completing their audit requirements.

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 within the required timeframes. In 2020, 90% of agencies submitted an IT security audit plan. These results have remained the same for the last three years. While most agencies are completing this requirement, there are still a few agencies that do not 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.

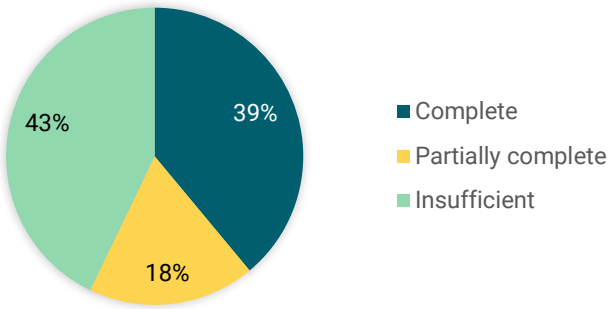
Audit Plan Status



IT security audit plan status remained the same

Agency three-year audit obligation metrics declined slightly. Of the agencies that have established an audit plan, 39% have fulfilled their obligation to audit every sensitive system at least once every three years, a decrease of 1% from last year. The percentage of agencies with insufficient three-year audit obligations also increased slightly. This decrease is likely attributed the challenges of auditing applications during the global pandemic that occurred during most of 2020. CSRM anticipates that this metric will progress as agencies adapt to auditing applications in this new environment going forward.

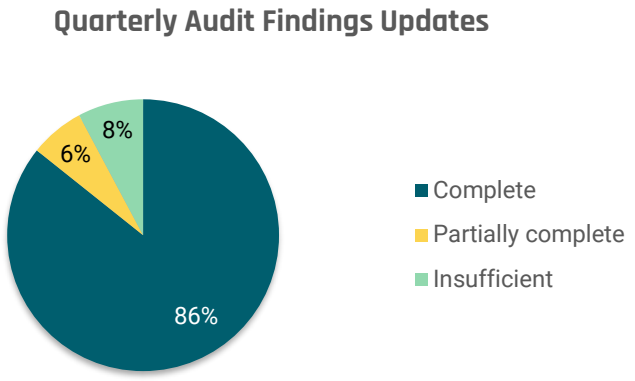
Three-year audit obligation



Three-year audit obligation completion decreased by 1%

Most agencies that perform IT security audits provide the required quarterly updates to the findings. Our analysis found that 86% of agencies that submitted audit findings provided the required quarterly IT security audit updates for open IT security audit findings. In addition, the percentage of agencies that had insufficient

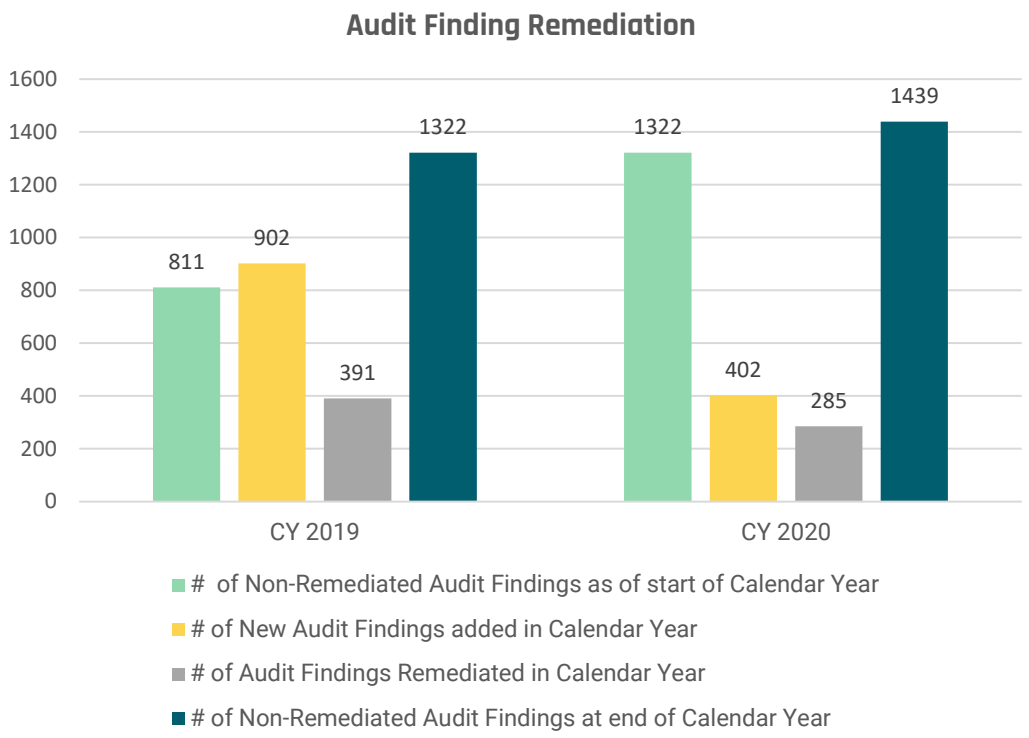
quarterly updates decreased by 12% from the prior year. CSRM anticipates this trend will continue as agencies are encouraged to report their progress toward closing the findings and prioritize their resources to address the most significant findings first.



Audit findings updates increased by 9%

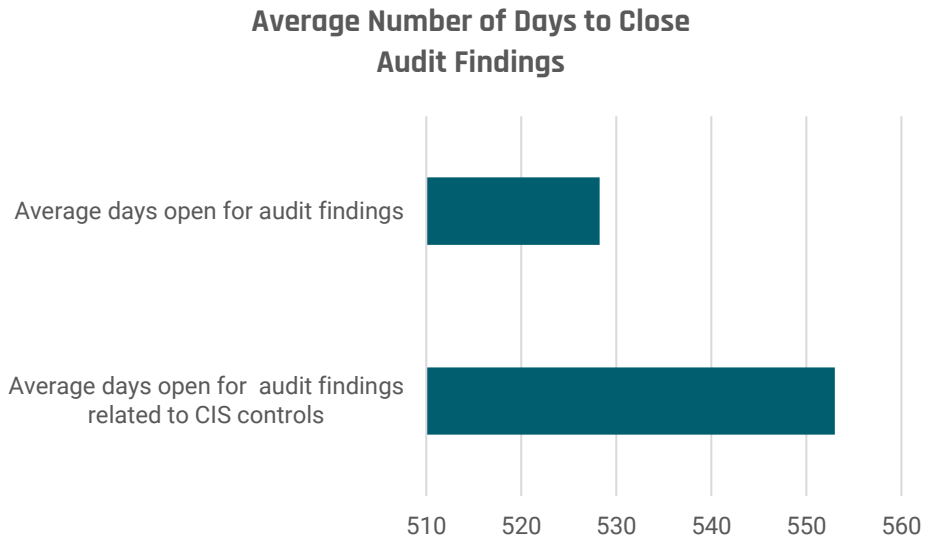
Audit Findings by Calendar Year Analysis

Far fewer audits were submitted in calendar 2020 than in the previous year. As a result, agencies reported only 402 new audit findings in 2020, compared to 902 new audit findings reported in 2019. Remediation of audit findings is also at a slower pace in 2020. 391 audit findings were remediated in 2019, but only 285 in 2020. As of the end of calendar year 2020, there were still over 1,400 audit findings in need of remediation. This decline can be attributed to disruptions caused by the COVID-19 pandemic during the 2020 calendar year. Many agencies focused a majority of staff resources on maintaining critical business operations and were not able to address findings in a timely manner. The COVID-19 pandemic also caused a drop in audits conducted in 2020, which resulted in a lower number of audit findings created. CSRM anticipates that agencies will devote the appropriate resources to remediate audit findings in a timely manner. 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 that they have implemented adequate mitigating controls until the issue can be resolved.



Audit findings are not quickly addressed. CSRM analyzed the average number of days to it took to close audit findings in 2020. It took an average of 528 days before an audit finding was resolved and closed. 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, was even longer. Some of the delays may be attributed to IT resources being shifted from audit resolution to address remote work issues during the global pandemic.

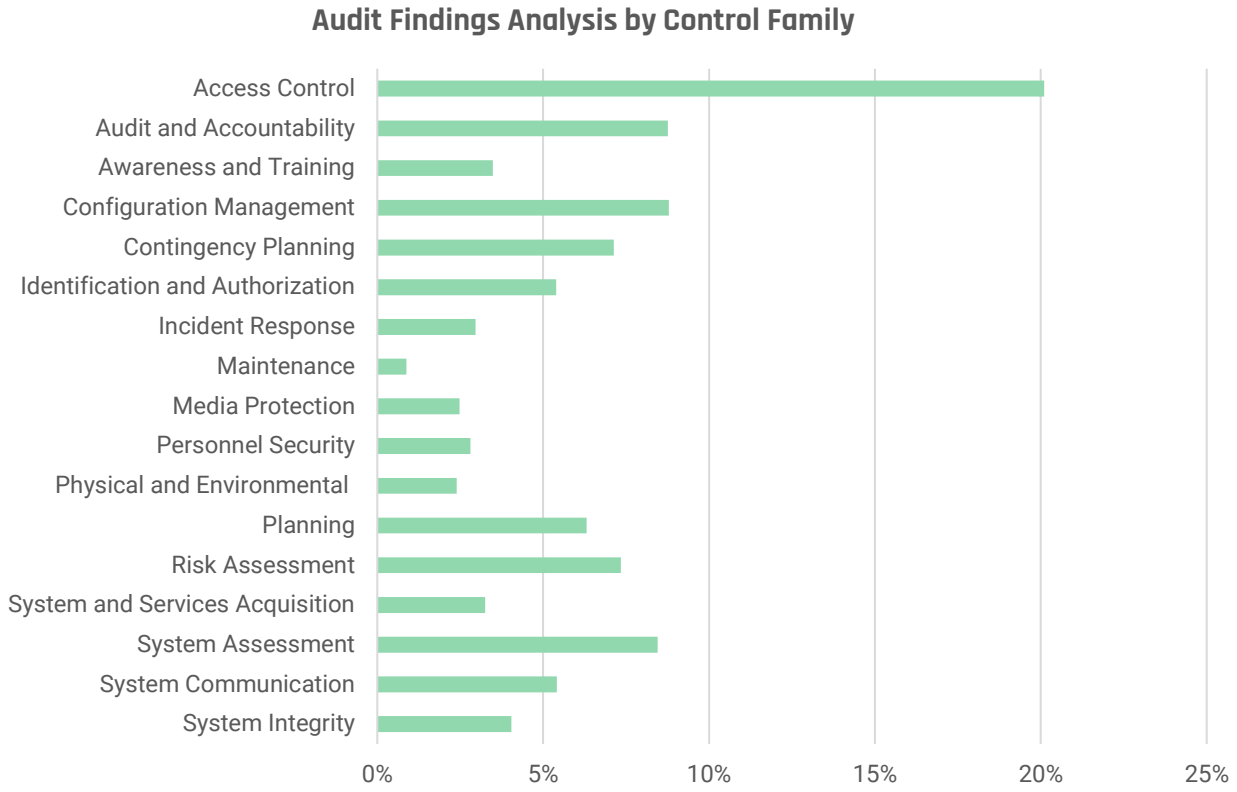
We recommend that agencies reevaluate their process to address the issues identified in audit and risk findings and dedicate the appropriate resources to remediate these findings more timely. Agencies should prioritize and remediate findings by criticality, first addressing the findings in any areas associated with critical controls.



CSRM analyzed IT security audit findings by security control family. Commonwealth security standards refer to 17 information security control families or groupings of similar IT security controls that are designed to support secure and resilient IT systems. Based on an analysis of the IT audit findings for the Commonwealth, the top three IT security controls families where audit issues were identified were:

- Access control family (20%)
- Audit & accountability family (9%)
- Contingency planning family (9%).

These are the same control families that had the most findings as last year. CSRM will use these results to provide agency training, develop further security guidance and offer tools for the agencies to address the control gaps in these areas.



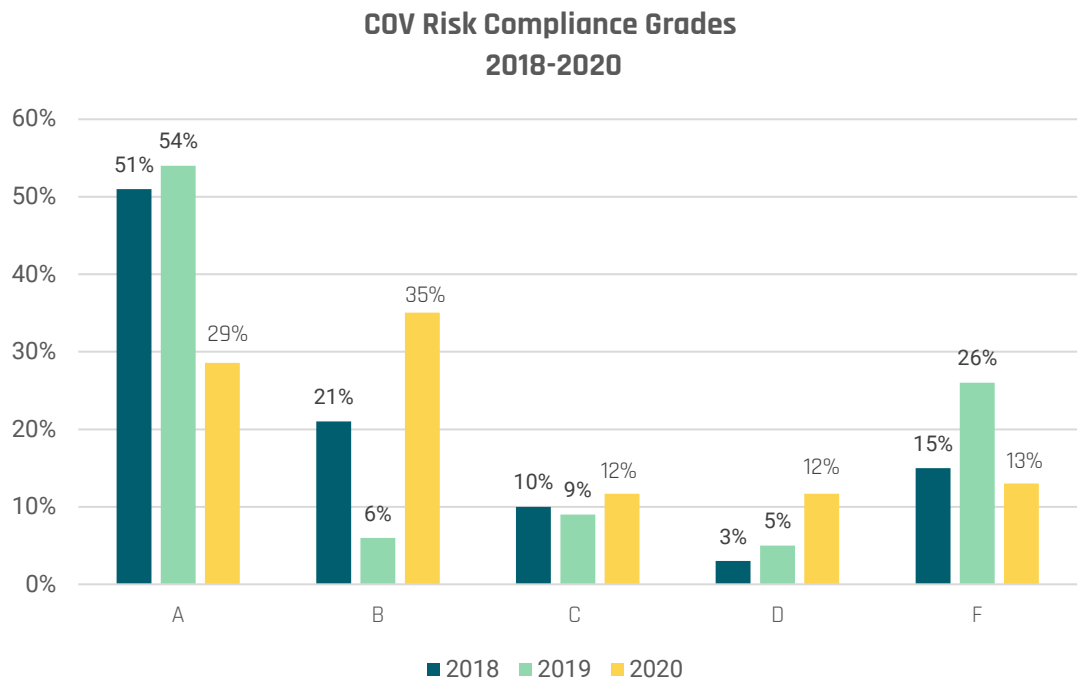
Commonwealth IT risk management program

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.

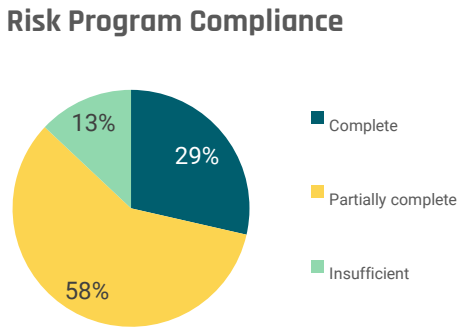
Risk compliance report card

The risk compliance grades reflect the varying maturity of risk management programs at the agencies. The agencies are graded using a ten point letter grade system. While the percentage of agencies with "A" grades has decreased in 2020 there was a 30% increase in agencies with "B" grades. Also noted was an increase in

"C" and "D" grades. "F" grades decreased by 50%. This risk metric was impacted by a new requirement that agency ISOs report to their agency head, the constraints imposed by the COVID-19 pandemic and by agencies inconsistency in reporting corrective actions related to open risk findings. CSRM anticipates risk program compliance grades will continue to improve as agencies comply with ISO reporting requirements, continue to complete IT risk assessments, and provide quarterly updates on the corrective actions taken to address risk assessment findings.



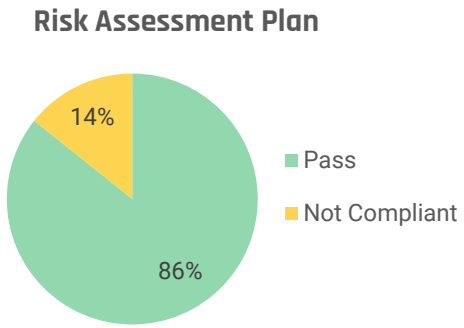
IT risk management program monitoring



Overall risk program compliance decreased by 4%

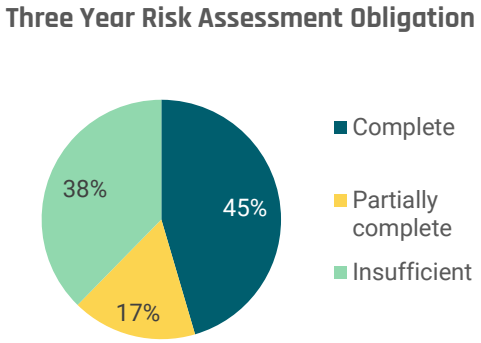
Risk management program compliance declines. Risk management activities experienced a slight downturn during 2020. Risk program compliance decreased by 4% from a 3% increase last year. There was a change in how we calculated the risk metric in 2020 that contributed to the decrease. CSRM recommends agencies continue implementing comprehensive risk management programs by providing additional attention to business impact analysis and risk assessments and dedicating the necessary resources to their IT risk management programs.

Many agencies submit their risk assessment plans. Agencies are required to submit a risk assessment plan on an annual basis identifying their plan to complete the required sensitive system risk assessments. Risk assessment plan submissions experienced a 4% increase in 2020.



Risk assessment plan submissions increased by 4

Three-year risk assessment obligation declines. Agencies are required by IT security standards to submit risk assessment plans for their sensitive IT systems. Risk assessments are central to ensuring agencies are monitoring and mitigating critical risks. This metric details agencies submission of risk assessments for sensitive systems at least once every three years. As more agencies enroll in the centralized ISO services and dedicate necessary resources to their risk programs, we anticipate improved compliance.



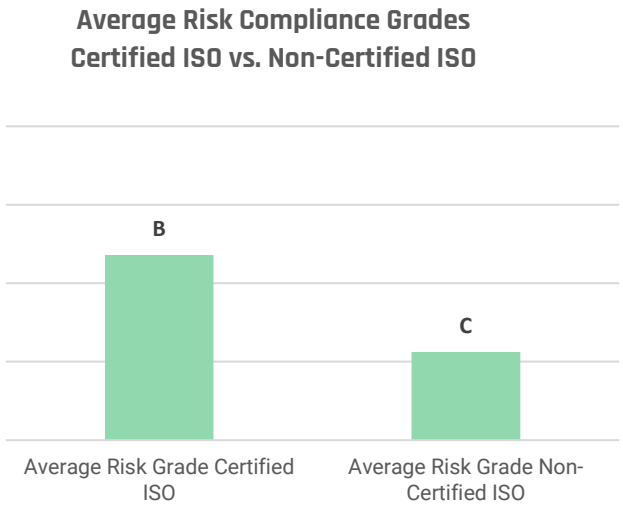
Three-year risk assessment obligation decreased by 4%

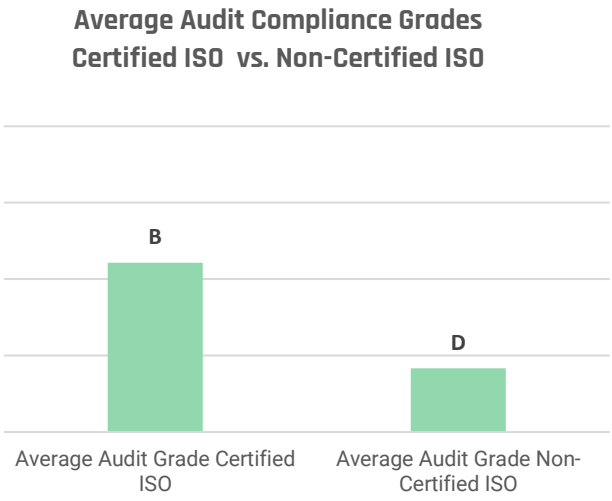
The percentage of agency ISOs that are certified has declined slightly since last year. 86% of ISOs are certified in 2020 compared to 90% in 2019**.** ISO certification is one way to demonstrate an ISO's proficiency in managing the agency's IT security program. The Commonwealth ISO certification demonstrates 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 2020:

- Tobacco Region Revitalization Commission
- Virginia Commission for the Arts
- Frontier Culture Museum of Virginia
- Indigent Defense Commission
- Motor Vehicle Dealer Board
- Science Museum of Virginia
- Southwest Virginia Higher Education Center

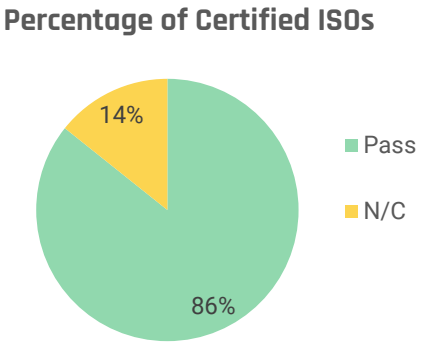
- Virginia Department of Emergency Management
- Virginia Foundation for Healthy Youth
- Virginia School for the Deaf and Blind

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





CSRM recommends that these agencies commit to recruiting, hiring, and training ISO staff to initiate improvements in their agencies' IT security posture. Recent changes to SEC501 IT security standard require that the ISO report to the agency head. CSRM is monitoring compliance with this metric and using it as criteria for each agency's risk compliance score.



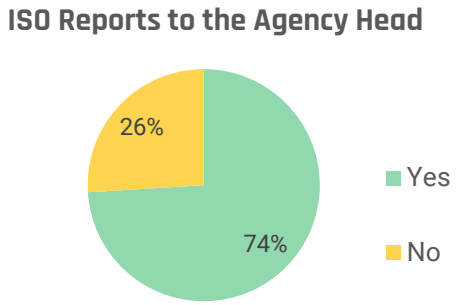
The percentage of ISOs that are certified decreased by 4%

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. This metric was new in 2019 and is now a part of the 2020 risk program compliance score. Most agencies (74%) have met this requirement, a 25% improvement from last year.

Agencies where the ISO reports directly to the agency head have an average risk grade of "B," while agencies where the ISO does not report to the agency head have an average risk grade of "D." While we recognize that each agency has its own unique organization, CSRM recommends that agencies take the necessary steps to ensure that the ISO reports directly to the agency head to confirm that information security has the needed

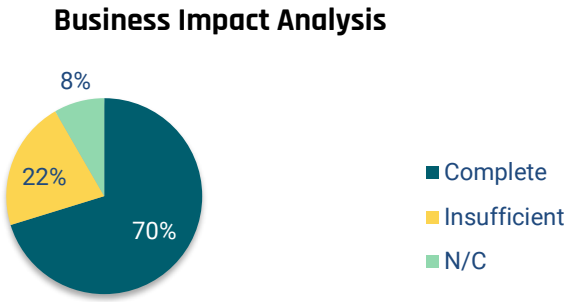
emphasis and support in every agency in the Commonwealth. The following ISOs were not reporting to agency heads and do not have an approved exception in place.

- Department of Fire Programs
- Department of Conservation and Recreation
- Department of Elections
- Department of Forensic Science
- Department of Forestry
- Department of Military Affairs
- Department of Professional and Occupational Regulation
- Department of Rail and Public Transportation
- 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
- Virginia Retirement System

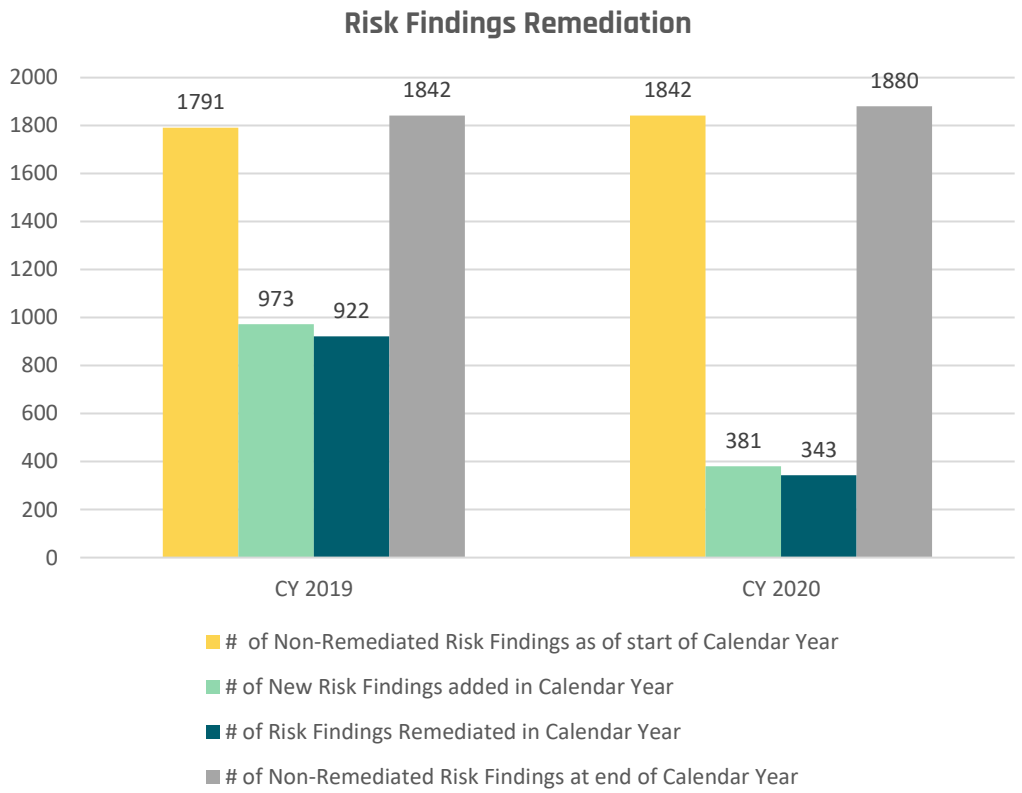


ISOs that are certified increased by 25%

BIA metrics declined. The percentage of completed BIAs had a decrease of 11%. This indicates a need for greater emphasis in this area. The information documented in BIAs are a primary input to data and application sensitivity, risk assessments, contingency plans and system security plans. This improvement can be achieved by obtaining support from VITA centralized services, if needed, and increased attention on addressing this key metric.

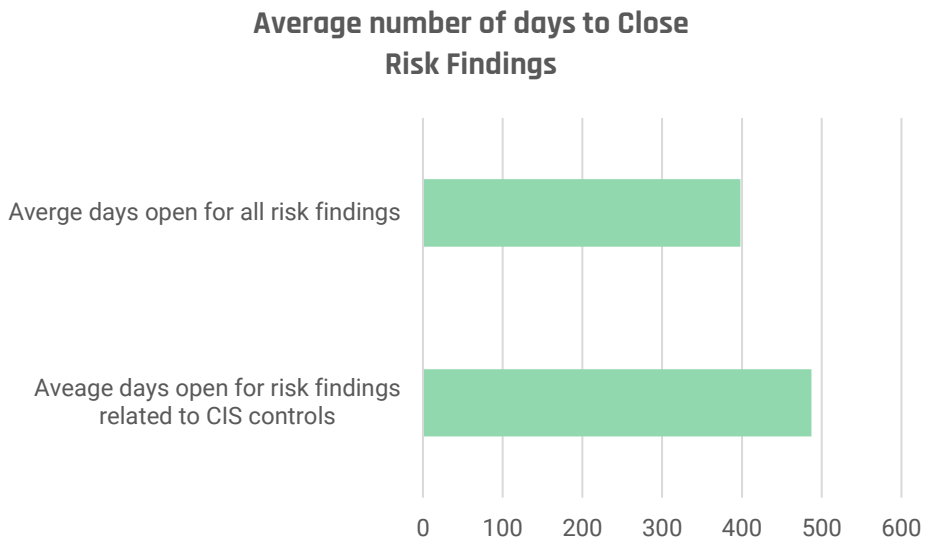


Agency risk assessments generate findings which require quarterly updates. In 2020, there were 381 new risk assessment findings compared to 973 new findings created in the previous year. This was due to fewer risk assessments being performed. Analysis indicates that remediation of risk findings also dropped significantly. 922 findings were remediated in 2019, but only 343 in 2020. As of the end of calendar year 2020, there were still 1880 risk findings requiring remediation. CSRM anticipates that remediation rates will improve as agency risk management programs mature.



Risk findings are not quickly addressed. CSRM analyzed the average number of days to it took to close risk assessment findings in 2020. Closed risk assessment findings had been open an average of 398 days before being resolved and closed. The average number of days to close findings associated with CIS controls, key controls that protect against attacks from known attack vectors, was even longer. While risk findings were closed more quickly than audit findings, improvement is still needed.

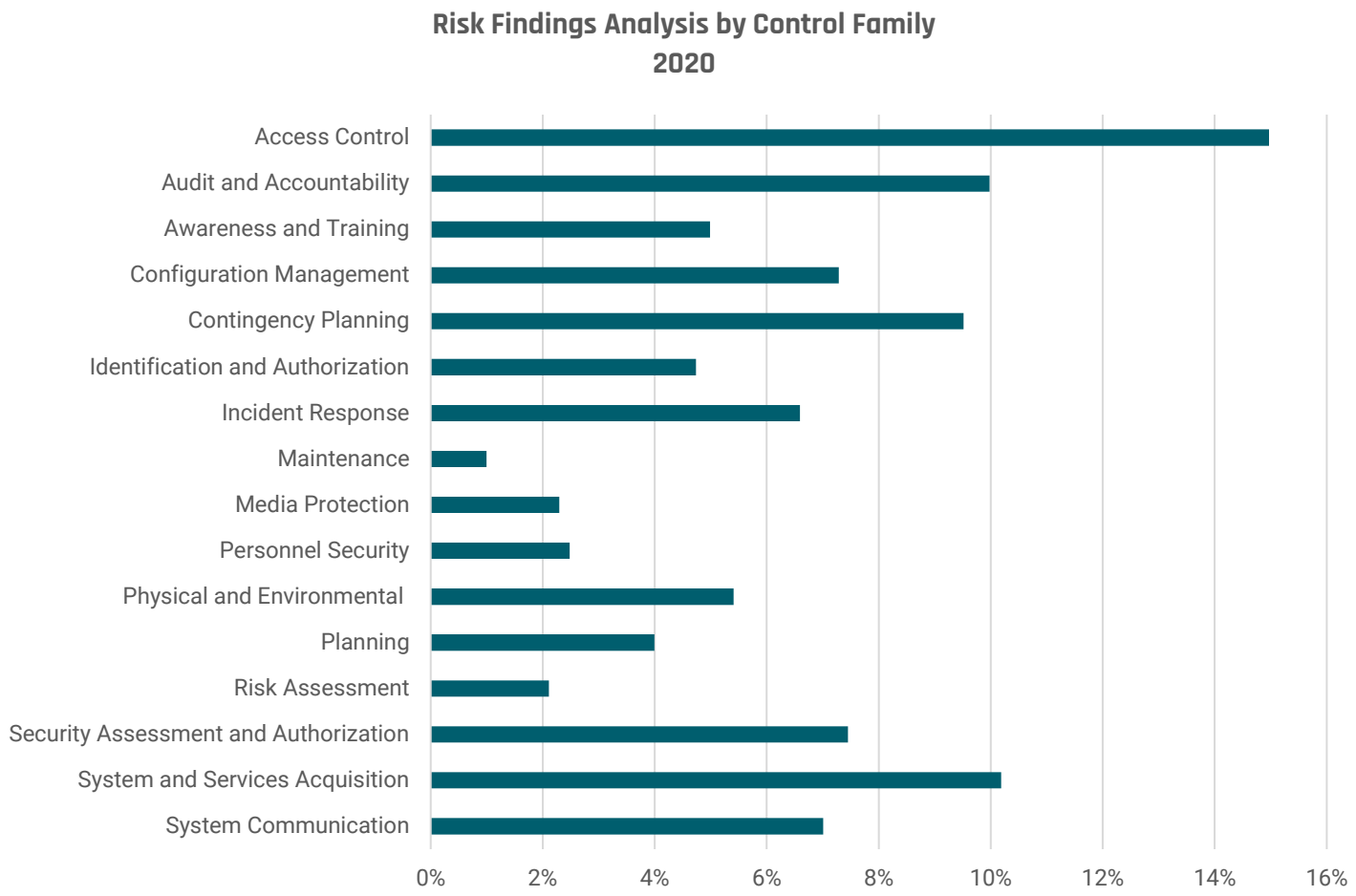
We recommend that agencies reevaluate their process and dedicate the appropriate resources to remediate these findings more timely. Agencies should prioritize and remediate findings by criticality, first addressing the findings in any areas associated with critical controls.



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. The security families that had the most IT risk findings were:

- Access control family (15%)
- System and services acquisition family (10%)
- Audit and accountability family (10%)

Poor access controls create an increased risk that agencies will be exposed to unauthorized access of data, fraud or disruption of IT services. To address this issue, VITA has made a budget request for resources to implement an identity access management (IAM) solution for the Commonwealth. IAM will create an automated framework for policies and technologies to ensure that users are properly authorized and have appropriate access to technology resources.



Nationwide Cyber Security Review

National Cyber Security Review Analysis

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. Each agency participating in the survey, ranked their performance on a maturity scale for five core cybersecurity functions: *identify, protect, detect, respond and recover*.

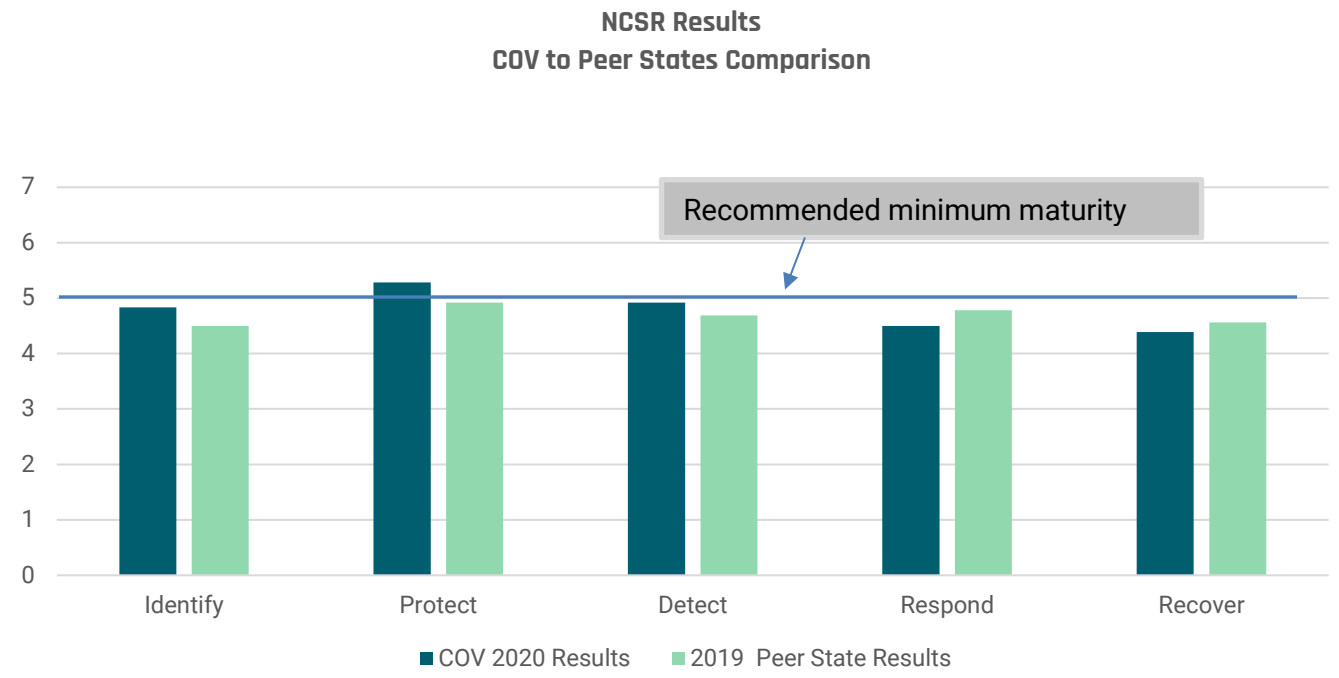
> ***Identify*:** The activities measured for this function are key for an agency's understanding of their internal culture, infrastructure and risk tolerance.
>
> ***Protect*:** The activities under the protect function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services.
>
> ***Detect*:** The quicker an agency is able to detect a cybersecurity incident, the better positioned it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the detect function pertain to an 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.

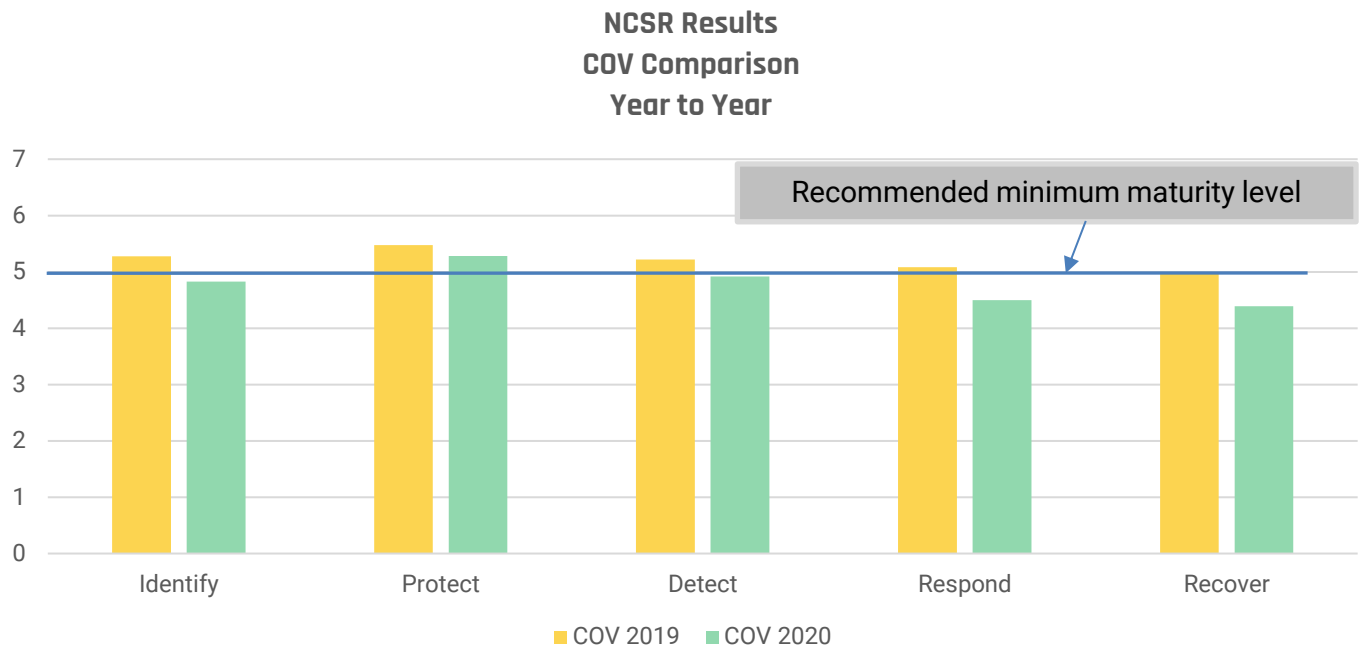
Using a maturity scale measurement, each agency evaluates itself on several activities that support each core function. The scale goes from one (activity is not performed) to seven (activity is optimized). NCSR recommends a minimum maturity level score of five.

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

Sixty-five agencies participated in the survey in 2020. The survey requires agencies to evaluate the maturity level of their processes and controls using the scoring described in the table above. On average, participating Commonwealth agencies rank themselves close to the recommended minimum maturity level score (of five) in all core cybersecurity functions. In addition, Commonwealth agency assessed themselves slightly above the national average of all peer states.

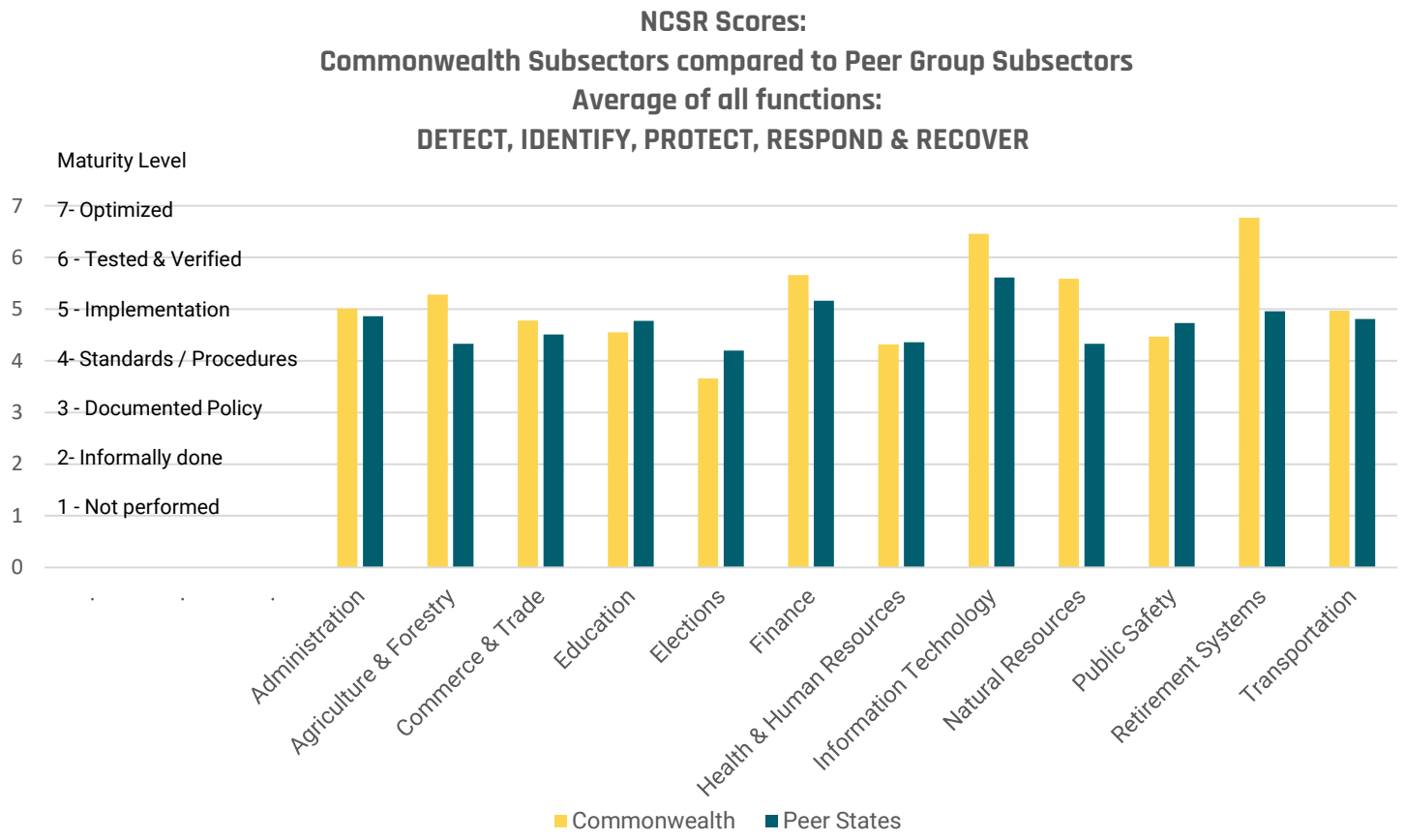


Commonwealth results declined from the prior year. Self-assessments scores for all agencies were slightly down in 2020 compared to the previous year. For the agencies that participated, the "Protect" function is consistently the most mature function and "Recover" is the least mature function. Agency results exceed the recommended minimum maturity level score of five for the "Protect" function in calendar year 2020 and nearly achieved the recommended score for the remaining functions.



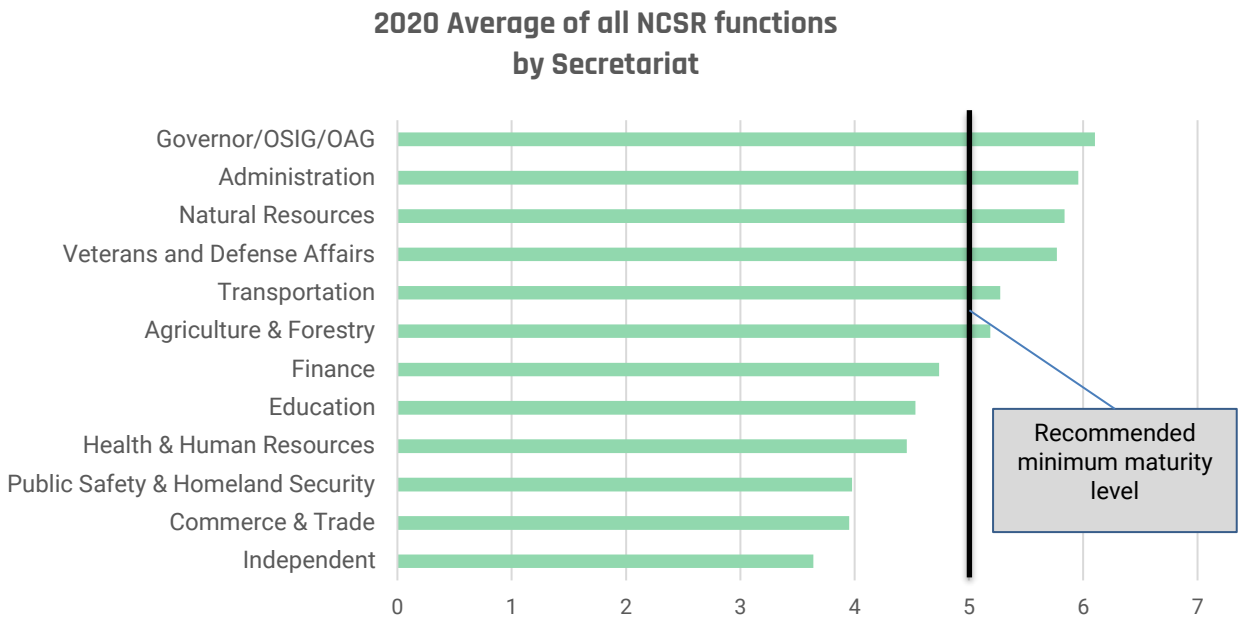
Commonwealth agencies compared well with their peers state agencies. MS-ISAC grouped all nationally participating agencies into peer group subsectors by government service/business function. CSRM combined COV agencies into similar subsector groups to compare. The results demonstrate that Commonwealth

subsectors self-reported maturity levels slightly higher on average than the maturity level of peer state subsectors. Commonwealth agencies in retirement systems, information technology, and finance subsectors rated themselves the highest compared to their peers.



NCSR analysis by secretariat

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



Cybersecurity framework – analysis by function

<u>Identify</u>
The activities under the "Identify" functional area are key for an agency's understanding of their current internal culture, infrastructure and risk tolerance. Immature capabilities in the identify function may hinder an agency's ability to effectively apply risk management principles for cybersecurity. By incorporating sound risk management principles into cybersecurity programs, agencies will be able to continuously align their efforts towards protecting their most valuable assets against the most relevant risks.

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.

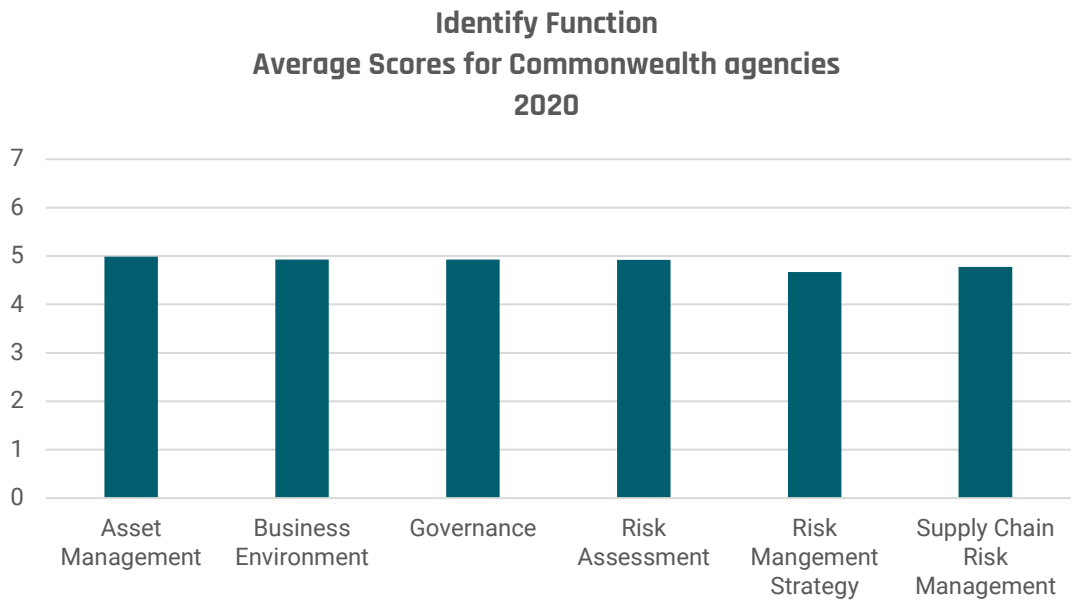
- The "Business Environment" category is related to how the organization's missions, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

- "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 mature 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.



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.

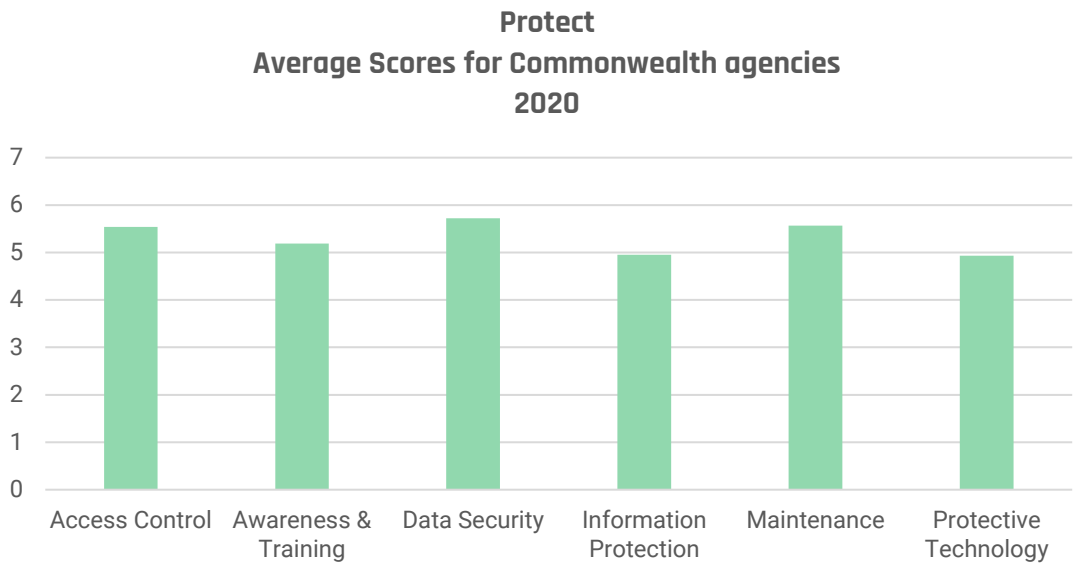
- “Data Security,” the most mature category for the Commonwealth in the Protect function, refers to the idea that information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.

- “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 least

mature 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.



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 in order to monitor logs efficiently and effectively.

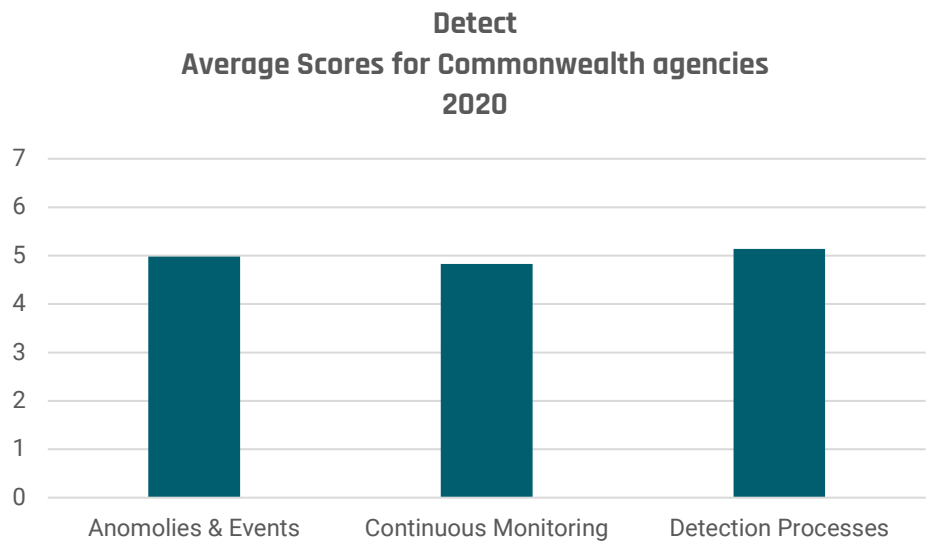
Within the Detect function, are the following categories:

- "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.

Compared to last year, these measures in the Detect function have decreased slightly. It is recommended that this decrease should be addressed right away by all agencies in view of the increase in cybersecurity attacks in 2020.



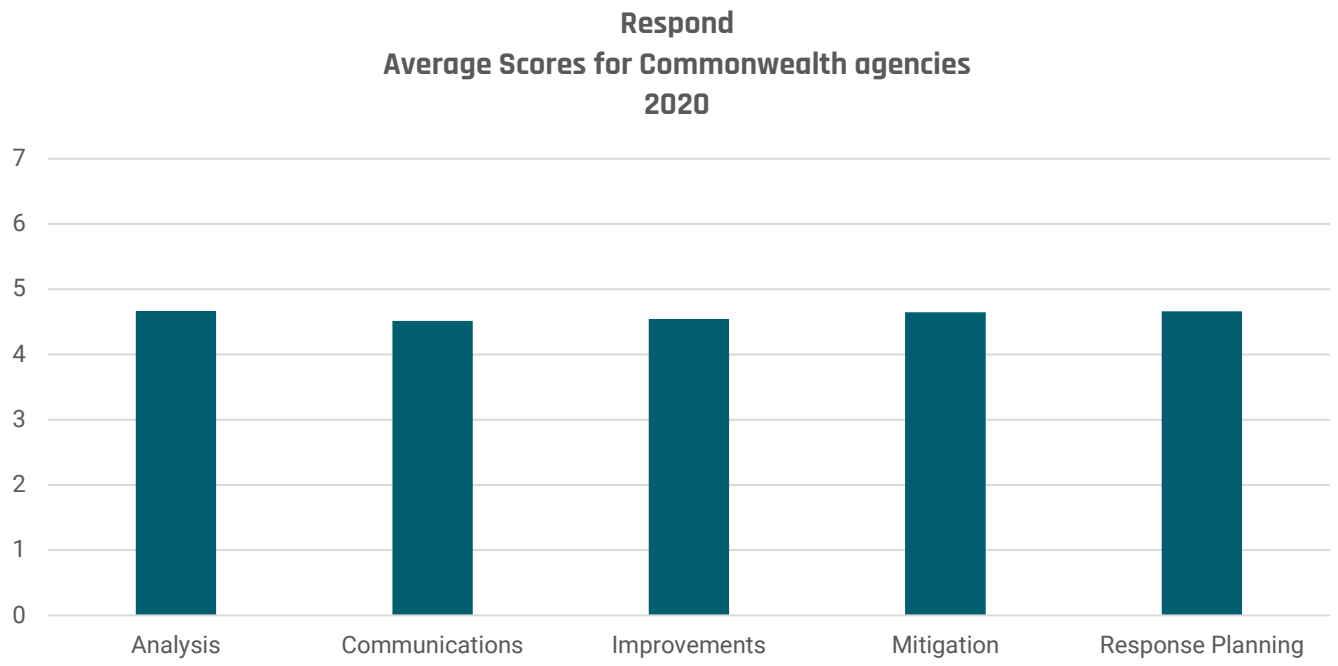
Respond

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.

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.

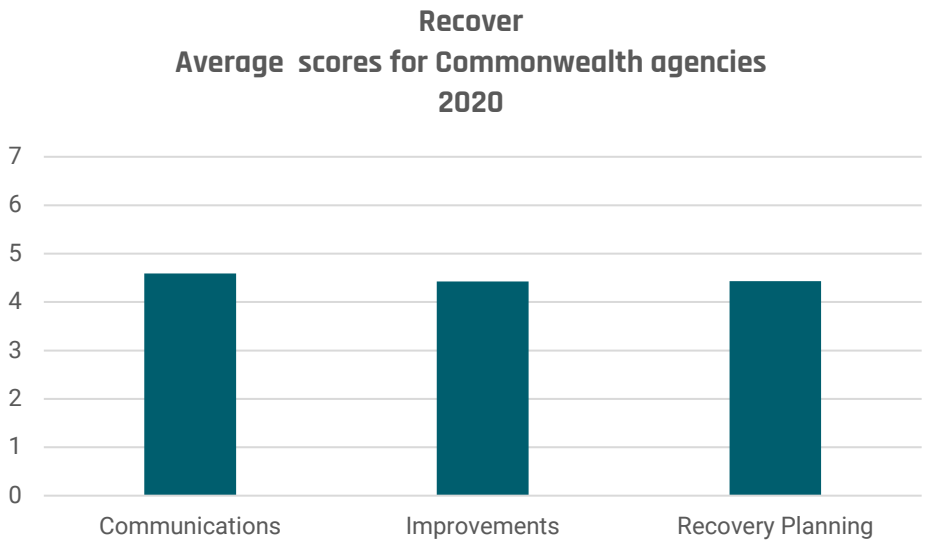


Recover

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:

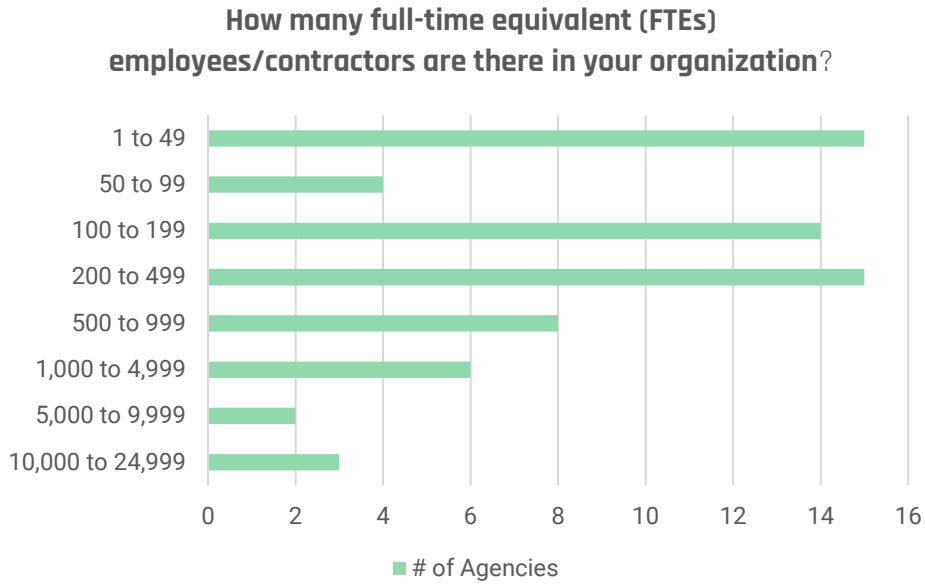
- The "Communications" category relates to coordination with internal and external parties during a security event.
- "Improvements" describes the processes related to incorporating lessons learned from handling IT security incidents into improving recovery planning and processes.
- "Recovery Planning"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

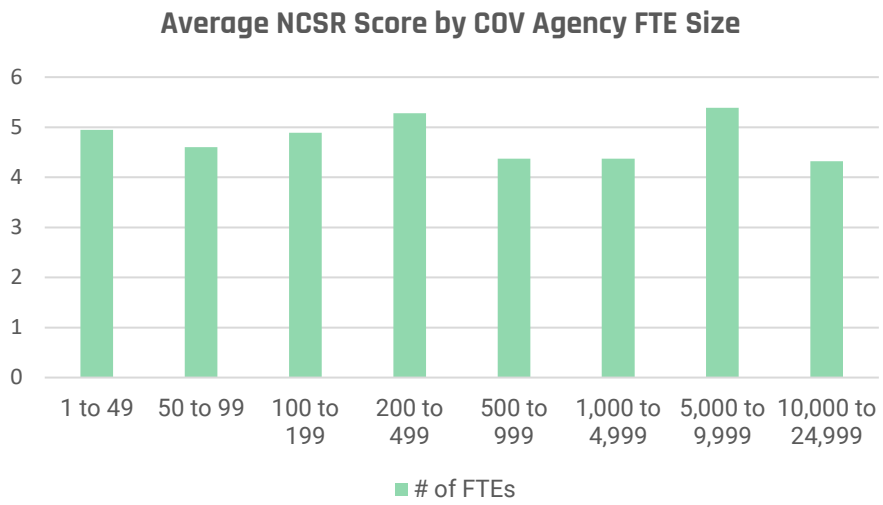


NCSR survey demographic analysis

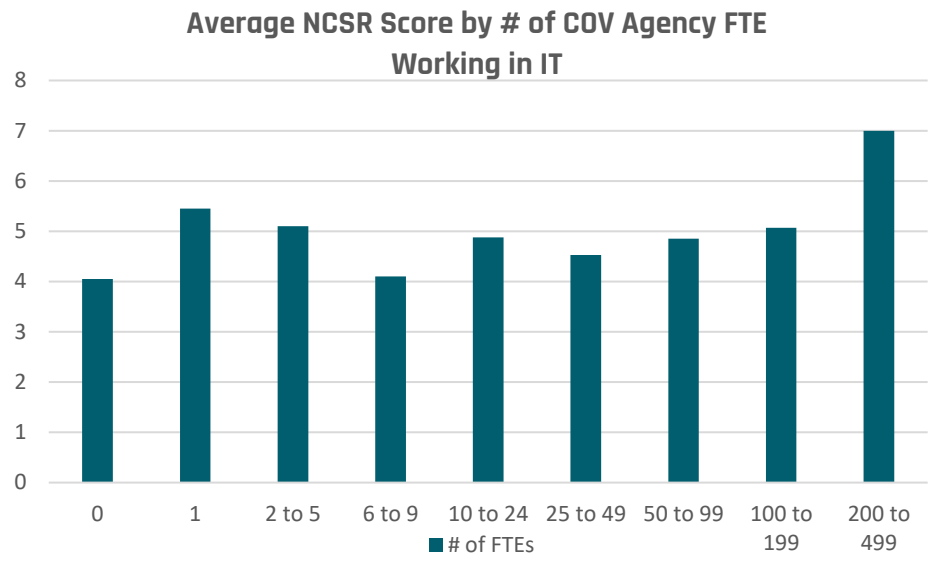
Number of employees and contractors on staff

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

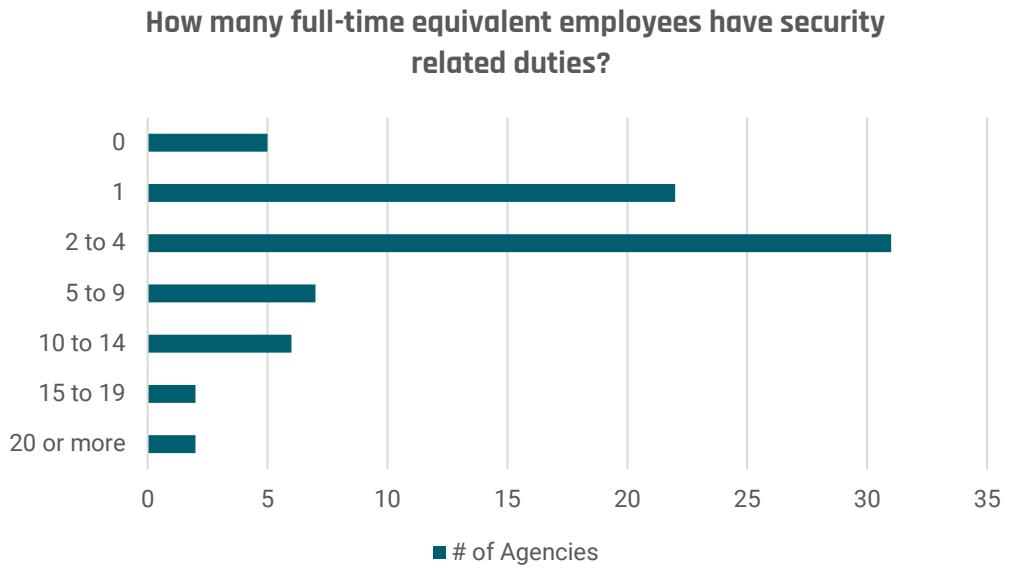


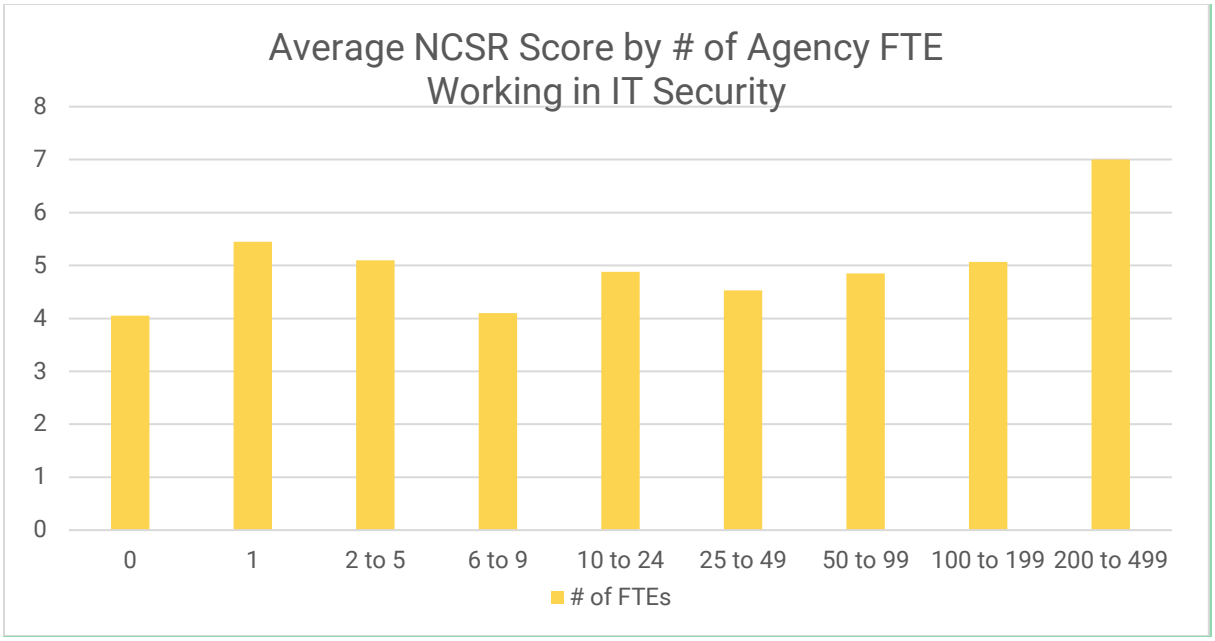


Agencies with fewer than 500 full-time equivalents averaged 4.93 on the NCSR. Larger agencies with over 500 FTEs averaged 4.63.



Agencies with fewer than 10 full-time equivalents working in IT averaged 4.67 on the NCSR. Agencies with over 10 FTEs in IT averaged 5.26.





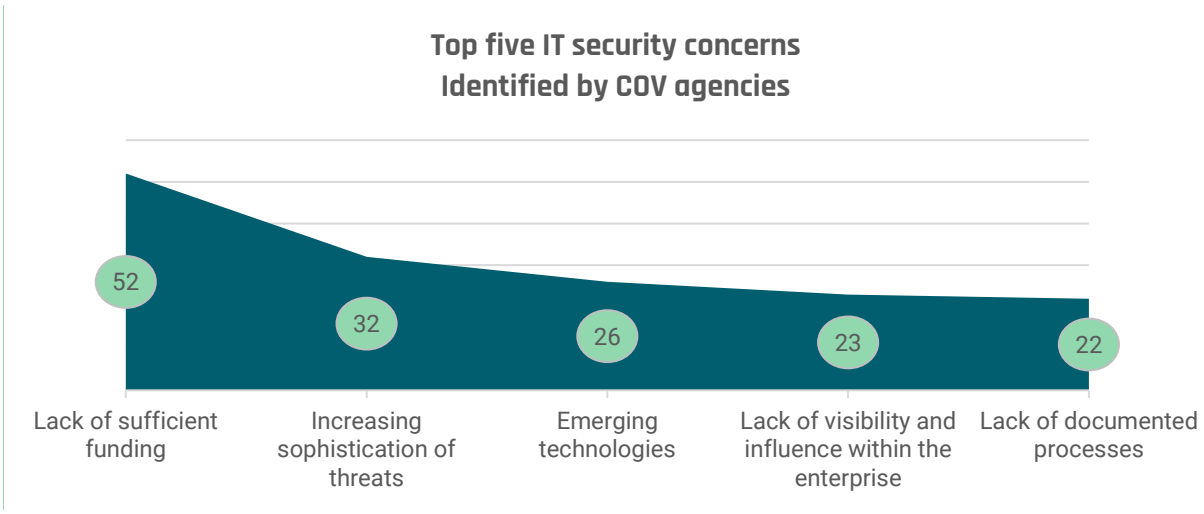
Agencies with fewer than six employees working full-time in IT security scored 4.87 on the NCSR. Agencies with six or more employees working in IT security scored an average of 4.57 on the NCSR. Agencies with no employees (zero) dedicated to IT security scored only 4.05 overall on the NCSR survey.

Staffing totals key takeaways

- Smaller Commonwealth agencies with less than 500 total employees scored 7.5% higher than larger Commonwealth agencies on the NCSR.
- Agencies with 10 or more full-time persons working in IT, scored 12.6% higher on the NCSR than agencies employing fewer than 10 people in IT.
- Agencies with no employees working full-time in IT security scored 26% lower on the NCSR than Commonwealth agencies that had at least one person in that role.

Top five security concerns

Commonwealth agencies participating in the NCSR survey were asked to identify their top five IT security concerns. This year, as last year, the top concern by far was a "Lack of Sufficient Funding". Fifty-two of 65 agencies participating in the survey named it as a top five concern.



Summary of NCSR survey results

The NCSR evaluates cybersecurity maturity. 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 maturity 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 maturity 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 Compliance Report Card

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Finance	Audit, ISO	BOA	Board of Accountancy	A	A
Commerce and Trade		IEIA	Center for Innovative Technologies	A	A
Public Safety and Homeland Security		CASC	Commonwealths Attorneys Services Council	A	A
Administration	Audit, ISO	CB	Compensation Board	A	A
Health and Human Resources		DARS	Department for Aging and Rehabilitative Services	A	F
Health and Human Resources	Audit	DDHH	Department for the Deaf and Hard of Hearing	A	F
Finance	Audit	DOA	Department of Accounts	C	B
Transportation		DOAV	Department of Aviation	A	A
Health and Human Resources		DBHDS	Department of Behavioral Health and Development Services	C	D
Natural Resources	ISO	DCR	Department of Conservation and Recreation	D	B
Public Safety and Homeland Security		DOC	Department of Corrections	B	B
Public Safety and Homeland Security	Audit, ISO	DCJS	Department of Criminal Justice Services	A	B
Education	Audit	DOE	Department of Education	A	A
Administration	ISO	ELECT	Department of Elections	B	B

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Natural Resources	Audit, ISO	DEQ	Department of Environmental Quality	A	B
Public Safety and Homeland Security		DFP	Department of Fire Programs	F	D
Public Safety and Homeland Security	Audit	DFS	Department of Forensic Science	A	B
Agriculture & Forestry	Audit, ISO	DOF	Department of Forestry	A	B
Administration		DGS	Department of General Services	A	A
Health and Human Resources	Audit, ISO	DHP	Department of Health Professions	A	A
Natural Resources	Audit	DHR	Department of Historic Resources	A	B
Commerce and Trade	Audit	DHCD	Department of Housing and Community Development	D	A
Administration	Audit, ISO	DHRM	Department of Human Resource Management	A	A
Public Safety and Homeland Security	Audit, ISO	DJJ	Department of Juvenile Justice	D	B
Commerce and Trade	Audit, ISO	DOLI	Department of Labor and Industry	B	A
Health and Human Resources		DMAS	Department of Medical Assistance Services	B	C
Veterans an Defense Affairs		DMA	Department of Military Affairs	D	D
Commerce and Trade	Audit, ISO	DMME	Department of Mines, Minerals and Energy	A	B
Transportation		DMV	Department of Motor Vehicles	B	A

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Finance	Audit, ISO	DPB	Department of Planning and Budget	A	A
Commerce and Trade	ISO	DPOR	Department of Professional and Occupational Regulation	D	C
Transportation	Audit	DRPT	Department of Rail and Public Transportation	A	B
Commerce and Trade	Audit, ISO	SBSD	Department of Small Business and Supplier Diversity	A	A
Health and Human Resources		DSS	Department of Social Services	F	C
Finance		TAX	Department of Taxation	B	A
Finance		TD	Department of Treasury	B	A
Veterans and Defense Affairs		DVS	Department of Veterans Services	A	D
Natural Resources	ISO	DWR	Department of Wildlife Resources	C	C
Education	ISO	FCMV	Frontier Culture Museum of Virginia	D	B
Education	ISO	GH	Gunston Hall	D	B
Independent	Audit, ISO	IDC	Indigent Defense Commission	B	D
Education	Audit, ISO	JYF	Jamestown-Yorktown Foundation	B	F
Education		LVA	Library of Virginia	D	A
Natural Resources	Audit	MRC	Marine Resources Commission	A	B

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Transportation	Audit, ISO	MVDB	Motor Vehicle Dealer Board	D	B
Education	Audit, ISO	NSU	Norfolk State University	C	B
Health and Human Resources	Audit	CSA	Office for Children's Services	A	A
Executive	ISO	OAG	Office of Attorney General	F	F
Executive		OSIG	Office of State Inspector General	A	B
Executive	ISO	GOV	Office of the Governor	F	B
Education		RBC	Richard Bland College	A	D
Education	ISO	SMV	Science Museum of Virginia	D	C
Education	ISO	SVHEC	Southern Virginia Higher Education Center	A	B
Education		SWVHEC	Southwest Virginia Higher Education Center	F	F
Independent		SCC	State Corporation Commission	A	F
Education	Audit, ISO	SCHEV	State Council of Higher Education for Virginia	F	B
Independent		SLD	State Lottery Department	A	C
Commerce and Trade		TIC	Tobacco Region Revitalization Commission	A	C
Independent		VCSP	Virginia College Savings Plan	A	B

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Education	ISO	VCA	Virginia Commission for the Arts	D	C
Agriculture & Forestry		VDACS	Virginia Department of Agriculture and Consumer Services	A	B
Public Safety and Homeland Security		VDEM	Virginia Department of Emergency Management	F	F
Health and Human Resources		VDH	Virginia Department of Health	F	B
Transportation		VDOT	Virginia Department of Transportation	A	D
Commerce and Trade		VEDP	Virginia Economic Development Partnership	F	F
Commerce and Trade		VEC	Virginia Employment Commission	B	A
Health and Human Resources		VFHY	Virginia Foundation for Healthy Youth	F	D
Administration	Audit, ISO	VITA	Virginia Information Technologies Agency	A	B
Education	Audit	VMFA	Virginia Museum of Fine Arts	D	B
Education	Audit, ISO	VMNH	Virginia Museum of Natural History	A	A
Agriculture & Forestry	Audit, ISO	VRC	Virginia Racing Commission	B	A
Independent		VRS	Virginia Retirement System	A	C
Education		VSDB	Virginia School for the Deaf and Blind	D	F
Public Safety and Homeland Security	Audit, ISO	VSP	Virginia State Police	F	D

Agency Secretariat	Audit or ISO Services?	Agency Acronym	Agency Name	Audit Compliance Grade	Risk Compliance Grade
Education	Audit, ISO	VSU	Virginia State University	B	A
Independent	Audit	VWC	Virginia Workers Compensation Commission	A	A

Appendix II - Agency Information Security Data Points

Agency information security data points detail - Legend

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

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

Three-year audit obligation
X% - The percentage of audit work completed as measured against the agency's security audit plans over the past three years
N/A - Not applicable as the agency had no audits due
N/C - The agency head has not submitted a security audit plan

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

Three year risk assessment obligation completed
X% - The percentage of risk assessments completed as measured against the agency's sensitive systems over the past three years
N/A - Not applicable as the agency had no risk assessments due
N/C - The agency head has not submitted 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 process
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 - Data set information was provided
Non-Compliant - Data set information was not provided fully

ISO certification status
Pass - The primary ISO is certified
Incomplete - The ISO met all other requirements but did not attend the mandatory ISOAG meeting
N/C - The primary ISO is NOT certified

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

Agency Secretariat	Agency Name	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
Administration	Compensation Board	Pass	100%	N/A	Pass	100%	75%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Administration	Department of Elections	Pass	67%	N/A	Pass	100%	N/A	100%	Pass	Compliant	Pass	No	Yes	No
Administration	Department of General Services	Pass	94%	100%	Pass	94%	100.00%	100%	Pass	Compliant	Pass	Yes	No	No
Administration	Department of Human Resource Management	Pass	100%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Administration	Virginia Information Technologies Agency	Pass	82%	100%	Pass	17%	100%	96%	Pass	Compliant	Pass	Yes	Yes	No
Agriculture & Forestry	Department of Forestry	Pass	74%	100.00%	Pass	74%	100%	100%	Pass	Compliant	Pass	No	Yes	Yes
Agriculture & Forestry	Virginia Department of Agriculture and Consumer Services	Pass	100%	100%	Pass	100%	0%	100%	Pass	Compliant	Pass	Yes	No	No
Agriculture & Forestry	Virginia Racing Commission	Pass	60%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Commerce and Trade	Center for Innovative Technologies	Pass	100%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	No	No
Commerce and Trade	Department of Housing and Community Development	Pass	0%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	No	Yes
Commerce and Trade	Department of Labor and Industry	Pass	43%	100%	Pass	100%	100.00%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Commerce and Trade	Department of Mines, Minerals and Energy	Pass	100%	100%	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes

Agency Secretariat	Agency Name	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
Commerce and Trade	Department of Professional and Occupational Regulation	Pass	0%	N/A	Pass	100%	24.44%	100%	Pass	Compliant	Pass	No	Yes	No
Commerce and Trade	Department of Small Business and Supplier Diversity	Pass	100%	N/A	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Commerce and Trade	Tobacco Region Revitalization Commission	Pass	100%	100%	Pass	N/C	N/A	100%	Pass	Compliant	N/C	Yes	No	No
Commerce and Trade	Virginia Economic Development Partnership	N/C	N/C	N/A	N/C	N/C	N/A	N/C	Fail	Non-Compliant	Pass	No	No	No
Commerce and Trade	Virginia Employment Commission	Pass	73%	83.00%	Pass	100%	98%	100%	Pass	Compliant	Pass	Yes	No	No
Education	Department of Education	Pass	100%	100.00%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	No	Yes
Education	Frontier Culture Museum of Virginia	Pass	0%	N/A	Pass	100%	47.37%	100%	Pass	Compliant	N/C	Yes	Yes	No
Education	Gunston Hall	Pass	0%	N/A	Pass	100%	0%	100%	Pass	Compliant	Pass	Yes	Yes	No
Education	Jamestown-Yorktown Foundation	Pass	67%	100%	N/C	67%	100%	100%	Fail	Compliant	Pass	No	No	Yes
Education	Library of Virginia	Pass	6%	N/A	Pass	67%	N/A	100%	Pass	Compliant	Pass	Yes	No	No
Education	Norfolk State University	Pass	30%	100.00%	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Education	Richard Bland College	Pass	100%	100%	N/C	N/C	N/A	100%	Fail	Compliant	Pass	Yes	No	No
Education	Science Museum of Virginia	Pass	0%	N/A	Pass	86%	0%	100%	Pass	Compliant	N/C	Yes	Yes	No
Education	Southern Virginia Higher Education Center	Pass	N/A	N/A	Pass	N/A	N/A	100%	Pass	Compliant	Pass	No	Yes	No
Education	Southwest Virginia Higher	N/C	N/C	N/A	N/C	N/C	N/A	0%	Fail	Compliant		No	No	

Agency Secretariat	Agency Name	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
	Education Center													
Education	State Council of Higher Education for Virginia	Pass	0%	0%	Pass	100%	0%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Education	Virginia Commission for the Arts	N/C	N/A	N/A	Pass	N/C	N/A	100%	Pass	Compliant	N/C	Yes	Yes	No
Education	Virginia Museum of Fine Arts	Pass	0%	N/A	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes	No	Yes
Education	Virginia Museum of Natural History	Pass	100%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Education	Virginia School for the Deaf and Blind	Pass	0%	N/A	N/C	N/C	N/A	100%	Fail	Compliant	N/C	Yes	No	No
Education	Virginia State University	Pass	75%	75.00%	Pass	92%	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Executive	Office of Attorney General	N/C	N/C	0%	Pass	0%	N/A	0%	Pass	Non-Compliant	Pass	No	Yes	No
Executive	Office of State Inspector General	Pass	100%	71.43%	Pass	100%	N/A	0%	Pass	Compliant	Pass	Yes	No	No
Executive	Office of the Governor	N/C	N/C	N/A	Pass	100%	100%	0%	Pass	Compliant	Pass	Yes	Yes	No
Finance	Board of Accountancy	Pass	100%	100%	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Finance	Department of Accounts	Pass	39%	N/A	Pass	78%	N/A	0%	Pass	Compliant	Pass	Yes	No	Yes
Finance	Department of Planning and Budget	Pass	100%	N/A	Pass	100%	75%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Finance	Department of Taxation	Pass	64%	75%	Pass	51%	100%	100%	Pass	Compliant	Pass	Yes	No	No
Finance	Department of Treasury	Pass	55%	50%	Pass	90%	N/A	100%	Pass	Compliant	Pass	Yes	No	No
Health and Human Resources	Department for Aging and Rehabilitative Services	Pass	100%	100%	N/C	N/C	0%	0%	Pass	Compliant	Pass	Yes	No	No

Agency Secretariat	Agency Name	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
Health and Human Resources	Department for the Deaf and Hard of Hearing	Pass	100%	100%	N/C	N/C	0%	0%	Pass	Compliant		Yes	No	Yes
Health and Human Resources	Department of Behavioral Health and Development Services	Pass	34%	87%	Pass	0%	25%	100%	Pass	Compliant	Pass	Yes*	No	No
Health and Human Resources	Department of Health Professions	Pass	100%	N/A	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Health and Human Resources	Department of Medical Assistance Services	Pass	67%	100%	Pass	70%	0%	0%	Pass	Compliant	Pass	Yes	No	No
Health and Human Resources	Department of Social Services	Pass	26%	0%	Pass	67%	0%	N/C	Pass	Compliant	Pass	Yes	No	No
Health and Human Resources	Office for Children's Services	Pass	100%	100%	Pass	83%	N/A	100%	Pass	Compliant	Pass	Yes	No	Yes
Health and Human Resources	Virginia Department of Health	Pass	36%	11.90%	Pass	76%	100%	100%	Pass	Compliant	Pass	No	No	No
Health and Human Resources	Virginia Foundation for Healthy Youth	N/C	N/C	N/A	Pass	57%	N/A	0%	Pass	Compliant	N/C	Yes	No	No
Independent	Indigent Defense Commission	Pass	40%	N/A	Pass	60%	100%	100%	Fail	Partial	N/C	Yes	Yes	Yes
Independent	State Corporation Commission	Pass	78%	100%	N/C	N/C	N/A	100%	Fail	Non-Compliant	Pass	Yes	No	No
Independent	State Lottery Department	Pass	81%	N/A	Pass	0%	N/A	100%	Fail	Compliant	Pass	Yes	No	No
Independent	Virginia College Savings Plan	Pass	78%	N/A	Pass	67%	N/A	100%	Pass	Non-Compliant	Pass	Yes	No	No
Independent	Virginia Retirement System	Pass	100%	100.00%	Pass	100%	100%	100%	Pass	Non-Compliant	Pass	No	No	No
Independent	Virginia Workers Compensation Commission	Pass	100%	N/A	Pass	100%	N/A	100%	Pass	Compliant	Pass	Yes	No	Yes

Agency Secretariat	Agency Name	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
Natural Resources	Department of Conservation and Recreation	Pass	0%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	No	Yes	No
Natural Resources	Department of Environmental Quality	Pass	100%	100%	Pass	100%	100%	N/C	Pass	Compliant	Pass	Yes	Yes	Yes
Natural Resources	Department of Historic Resources	Pass	100%	100%	Pass	0%	100%	100%	Pass	Compliant	Pass	Yes	No	Yes
Natural Resources	Department of Wildlife Resources	Pass	31%	N/A	Pass	0%	N/A	100%	Pass	Compliant	Pass	No	Yes	No
Natural Resources	Marine Resources Commission	Pass	100%	100.00%	Pass	0%	N/A	100%	Pass	Compliant	Pass	Yes	No	Yes
Public Safety and Homeland Security	Commonwealths Attorneys Services Council	Pass	N/A	N/A	Pass	N/A	N/A	100%	Pass	Compliant	Pass	Yes	No	No
Public Safety and Homeland Security	Department of Corrections	Pass	50%	100%	Pass	64%	N/A	2%	Pass	Compliant	Pass	Yes	No	No
Public Safety and Homeland Security	Department of Criminal Justice Services	Pass	100%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	Yes*	Yes	Yes
Public Safety and Homeland Security	Department of Fire Programs	Pass	N/C	100%	Pass	N/C	N/A	14%	Pass	Compliant	Pass	No	No	No
Public Safety and Homeland Security	Department of Forensic Science	Pass	100%	N/A	Pass	100%	100%	100%	Pass	Compliant	Pass	No	No	Yes
Public Safety and Homeland Security	Department of Juvenile Justice	Pass	0%	N/A	Pass	N/C	N/A	100%	Pass	Compliant	Pass	Yes	Yes	Yes
Public Safety and Homeland Security	Virginia Department of Emergency Management	N/C	N/C	N/A	N/C	N/C	N/A	N/C	Pass	Compliant	Incomplete	No	No	No
Public Safety and Homeland Security	Virginia State Police	Pass	2%	0%	Pass	2%	0%	100%	Pass	Compliant	Pass	No	Yes	Yes
Transportation	Department of Aviation	Pass	100%	100.00%	Pass	100%	90.00%	100%	Pass	Compliant	Pass	Yes	No	No

Agency Secretariat	Agency Name	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
Transportation	Department of Motor Vehicles	Pass	45%	98.00%	Pass	100%	98%	100%	Pass	Compliant	Pass	Yes	No	No
Transportation	Department of Rail and Public Transportation	Pass	80%	100%	Pass	100%	100%	100%	Pass	Compliant	Pass	No	No	Yes
Transportation	Motor Vehicle Dealer Board	Pass	0%	100%	Pass	60%	N/A	100%	Pass	Compliant	N/C	Yes	Yes	Yes
Transportation	Virginia Department of Transportation	Pass	76%	99.00%	Pass	33%	57.37%	N/C	Pass	Compliant	Pass	No	No	No
Veterans and Defense Affairs	Department of Military Affairs	Pass	0%	N/A	Pass	0%	N/A	100%	Pass	Compliant	Pass	No	No	No
Veterans and Defense Affairs	Department of Veterans Services	Pass	100%	N/A	N/C	N/C	N/A	N/C	Pass	Compliant	Pass	Yes	No	No

*Approved exception on file

Appendix III – Cybersecurity framework results – Detail

National Cybersecurity Review (NCSR) Results

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

Agency	Identify	Detect	Protect	Respond	Recover	Average
Compensation Board	3.73	4.87	4.08	3.4	3.44	3.904
Department of Education	5.56	2.06	5.93	1.92	1.33	3.36
Department for Aging and Rehabilitative Services	2.92	4.03	4.91	2.12	2	3.196
Board of Accountancy	5.54	5.47	5.54	5.4	5.67	5.524
Commonwealths Attorneys Services Council	7	7	7	6.76	7	6.952
Department for the Deaf and Hard of Hearing (1)	2.92	4.03	4.91	2.12	2	3.196
Department of Accounts	6.53	6.63	6.48	6	6	6.328
Department of Conservation and Recreation	5.72	5.79	6.03	5.72	5.17	5.686
Department of Behavioral Health and Development Services	5.7	6.01	5.74	5.92	6	5.874
Department of Environmental Quality	4.55	3.59	5.31	4.14	4.33	4.384
Department of Blind and Visually Impaired	2.92	4.03	4.91	2.12	2	3.196
Department of Wildlife Resources	5.53	5.87	5.66	4.77	5.78	5.522

Agency	Identify	Detect	Protect	Respond	Recover	Average
Center for Innovative Technologies	4.92	4.13	5.07	2.39	2	3.702
Department of Corrections	5.38	5.5	5.94	5.92	5.17	5.582
Department of Elections	3.67	3.39	3.37	4.04	3.83	3.66
Department of Forestry	5.24	3.49	4.95	3.41	2	3.818
Department of Criminal Justice Services	3.65	5.47	5.18	3.13	2.17	3.92
Department of Historic Resources	7	7	7	7	7	7
Department of Housing and Community Development	5.84	5.57	5.86	5.78	5.83	5.776
Department of Human Resource Management	6.05	5.93	6.04	6.06	6	6.016
Frontier Culture Museum of Virginia	5.01	5.38	5.4	5.29	5	5.216
Department of Aviation	5.76	6	6	6	6	5.952
Department of Fire Programs	3.4	2.43	3.79	2.24	2	2.772
Department of Mines, Minerals and Energy	4	4	4	4	3	3.8
Jamestown-Yorktown Foundation	3.91	3.99	4.64	2.15	3	3.538
Department of Motor Vehicles	6.49	6.46	6.36	6.71	7	6.604
Library of Virginia	6.71	5.95	6.41	6.23	6	6.26
Department of Forensic Science	5	5	5.03	5	5	5.006
Norfolk State University	3.53	2.75	4.8	1.94	2.11	3.026
Richard Bland College	4.25	4.29	4.36	3.77	3	3.934
Department of Labor and Industry	5.03	6.38	5.3	5.59	5.33	5.526

Agency	Identify	Detect	Protect	Respond	Recover	Average
Department of Professional and Occupational Regulation	3.78	3.33	4.02	3.33	3.56	3.604
Department of Health Professions	6	5.93	5.88	5.93	6	5.948
Motor Vehicle Dealer Board	3.18	4.4	4.18	2.96	2	3.344
Marine Resources Commission	5.05	5.67	5.56	5.48	5.11	5.374
Virginia Department of Transportation	4.17	4.36	4.14	3.88	3.33	3.976
Department of Juvenile Justice	4	4	4	4	4	4
Virginia Information Technologies Agency	6.42	6.37	6.26	6.83	6.44	6.464
Virginia Employment Commission	4.25	4.67	5.56	4.19	5.67	4.868
Department of Medical Assistance Services	3.1	3.5	4.89	3.52	3.61	3.724
Department of Military Affairs	5.75	5.76	5.98	5.86	5.44	5.758
Department of Planning and Budget	5.74	5.93	5.82	5.68	5.56	5.746
Department of Small Business and Supplier Diversity	7	6	6.04	5.93	6	6.194
Department of Social Services	2.7	3.78	4	2.71	3.89	3.416
Department of Taxation	3.72	4.05	4.24	5.28	5.22	4.502
Southern Virginia Higher Education Center	2.44	3.94	5.03	2.12	2	3.106
State Corporation Commission	3.52	5.63	4.48	5.88	6	5.102
State Lottery Department	3.92	4.77	5.55	4.96	4	4.64
Virginia Department of Agriculture and Consumer Services	6.74	6.89	6.57	7	6.11	6.662
Department of Treasury	6.42	6.37	6.28	6	5.89	6.192

Agency	Identify	Detect	Protect	Respond	Recover	Average
Virginia Museum of Fine Arts	7	7	7	7	7	7
Virginia Museum of Natural History	5.62	5.53	5.19	5.2	6	5.508
Virginia Racing Commission	5.42	5.45	5.63	5.33	5	5.366
Virginia Retirement System	6.73	6.93	6.9	6.6	6.67	6.766
Department of Veterans Services	3.05	2.99	4.25	2.6	1.67	2.912
Office for Children's Services	5.75	6.67	6.67	6.92	6.67	6.536
Office of State Inspector General	7	6.35	6.93	6.16	7	6.688
Virginia Workers Compensation Commission	7	6.61	7	6.96	7	6.914
Virginia Board for People with Disabilities	2.92	4.03	4.91	2.12	2	3.196
Virginia Department of Emergency Management	2.58	2.41	2.47	1.96	2.17	2.318
Virginia Department of Health	5.74	5.47	5.48	4.24	3.67	4.92
Virginia Foundation for Healthy Youth	5.03	5.57	5.77	6.2	4.67	5.448
Virginia State Police	5.55	4.35	5.26	5.21	5.67	5.208
Wilson Workforce and Rehabilitation Center [1]	2.92	4.03	4.91	2.12	2	3.196

[1] This is an agency of the Department for Aging and Rehabilitative Services