VIRGINIA IT AGENCY

WELCOME TO THE OCT. 5, 2022,

ISOAG MEETING

AGENDA	
Welcome	Ed Miller / VITA
Combining SEC501-SEC525	Chandos Carrow
October Cyber Security Awareness Month Activities	Tina Gaines
Commonwealth Security Awareness Training	Ed Miller
Quarterly Phishing Results - Incident Reporting Procedures	Kathy Bortle
NAC Enforcement	Bill Stewart
IT Risk Management Update	Jon Smith
IT Auditing Services Update	Mark McCreary
Zero Trust in the Commonwealth	
Vulnerability Management	
CISA Cybersecurity Grant Funding Overview	
Upcoming Contract Changes	

COMBINING SEC501-SEC525

By: Chandos Carrow

VITA/CSRM Security Architect

WHO/WHAT/WHY/WHEN/HOW

- Who?:
  - SEC501 – Security standard for systems hosted in a owned or leased COV data center
  - SEC525 – Security standard for systems hosted in a third party environment (not owned or leased by the COV)
  - In other words: Confusion

WHO/WHAT/WHY/WHEN/HOW

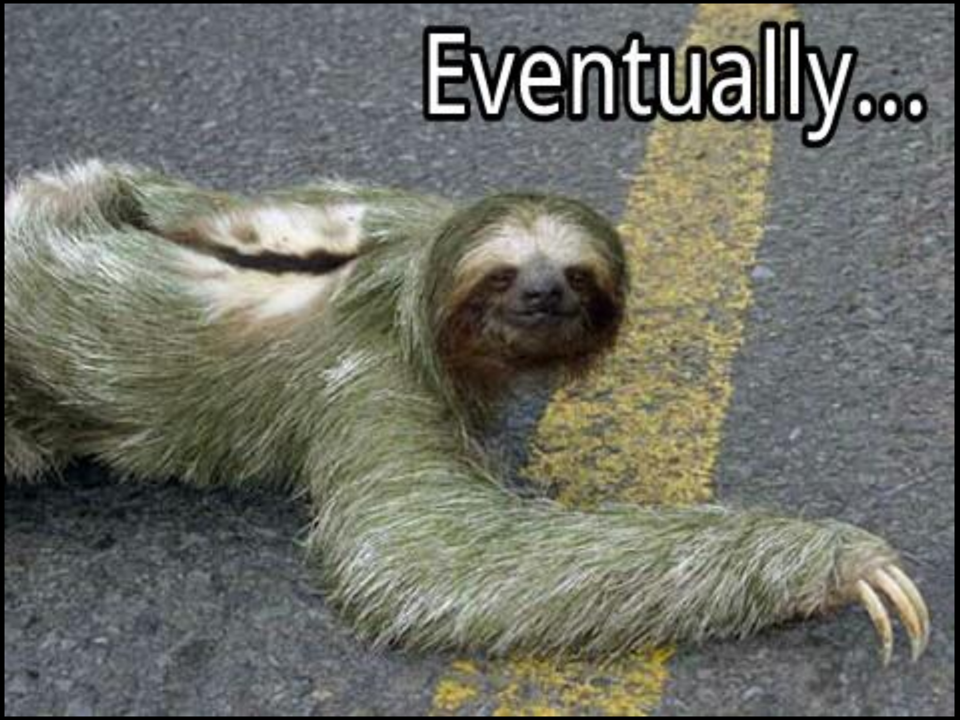
- What?
  - Combining the two security standards into one single security standard for all systems to comply with
  - In other words: Simplicity

WHO/WHAT/WHY/WHEN/HOW

- Why?
  - Reduce confusion
  - NIST 800-53 rev 5
  - Suggestion from ISO Council
  - Why does security have to be stronger in a third party environment versus our own environment? Shouldn’t they both have to be equally secure? Also, isn’t QTS just a third party environment?
  - In other words: Reality

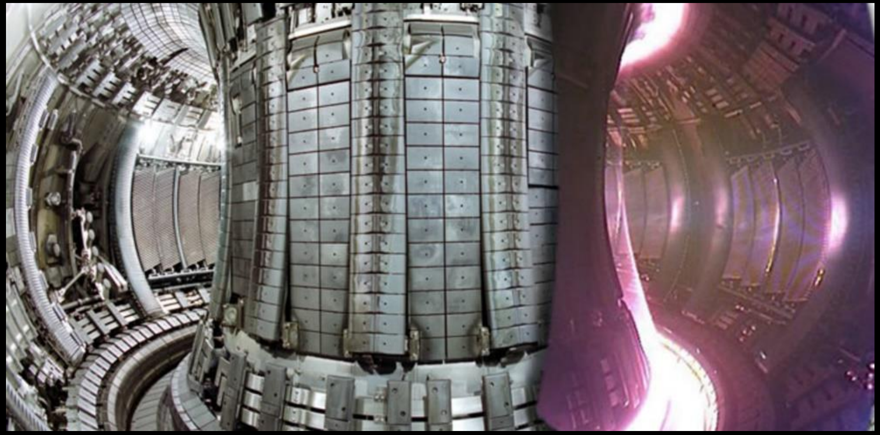
WHO/WHAT/WHY/WHEN/HOW

- When?
  - Early draft phase
  - Will be working with ISO Council and Risk Management Committees to review
  - Then VITA upper management
  - Then ORCA public review
  - Then release
  - Then compliance
  - In other words: Eventually…



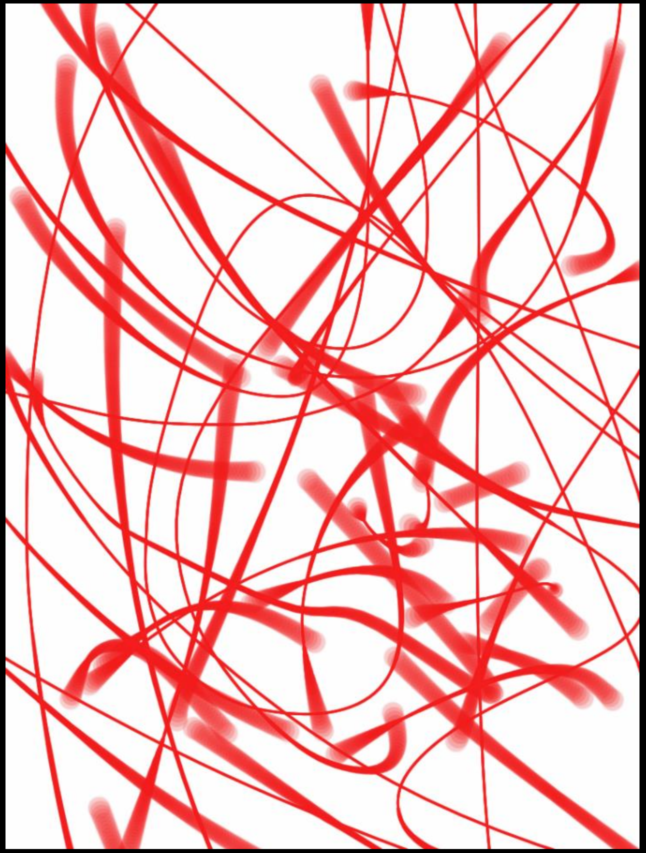
WHO/WHAT/WHY/WHEN/HOW

- How?
  - Compared SEC501 and SEC525
    - SEC525 has more controls and is more restrictive
    - 300 controls are the same
    - 61 controls had differences
    - In most cases went with the more restrictive control (examples later)
    - Then combined into 1 document
    - This new document, which will become the new security standard called SEC530
    - In other words: Fusion



WHO/WHAT/WHY/WHEN/HOW

- How? Continued…
  - Compared SEC530 to NIST 800-53 rev 5
    - SEC501 and SEC525 based on rev 4
    - Rev 4 to rev 5 has significant changes
      - 698 of 1190 control changes identified as more than editorial or administrative changes by NIST
      - Two brand new sections to be considered
        - Personally Identifiable Information Processing and Transparency
        - Supply Chain Risk Management
    - In other words: Red lines…so many red lines



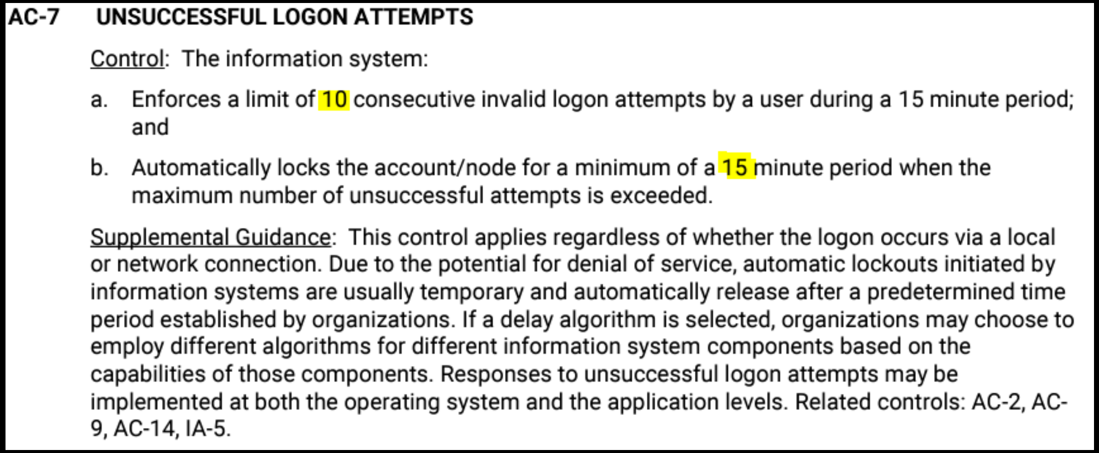
QUESTIONS FOR AUDIENCE

- For the ISO Council and Risk Management Committee members, how would you all like to review SEC530:
  - Section by section
  - Whole document
  - Other suggestions?

- ISOAG attendees, how would you all like to review SEC530 before ORCA:
  - Section by section updates after review by the Council and Committee
  - Whole document (e.g. an entire ISOAG 3 hour presentation)
  - Other suggestions?

EXAMPLES OF SEC501 TO SEC525 COMPARISON

SEC501



AC-7 UNSUCCESSFUL LOGON ATTEMPTS

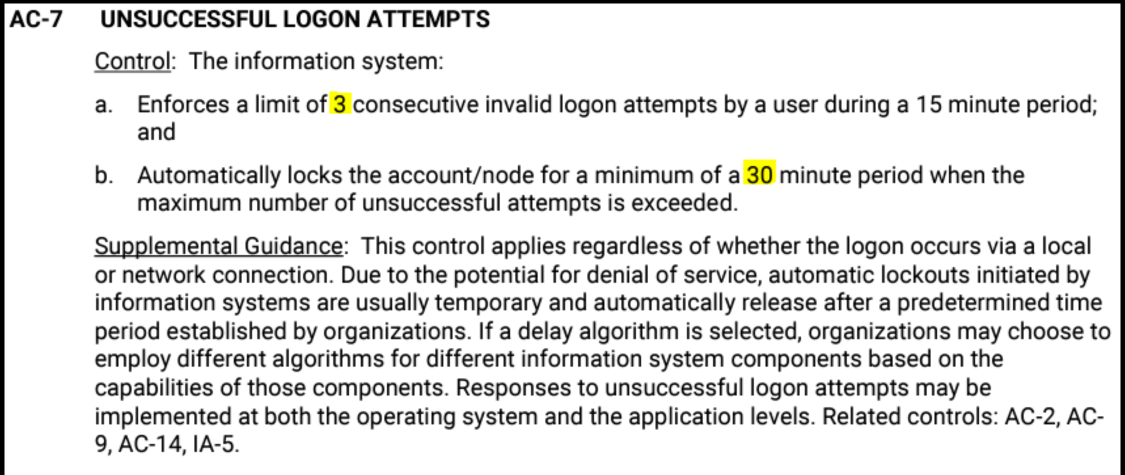
Control: The information system:

a. Enforces a limit of 10 consecutive invalid logon attempts by a user during a 15 minute period; and

b. Automatically locks the account/node for a minimum of a 15 minute period when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

SEC525



AC-7 UNSUCCESSFUL LOGON ATTEMPTS

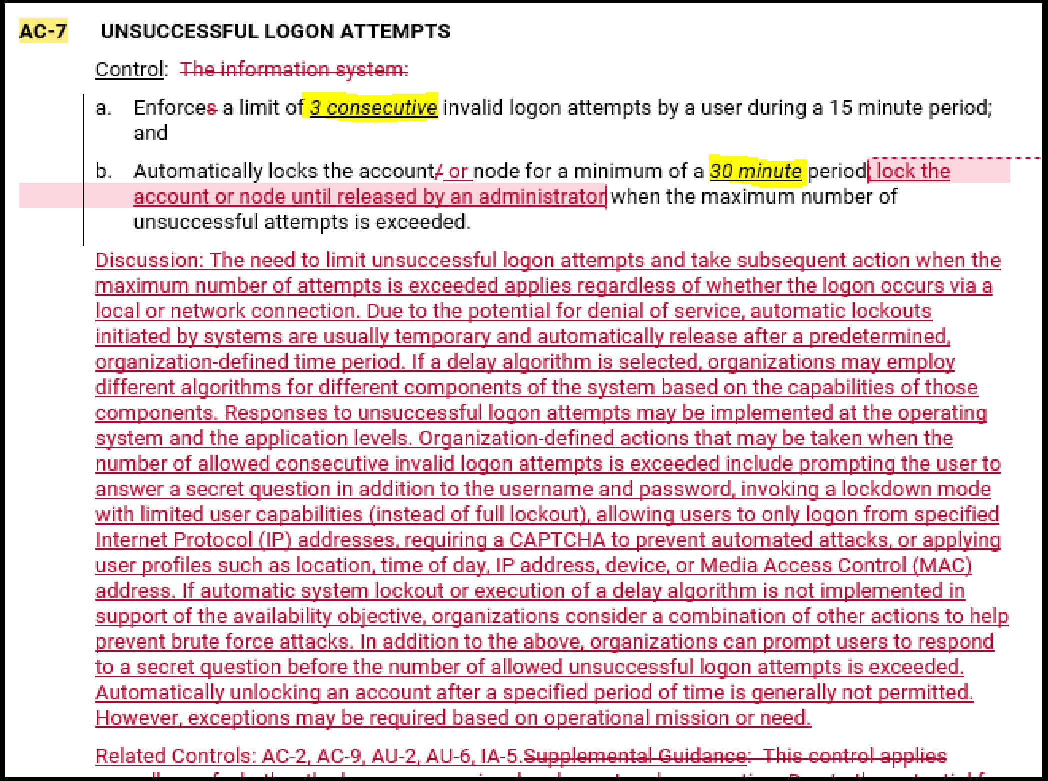
Control: The information system:

a. Enforces a limit of 3 consecutive invalid logon attempts by a user during a 15 minute period; and

b. Automatically locks the account/node for a minimum of a 30 minute period when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

SEC530



AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control: ~~The information system:~~

a. Enforce~~s~~ a limit of *3 consecutive* invalid logon attempts by a user during a 15 minute period; and

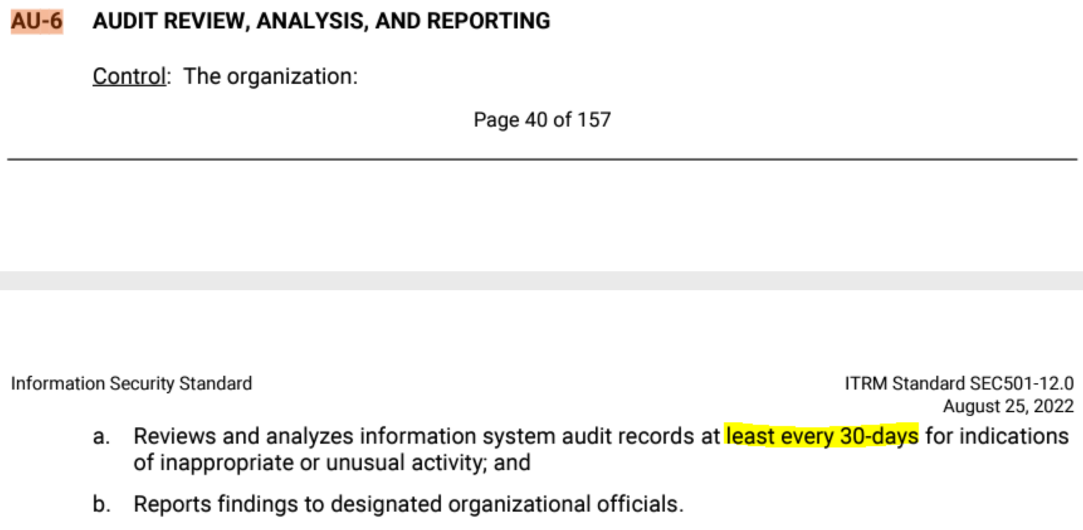
b. Automatically locks the account~~/~~ or node for a minimum of a *30 minute* period; lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

Discussion: The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time period. If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at the operating system and the application levels. Organization-defined actions that may be taken when the number of allowed consecutive invalid logon attempts is exceeded include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles such as location, time of day, IP address, device, or Media Access Control (MAC) address. If automatic system lockout or execution of a delay algorithm is not implemented in support of the availability objective, organizations consider a combination of other actions to help prevent brute force attacks. In addition to the above, organizations can prompt users to respond to a secret question before the number of allowed unsuccessful logon attempts is exceeded. Automatically unlocking an account after a specified period of time is generally not permitted. However, exceptions may be required based on operational mission or need.

Related Controls: AC-2, AC-9, AU-2, AU-6, IA-5.~~Supplemental Guidance: This control applies~~

EXAMPLES OF SEC501 TO SEC525 COMPARISON

SEC501



AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The organization:

Page 40 of 157

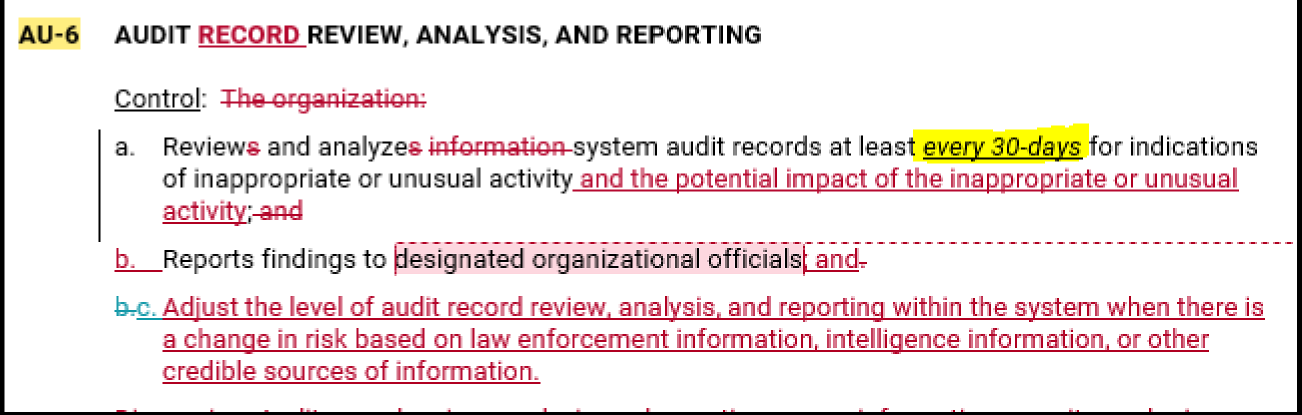
Information Security Standard

ITRM Standard SEC501-12.0
August 25, 2022

a. Reviews and analyzes information system audit records at least every 30-days for indications of inappropriate or unusual activity; and

b. Reports findings to designated organizational officials.

SEC530



AU-6 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

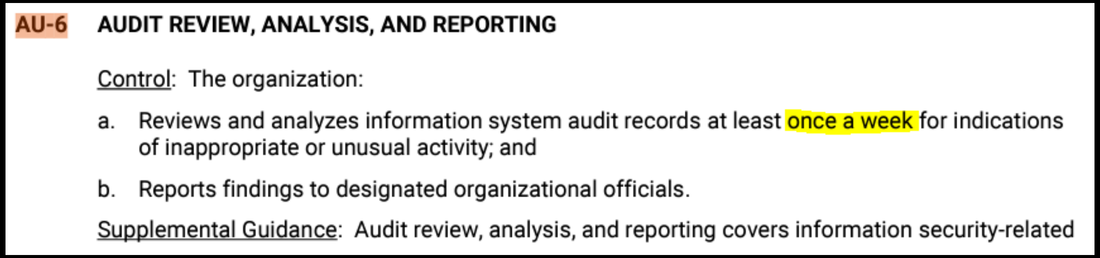
Control: ~~The organization:~~

a. Review~~s~~ and analyze~~s~~ ~~information~~ system audit records at least *every 30-days* for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity; ~~and~~

b. Reports findings to designated organizational officials; and~~.~~

~~b.~~c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

SEC525



AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The organization:

a. Reviews and analyzes information system audit records at least once a week for indications of inappropriate or unusual activity; and

b. Reports findings to designated organizational officials.

Supplemental Guidance: Audit review, analysis, and reporting covers information security-related

QUESTIONS?

THANK YOU!

Chandos Carrow
chandos.carrow@vita.virginia.gov

NCSAM

We’re all in

#CybersecurityAwarenessMonth 2022

We are excited to share information for Cybersecurity Awareness Month (CSAM) 2022.

As the month progresses, we’ll add resources that you can use to customize your CSAM activities and communications. If you have any questions, email vitacomms@vita.virginia.gov.

Overall Campaign

This year’s focus are on four key behaviors instead of weekly themes

Topics covered:

- Enabling multi-factor authentication
- Using strong passwords and a password manager
- Updating software
- Recognizing and reporting phishing

NCSAM ACTIVITIES

- Governor’s Proclamation – https://www.governor.virginia.gov/newsroom/proclamations/proclamation-list/cybersecurity-awareness-month.html

- 2023 Kids Safe Online Poster Contest – Kids Safe Online Poster Contest | Virginia IT Agency (Joint news release with DOE coming out soon)
- CSAM Activities - https://www.vita.virginia.gov/information-security/cyber-awareness/
- Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022 - National Cybersecurity Alliance (staysafeonline.org)

NCSAM ACTIVITIES

- VA529 Shred Event: October 21 from 10a -2p. You must register for the event at:

https://forms.office.com/g/QiRmZX6akL

- VA529 Virtual Escape Room: You can register at: Informationsecurity@virginia529.com
- VDH – Cyber Talk Series:

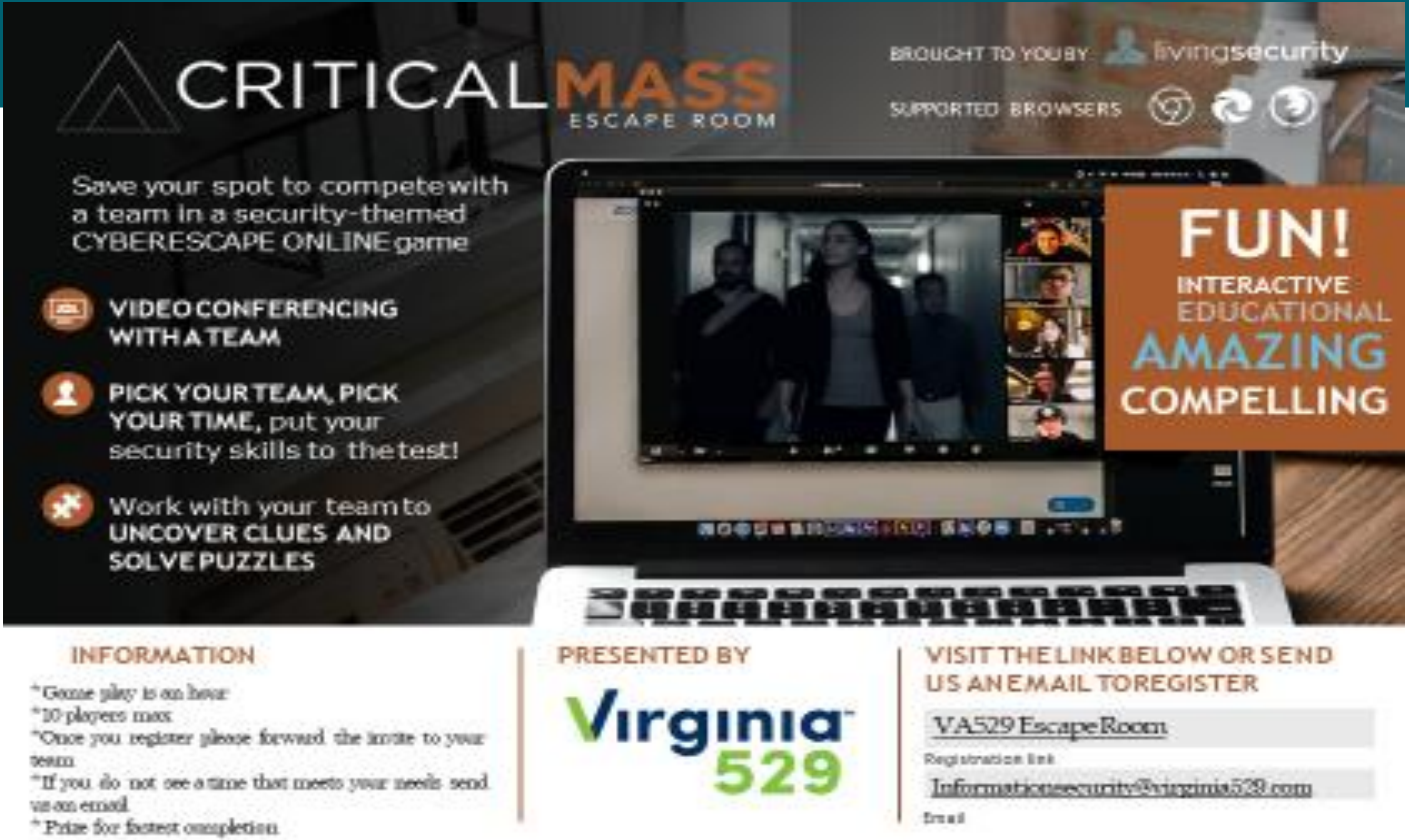
Cyber Talk Series:

Join us for the conversation on ***"Internet of Things (IOT) on October 14, 2022 at 12 noon – 1:00 p.m.*** Mr. Randy Marchany is the University Information Security Officer, Virginia Tech. We are connected via the Internet more than ever before with smart devices such as fitness trackers, vehicles, smart televisions, doorbells, light bulbs, home security systems, thermostats, and refrigerators. He will be discussing how the Internet of Things (IOT) works and how to protect them.

Register:

Copy and paste the link below. Add your First Name, Last Name and email address.

https://covaconf.webex.com/covaconf/j.php?RGID=r829cc43bf5aae3725f7b6c118a11e4ee



CRITICAL MASS

ESCAPE ROOM

BROUGHT TO YOU BY livingsecurity

SUPPORTED BROWSERS

Save your spot to compete with a team in a security-themed CYBERESCAPE ONLINE game

- VIDEO CONFERENCING WITH A TEAM
- PICK YOUR TEAM, PICK YOUR TIME, put your security skills to the test!
- Work with your team to UNCOVER CLUES AND SOLVE PUZZLES

FUN!
INTERACTIVE
EDUCATIONAL
AMAZING
COMPELLING

INFORMATION

*Game play is an hour
*10 players max
*Once you register please forward the invite to your team
*If you do not see a time that meets your needs send us an email
* Prize for fastest completion

PRESENTED BY

Virginia 529

VISIT THE LINK BELOW OR SEND US AN EMAIL TO REGISTER

VA529 EscapeRoom

Registration link

Informationsecurity@virginia529.com

Email

NCSAM ACTIVITIES

2022 Cybersecurity Career Panel

- **Date: Friday, 10/28/2022**
- **Time: 4:00 PM - 6:00 PM**
- **Location: VCU College of Engineering West Hall Room 106 (601 West Main Street, Richmond, VA 23220)**
- **Zoom Webinar for simultaneous broadcast available and will be provided following registration**
- **Panelists of the event include:**
- **Bob Austin** - President, Kore Logic
- **Jason Belford** - CISO, University of Virginia
- **Tyson Martin** - Principal CIO, CISO, CEO & Board Advisor, Amazon Web Services
- **Beth Waller** - Principal and Chair, Cybersecurity and Data Privacy Practice, Wood Rogers
- **Michael Watson** - CISO and Deputy CIO, Commonwealth of Virginia

2022 Cybersecurity Career Panel Registration Form (google.com

QUESTIONS

VIRGINIA IT AGENCY

CYBERSECURITY AWARENESS TRAINING

DATA POINTS

COMPLEMENTARY USER ENTITY CONTROLS

NCSR ANALYSIS

ED MILLER

DIRECTOR IT SECURITY GOVERNANCE

SEPTEMBER 30, 2022

VIRGINIA
IT AGENCY

CYBERSECURITY AWARENESS TRAINING

ED MILLER

DIRECTOR IT SECURITY GOVERNANCE

SEPTEMBER 30, 2022

OVERVIEW

- Cybersecurity Awareness Training plays a critical role in minimizing serious cybersecurity threats posed to Commonwealth employees by phishing attacks and social engineering.
- In addition, Commonwealth employees routinely handle and process highly confidential data. Cybersecurity Awareness Training helps reinforce their knowledge of their responsibilities in protecting this data.
- Cybersecurity Awareness Training is also necessary to:
  - Reduce cybersecurity risk related to user behavior
  - Address and comply with regulatory requirements
  - Comply with internal policies

LEGISLATIVE REQUIREMENTS

- § 2.2-2009. Additional duties of the CIO relating to security of government information.
  - Since 2009, VITA has been legislated to direct the development of policies, standards and guidelines that protect state government information from unauthorized uses, intrusions or other security threats. This governance applied to all Executive, Legislative, Judicial and Independent branch agencies
  - To that end, VITA developed policies and standards for IT security. This includes the requirement for IT security awareness training for all Commonwealth users. These requirements have been in effect for many years.
- In 2020, HB852 was approved. This bill requires VITA to:
  - Annually update a curriculum for *"state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats. The bill requires the Commonwealth's executive, legislative, and judicial branches and independent agencies, beginning January 1, 2021 to provide annual information security training for each of its employees…."*

- **The Governor and Administration are very interested in expanding and standardizing Cybersecurity Awareness Training across all branches of Commonwealth government.**
- **To this end, CSRM has been identifying and focusing on solutions that can be implemented.**
- **No decisions have been made yet.**

SCOPING PARAMETERS

- Obtained an employee count list by agencies from DHRM. I used the higher of MEL or SALARY+WAGE employees.
  - EXECUTIVE BRANCH – 81 agencies – 56,367 employees
  - LEGISLATIVE BRANCH – 16 agencies – 707 employees
  - JUDICIAL BRANCH – 11 agencies – 269 employees
  - INDEPENDENT – 5 agencies – 4,290 employees
  - We fudged in an estimate for contractors.
  - Then we rounded the whole total up higher.
  - If its determined that all HIGHER EDs should be included, the count of employees is double that.
  - We will have the flexibility to easily add additional licenses if we need it.
  - If approved, we hope that the new SAT will be available in early CY2023.

SCOPING PARAMETERS

- The solution we're looking most closely at:
  - Will meet the training requirements prescribed in § 2.2-2009 and the specific baseline training criteria developed in SEC 527.
  - It will include a phishing campaign capabilities as well as training capabilities.
  - The intent is to license it for all Executive, Legislative, Judicial and Independent branch agencies.
  - The training platform will have a multi-tenant capability allowing each agency a login portal to all of its information.
  - It will allow CSRM to centrally monitor training across the Commonwealth (it will eliminate the need for some of the compliance forms currently required by SEC527.
  - CSRM and agencies will be able to report training progress to their agency heads, Secretariats and other interested parties easily.

QUESTIONS

VIRGINIA IT AGENCY

DATA POINTS

ED MILLER

DIRECTOR IT SECURITY GOVERNANCE

SEPTEMBER 30, 2022

DATA POINTS

- We’re now in the final quarter of the calendar year.

- The compliance metrics we know as data points are revolve around each agency’s **“audit”** and “**risk**” programs.

- We use these metrics to get a baseline of where each agency is in terms of IT security that VITA is required to report on per § *2.2-2009. Additional duties of the CIO relating to security of government information*

- Based on the data point metrics, we use Archer to calculate a report card grade for each agency.

- The data point metrics are fairly straight forward. We convert each metric to a numeric score, add them up and then average it. Then the numeric score is reported as a letter grade: A B C D F

AUDIT DATA POINTS

- The Audit score is probably the simplest to calculate but may be one of the hardest to receive a high score on.

- Auditing has very specific requirements and actual audits can only be performed by qualified and independent auditors.

- Audits can also be very involved and time-consuming and costly (especially if they need to be out-sourced).

AUDIT DATA POINTS

- The Audit score is essential 3 data points:
  - Each agency must submit an **Audit Plan** annually. Anyone can submit an Audit Plan. The only requirement is that it lists all of the agency's sensitive systems and includes a scheduled audit date within 3 years of the date of the last audit. The metric will be either Pass or Fail (numerically that means 100% or 0%).
  - **Audits.** Each sensitive system should be audited at least once every 3 years. The metric is a percentage of sensitive systems audited. If the agency is reporting 10 sensitive systems and 8 were audited. It's a score of 80%
  - **Quarterly updates.** Remediation steps need to be reported for all findings on a quarterly basis. If a finding is open all year long, we are expecting at least 4 updates for the finding. The metric is a % of quarterly updates received for each finding.
- The Final audit metric is [(Audit plan) + (% of Audits) + (% of Quarterly Updates)] / 3

RISK DATA POINTS

- The Risk score is probably more directly controlled by the agency ISO.
- It consists of 8 different metrics.

1. Risk Assessment Plan (must be submitted annually/PASS or FAIL)
2. Risks Assessments Performed (% of RAs submitted)
3. Quarterly updates of risk assessment findings (works the same way as audit findings, reported as a %)
4. BIA (All reported business processes must be updated annually. Archer calculates a %)
5. Applications Certified (all applications must be “certified”, i.e. associated with at least 1 Bus Processes, 1 Dataset and at least 1 Device (or product/service). IT Strategic Plan approval requires app certification also.
6. IDS Reporting each quarter (for Enterprise managed agencies, this is always a PASS. For independent agencies, we expect quarterly updates)
7. ISO Certification (agency primary ISO must meet the certification requirement, this is reported as {PASS/FAIL)
8. ISO must report to the agency head (required by OSIG audit of security in the commonwealth in 2019)

RISK DATA POINTS

- The Risk score is then just a simple calculation:
- RA Plan

  + % RAs

  + % of QU received

  + BIA %

  + Applications Certified

  + IDS Reports +

  + ISO Certified

  + ISO Reporting

  SUBTOTAL / 8

That's it. The way we set up the metrics and also the way Archer works for some of them, most scores don't start to accurately reflect what the agency will receive until late in the 4th quarter and usually not until the 1st quarter of the next year. We'll start sending out Archer Data Points email in another week or so.

QUESTIONS

VIRGINIA IT AGENCY

COMPLEMENTARY USER ENTITY CONTROLS

ED MILLER

DIRECTOR IT SECURITY GOVERNANCE

SEPTEMBER 30, 2022

SOC AUDITS

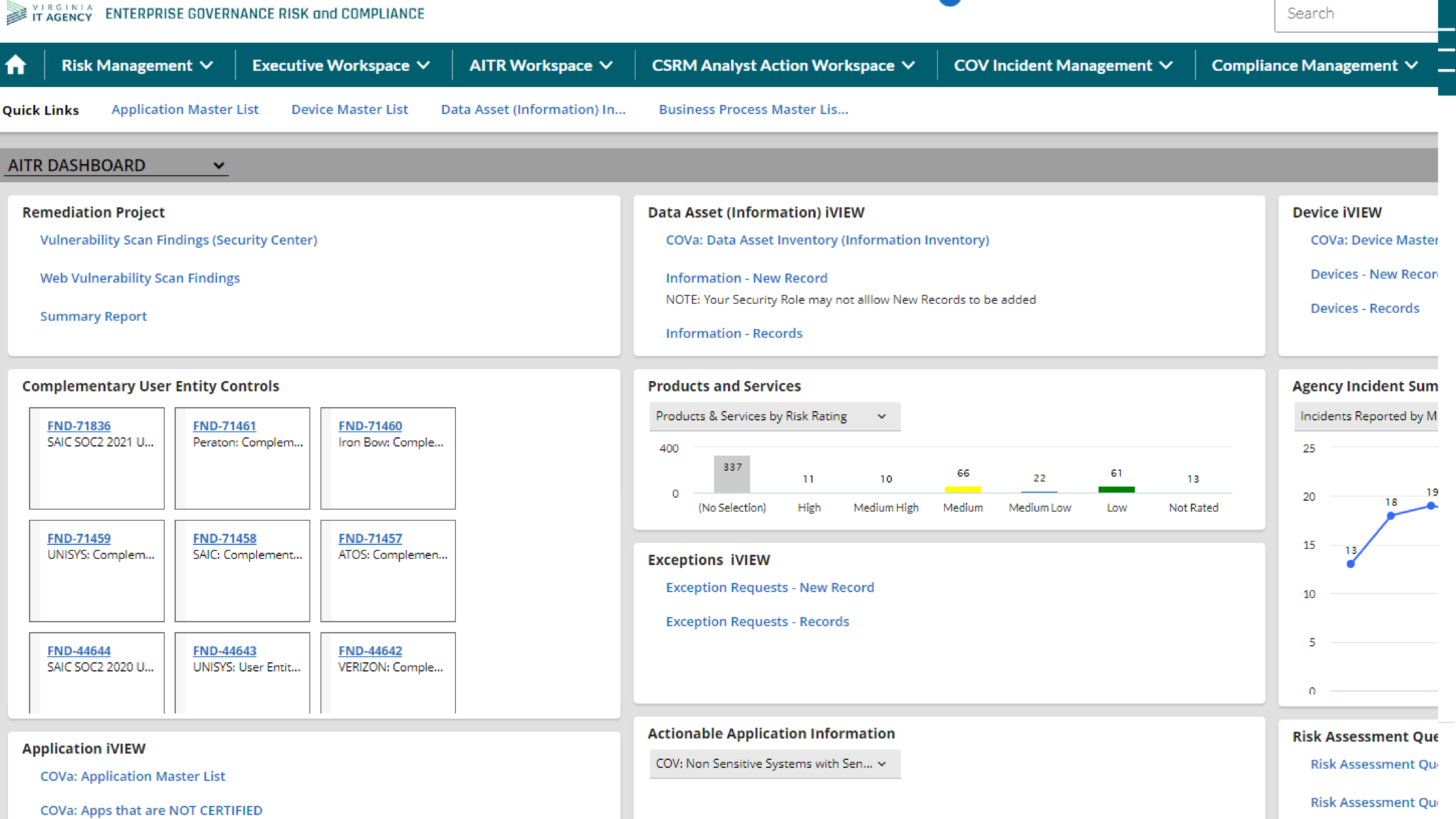
- **What is a SOC Audit?**
- SOC is an acronym that stands for “Service Organization Controls” and more recently as “System & Organization Controls.”
- In a nutshell, a SOC report is issued after a third-party auditor (conducts a thorough examination of an organization to verify that they have an effective system of controls related to security, availability, processing integrity, confidentiality and/or privacy.
- The SOC controls standards were created and overseen by the American Institute of Certified Public Accountants (AICPA).
- A SOC1 audit focuses on financial processes and reporting. The SOC2 audit focuses on how the company secures its data and technologies.
- You’ll also see SOC audits referred to as “Type 1” and “Type 2” audits. A “Type 1” is a point in time audit that evaluates how the company is performing at the time of the audit. A “Type 2” audit reviews a period of time, usually 12 months, to ensure that all controls were in place at all times.
- By contract, all Commonwealth enterprise service towers are required to have their services audited by independent SOC auditors annually. VITA requires two types of SOC audits, SOC1 Type 2 and SOC2 Type 2.

SOC AUDITS

- **What is a SOC Audit?**
- SOC audit reports are considered by most of our vendors as “confidential” documents so CSRM does not distribute paper or electronic copies of SOC reports.
- However, we do allow agency auditors and security personnel to review the reports. By reviewing SOC reports, agency auditors can structure and scope their own audits in a manner that places reliance on areas that the SOC auditor has already reviewed. This is a more efficient process since agency personnel are not having to address audit questions that may have already been reviewed in the SOC audit.
- We have started to receive SOC1 audits for FY2021 already and are expecting SOC2 audits for FY2021 to follow shortly after. We usually have all these in by the end of November.
- If your agency auditors wish to review SOC reports, please schedule a time with the CSRM Governance staff. You can come to our new office at the Boulders or we can arrange a remote WebEx session for you. We only ask that you not make copies of the reports.

COMPLEMENTARY USER ENTITY CONTROLS

- SOC audits usually have a section called **“Complementary User Entity Controls”.**
- **Complementary User Entity Controls (CUECs):** also known as **User Control Considerations (UCCs)** are controls that the vendor (a service tower or SaaS company) has included within its system, in which the user entity **(you!)** must implement to ensure the vendor's control objectives are accomplished.
- **Who Is Responsible for CUECs?** Service vendors include CUECs within their system and rely on customers to implement them, so the customer can achieve their control objectives. This means that **the customer using services provided by a service organization** is responsible for implementing CUECs and assuring that they are working.
- We’ve added a section in Archer to get this information about CUECs out to agencies in an easier manner than having to review the SOC audits and take notes.



Remediation Project

Vulnerability Scan Findings (Security Center)

Web Vulnerability Scan Findings

Summary Report

Data Asset (Information) iVIEW

COVa: Data Asset Inventory (Information Inventory)

Information - New Record

NOTE: Your Security Role may not alllow New Records to be added

Information - Records

Device iVIEW

COVa: Device Master

Devices - New Recor

Devices - Records

Complementary User Entity Controls

FND-71836 SAIC SOC2 2021 U...	FND-71461 Peraton: Complem...	FND-71460 Iron Bow: Comple...
FND-71459 UNISYS: Complem...	FND-71458 SAIC: Complement...	FND-71457 ATOS: Complemen...
FND-44644 SAIC SOC2 2020 U...	FND-44643 UNISYS: User Entit...	FND-44642 VERIZON: Comple...

Products and Services

Products & Services by Risk Rating

Agency Incident Sum

Incidents Reported by M

Exceptions iVIEW

Exception Requests - New Record

Exception Requests - Records

Application iVIEW

COVa: Application Master List

COVa: Apps that are NOT CERTIFIED

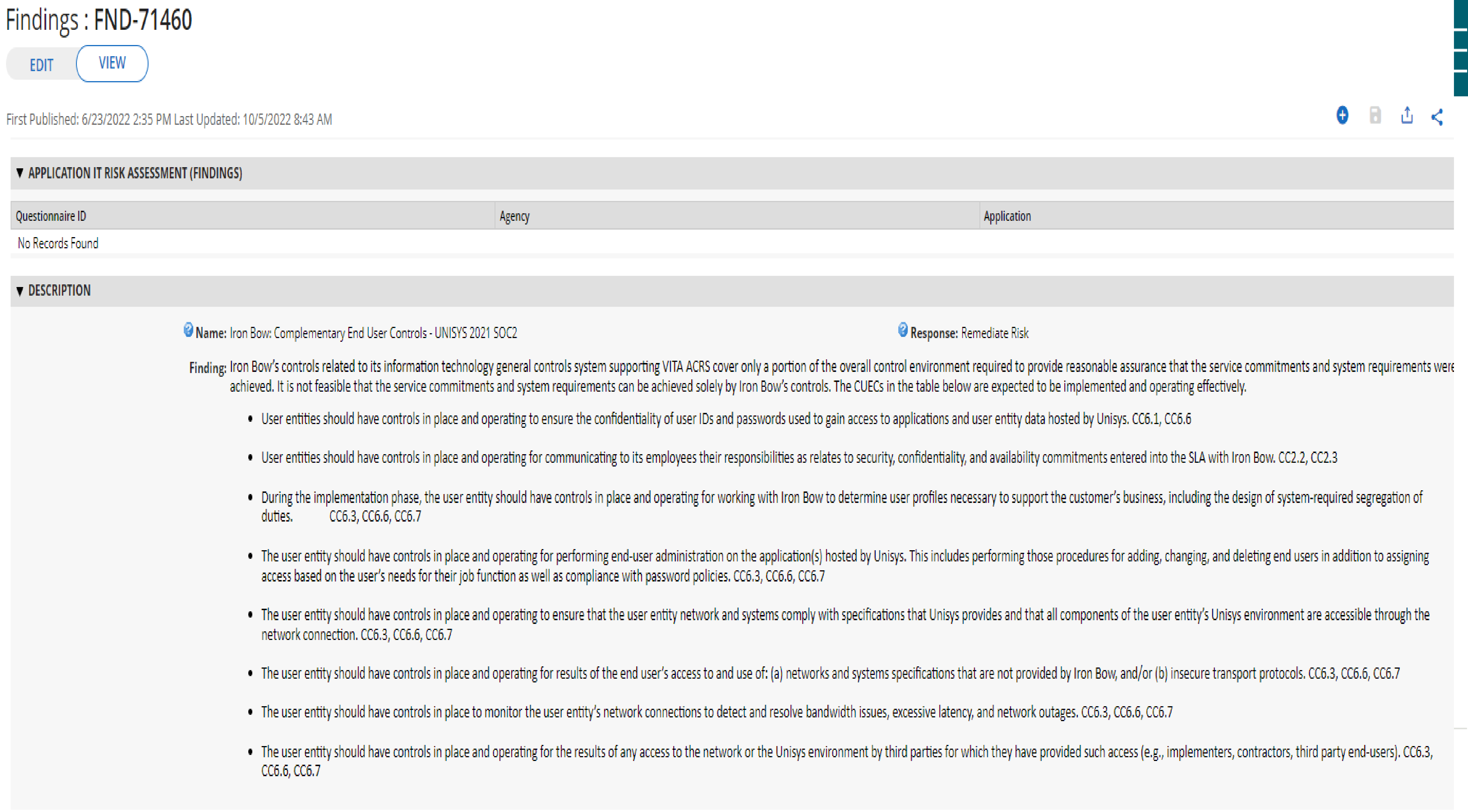
Actionable Application Information

COV: Non Sensitive Systems with Sen...

Risk Assessment Que

Risk Assessment Qu

Risk Assessment Qu



Findings : FND-71460

First Published: 6/23/2022 2:35 PM Last Updated: 10/5/2022 8:43 AM

▼ APPLICATION IT RISK ASSESSMENT (FINDINGS)

Questionnaire ID	Agency	Application
No Records Found		

▼ DESCRIPTION

Name: Iron Bow: Complementary End User Controls - UNISYS 2021 SOC2

Response: Remediate Risk

Finding: Iron Bow's controls related to its information technology general controls system supporting VITA ACRS cover only a portion of the overall control environment required to provide reasonable assurance that the service commitments and system requirements were achieved. It is not feasible that the service commitments and system requirements can be achieved solely by Iron Bow's controls. The CUECs in the table below are expected to be implemented and operating effectively.

- User entities should have controls in place and operating to ensure the confidentiality of user IDs and passwords used to gain access to applications and user entity data hosted by Unisys. CC6.1, CC6.6
- User entities should have controls in place and operating for communicating to its employees their responsibilities as relates to security, confidentiality, and availability commitments entered into the SLA with Iron Bow. CC2.2, CC2.3
- During the implementation phase, the user entity should have controls in place and operating for working with Iron Bow to determine user profiles necessary to support the customer's business, including the design of system-required segregation of duties. CC6.3, CC6.6, CC6.7
- The user entity should have controls in place and operating for performing end-user administration on the application(s) hosted by Unisys. This includes performing those procedures for adding, changing, and deleting end users in addition to assigning access based on the user's needs for their job function as well as compliance with password policies. CC6.3, CC6.6, CC6.7
- The user entity should have controls in place and operating to ensure that the user entity network and systems comply with specifications that Unisys provides and that all components of the user entity's Unisys environment are accessible through the network connection. CC6.3, CC6.6, CC6.7
- The user entity should have controls in place and operating for results of the end user's access to and use of: (a) networks and systems specifications that are not provided by Iron Bow, and/or (b) insecure transport protocols. CC6.3, CC6.6, CC6.7
- The user entity should have controls in place to monitor the user entity's network connections to detect and resolve bandwidth issues, excessive latency, and network outages. CC6.3, CC6.6, CC6.7
- The user entity should have controls in place and operating for the results of any access to the network or the Unisys environment by third parties for which they have provided such access (e.g., implementers, contractors, third party end-users). CC6.3, CC6.6, CC6.7

- Service Organizations are numerous and diverse entities, and CUECs can be very different depending on the specific type of SOC report, service organization, industry and types of services being provided

- User entities (agencies) should begin to evaluate CUECs by reviewing the SOC reports for the service organizations that they are currently using as part of their current business processes.

- Agencies should identify all the applicable CUECs that are outlined in the report during the annual SOC audit report review process.

- Upon completion of identifying the applicable CUECs from the current SOC reports the user entity should identify and document the specific control or controls that they implemented to address each CUEC.

- The process of mapping the controls at the agency level to each SOC report will ensure that the agency's controls are adequately designed to address the CUEC requirements outlined by the service organizations.

- Addressing all the CUECs in the SOC reports will ensure that your agency can effectively rely on the system of controls being performed by service organizations.

QUESTIONS

VIRGINIA IT AGENCY

NCSR ANALYSIS

ED MILLER

DIRECTOR IT SECURITY GOVERNANCE

SEPTEMBER 30, 2022

NCSR

- Annually, the Commonwealth participates in the **National Cyber Security Review (NCSR).**

- The NCSR is a self-assessment survey aligned within the **NIST cybersecurity framework (CSF)** to evaluate an agency's cybersecurity posture.

- The survey is distributed to government agencies in all states, localities, tribal nations, and US territories. Nationally the survey has a very high participation rate, and the cumulated results are reported bi-annually to the US Congress.

- The NCSR provides significant insight into IT security practices at each agency by identifying gaps in performance areas that allow us to benchmark year-to-year progress.

- In addition, it gives a way to measure and compare the Commonwealth against other peer survey participants across the nation.

NCSR

- 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. (Asset Mgmt, Business Environment, Governance, Risk Assessments, Risk Mgmt Strategy, & Supply Chain Management)

  - ***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. (Access Control, Awareness/Training, Data Security, Information Protection/Procedures, Maintenance, Protective Technologies).

  - ***Detect*:** The quicker an agency is able to detect a cybersecurity incident, the better positioned it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the detect function pertain to an organization's ability to identify incidents. (Anomalies/Events, Continuous Monitoring, Detection Processes)

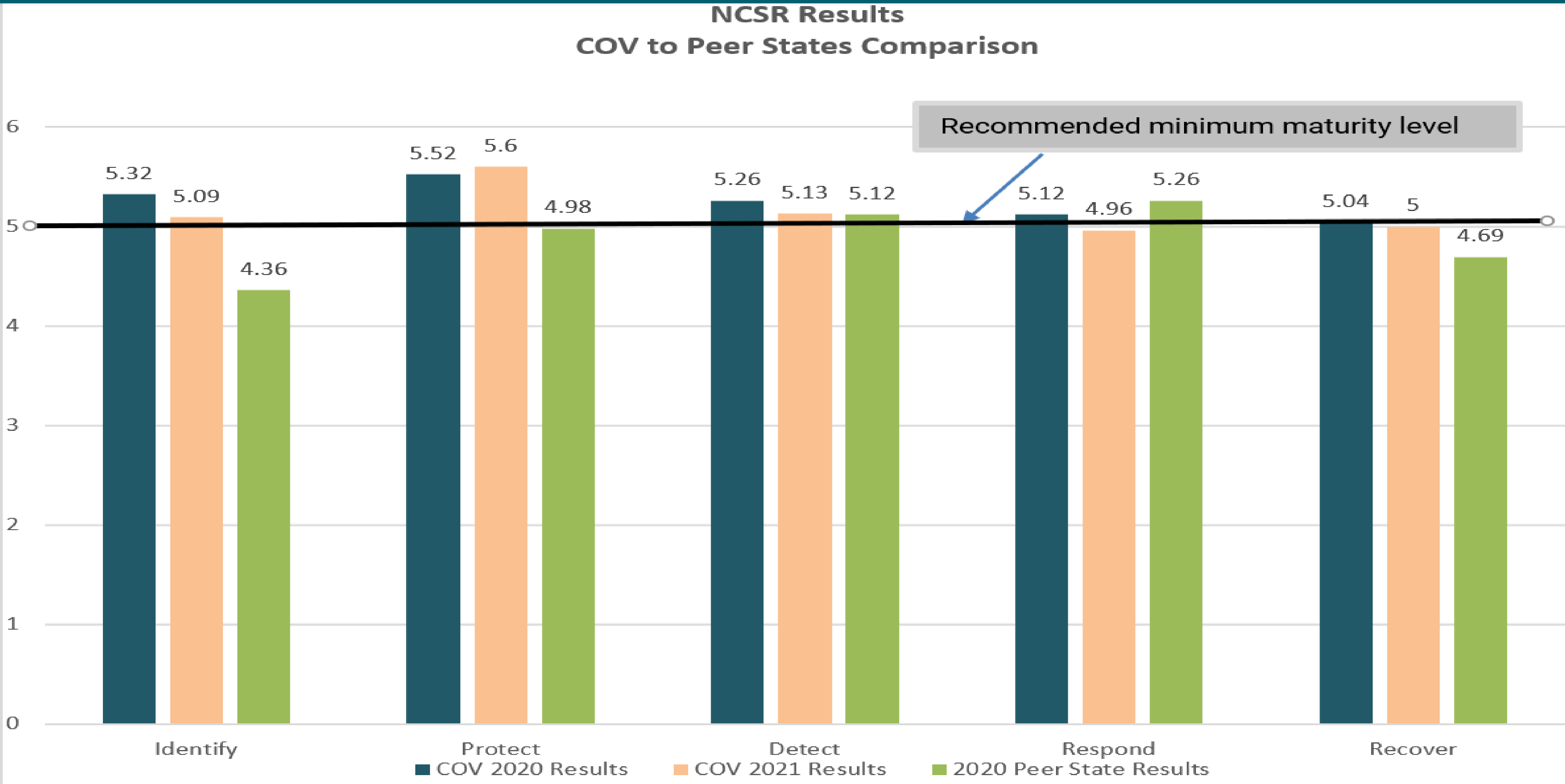
  - ***Respond*:** An agency's ability to quickly and appropriately respond to an incident plays a large role in reducing the incident's consequences. As such, the activities within the respond function examine how an agency plans, analyzes, communicates, mitigates, and improves its response capabilities. (Analysis, Communications, Improvements, Mitigation, Response Planning)

  - ***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 (Communications, Improvements, Recovery).

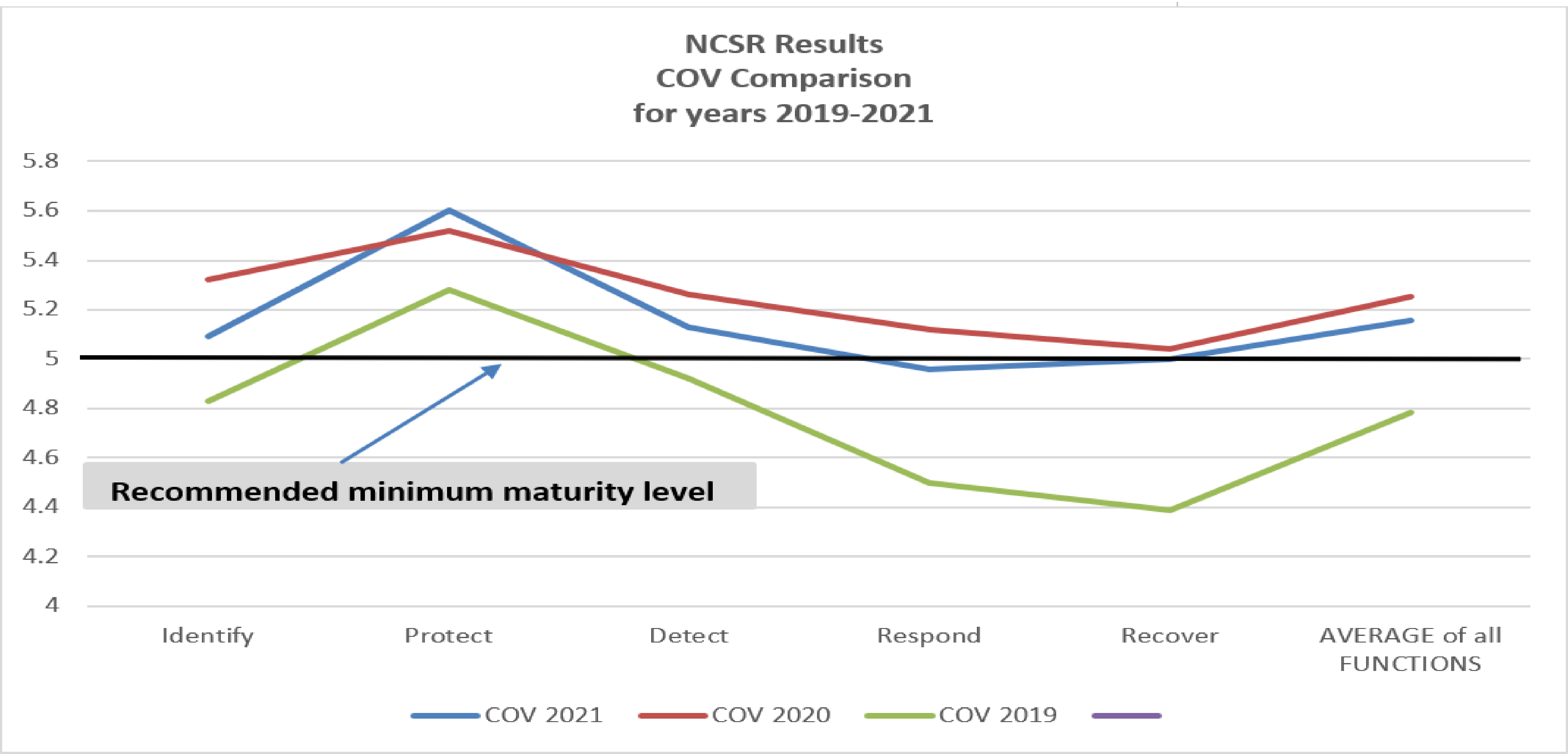
NCSR

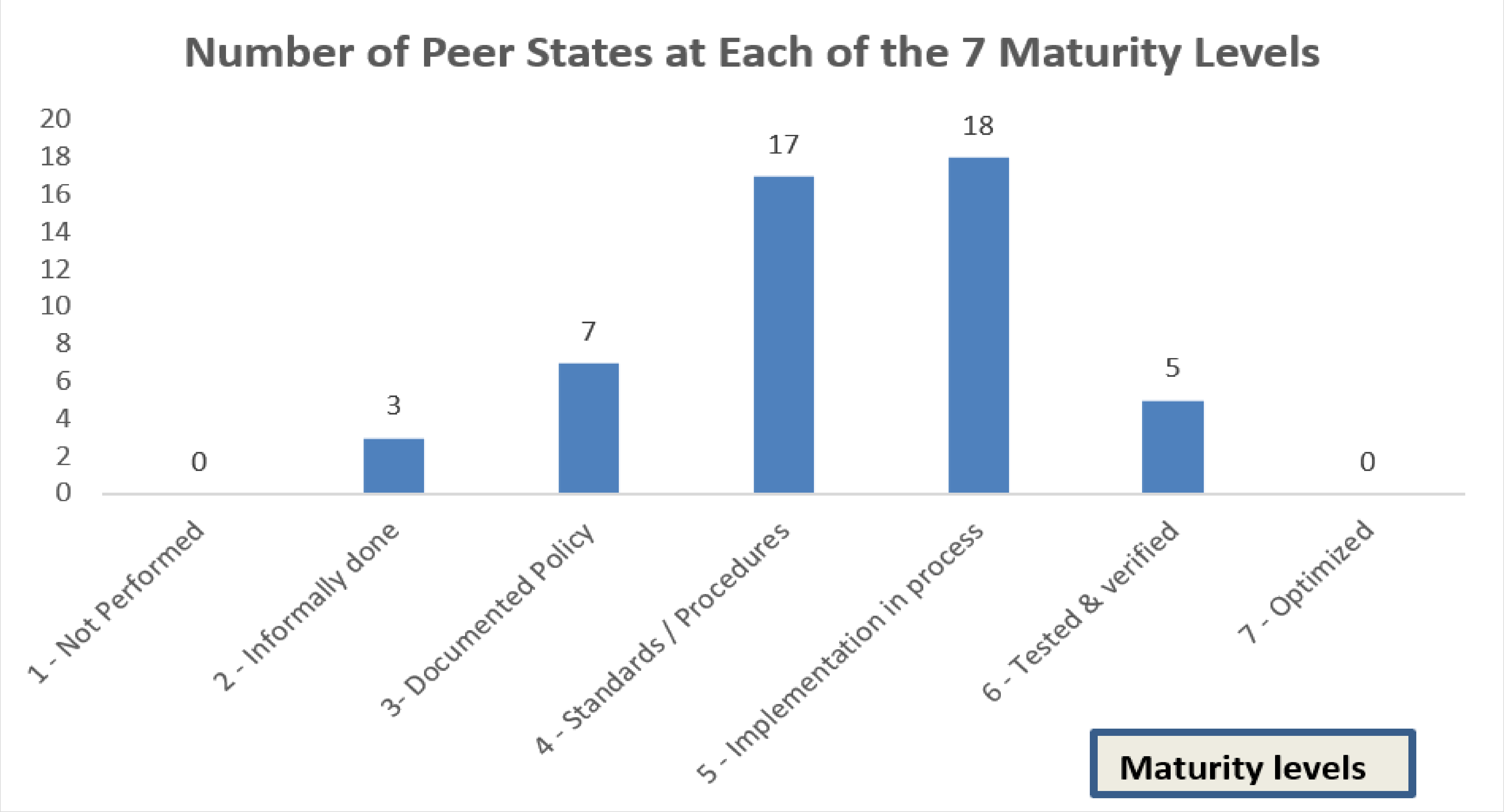
- Using a maturity scale measurement, each agency evaluates itself on several activities that support each core function. The scale is heavily policy focused and goes from a low score of one (activity is not performed, i.e., no processes, policies or technologies are in place) to a high score of seven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

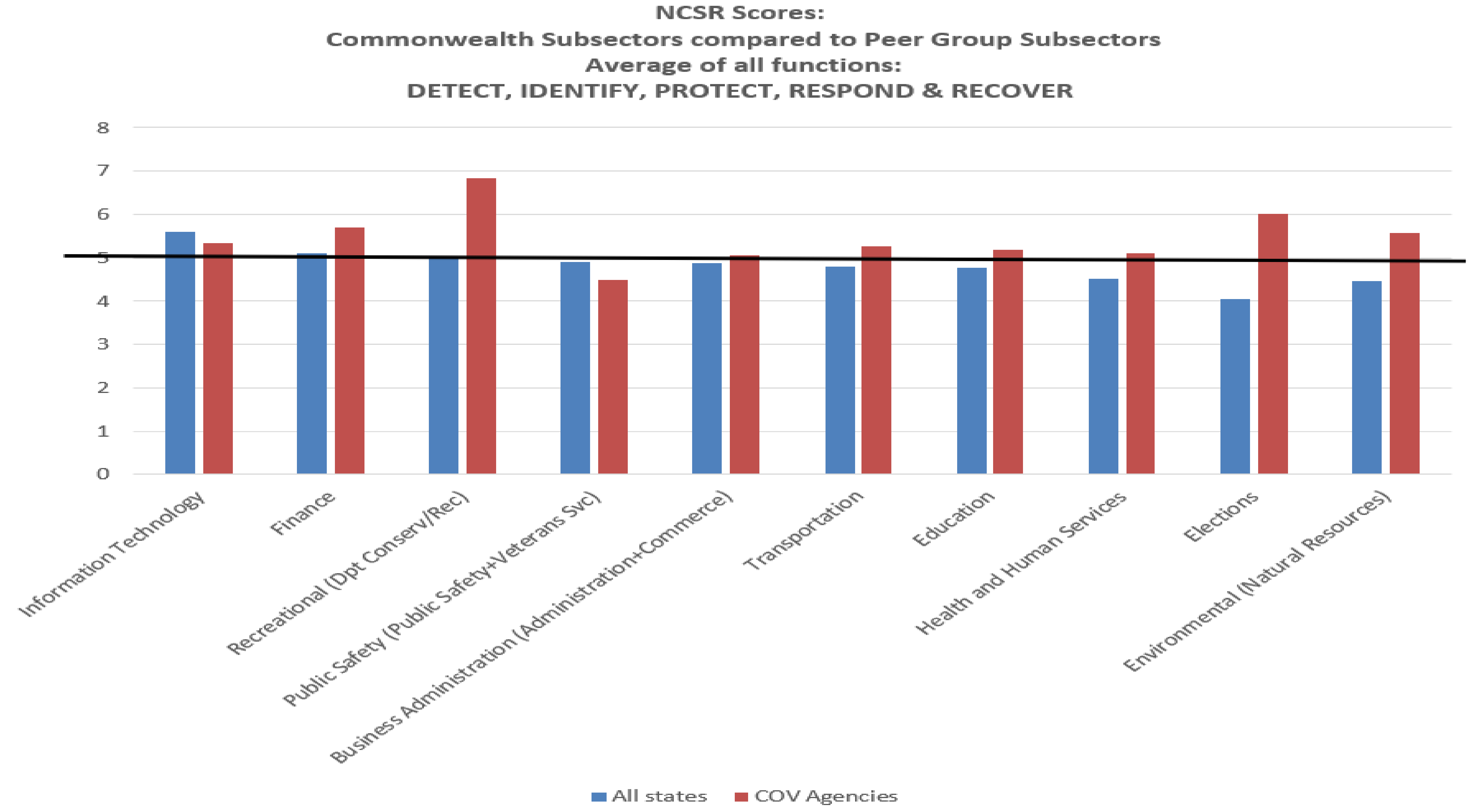

NCSR Results
COV to Peer States Comparison
Recommended minimum maturity level
6
5
4
3
2
1
0
5.32
5.09
4.36
5.52
5.6
4.98
5.26
5.13
5.12
5.12
4.96
5.26
5.04
5
4.69
Identify
Protect
Detect
Respond
Recover
COV 2020 Results
COV 2021 Results
2020 Peer State Results

NCSR


NCSR Results
COV Comparison
for years 2019-2021
5.8
5.6
5.4
5.2
5
4.8
4.6
4.4
4.2
4
Recommended minimum maturity level
Identify
Protect
Detect
Respond
Recover
AVERAGE of all FUNCTIONS
COV 2021
COV 2020
COV 2019



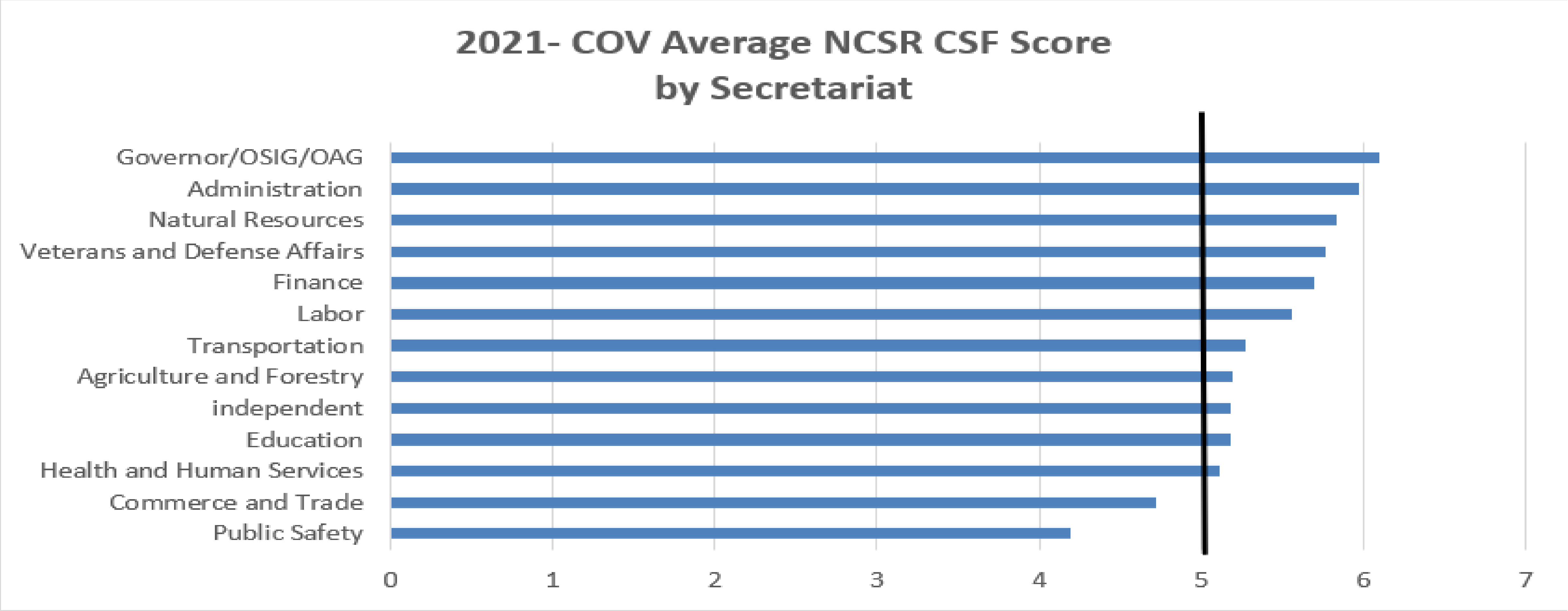
Number of Peer States at Each of the 7 Maturity Levels

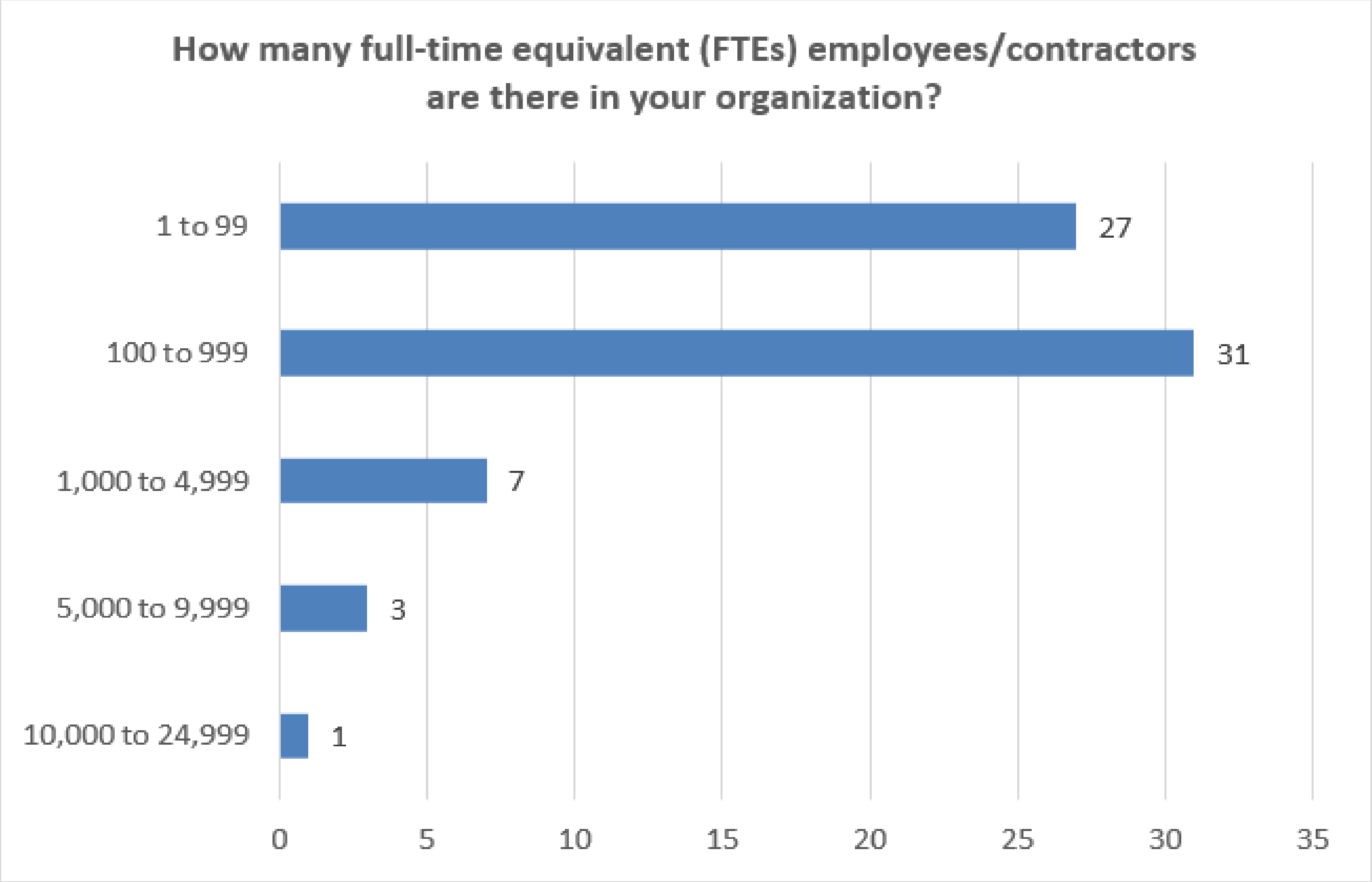


NCSR Scores:
Commonwealth Subsectors compared to Peer Group Subsectors
Average of all functions:
DETECT, IDENTIFY, PROTECT, RESPOND & RECOVER

NCSR

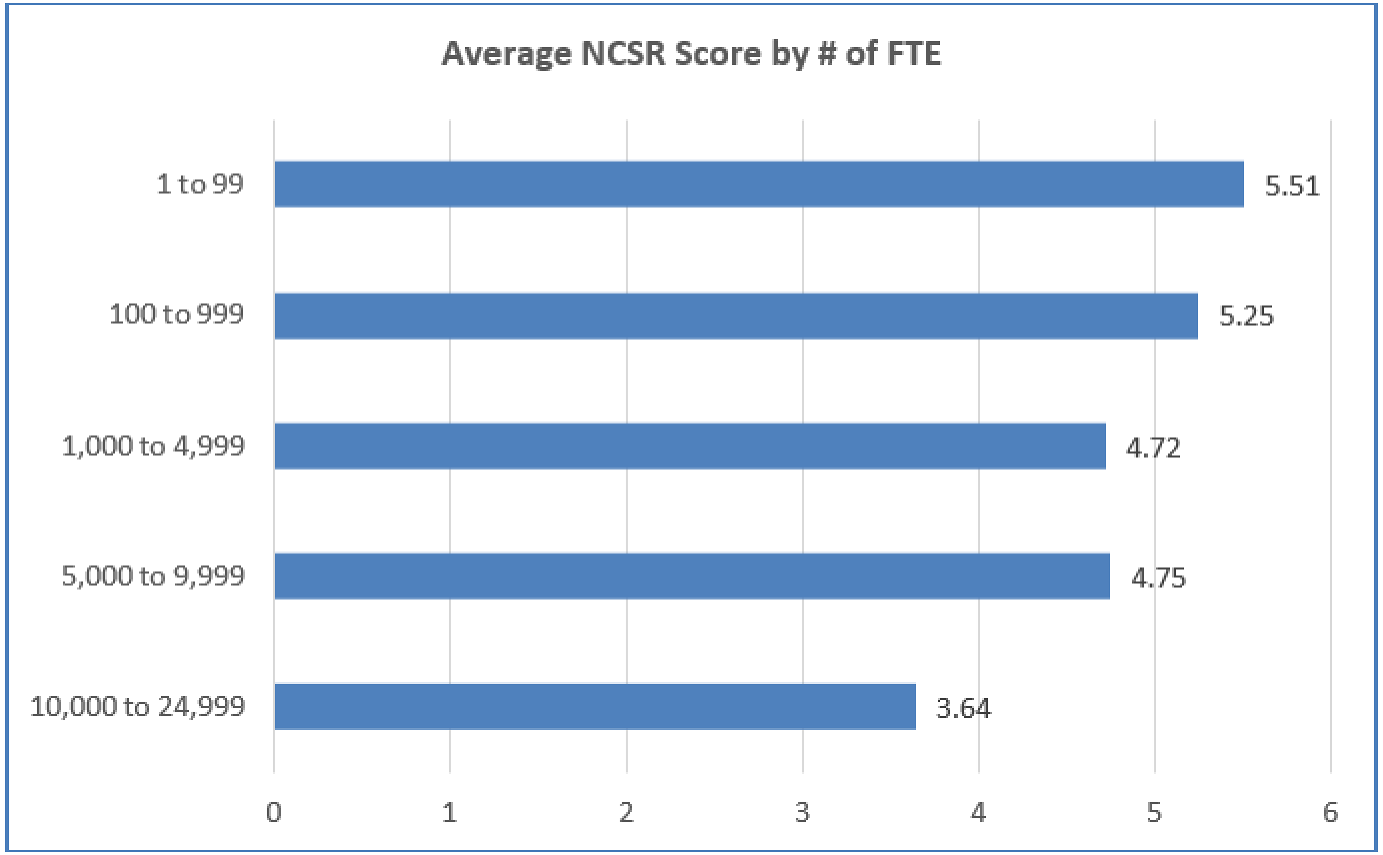
NCSR analysis by secretariat



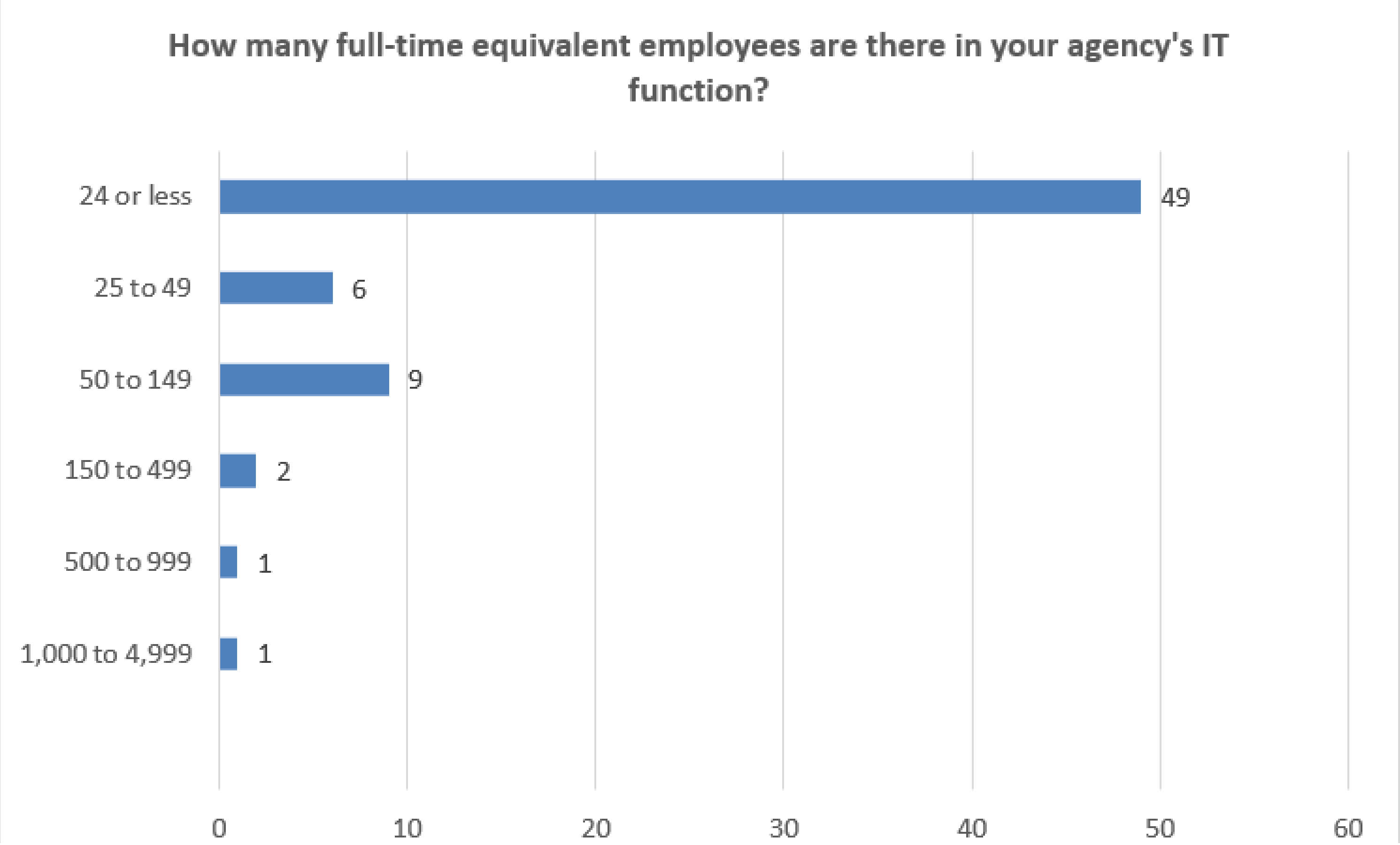

How many full-time equivalent (FTEs) employees/contractors are there in your organization?
1 to 99
27
100 to 999
31
1,000 to 4,999
7
5,000 to 9,999
3
10,000 to 24,999
1
0
5
10
15
20
25
30
35

NCSR

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

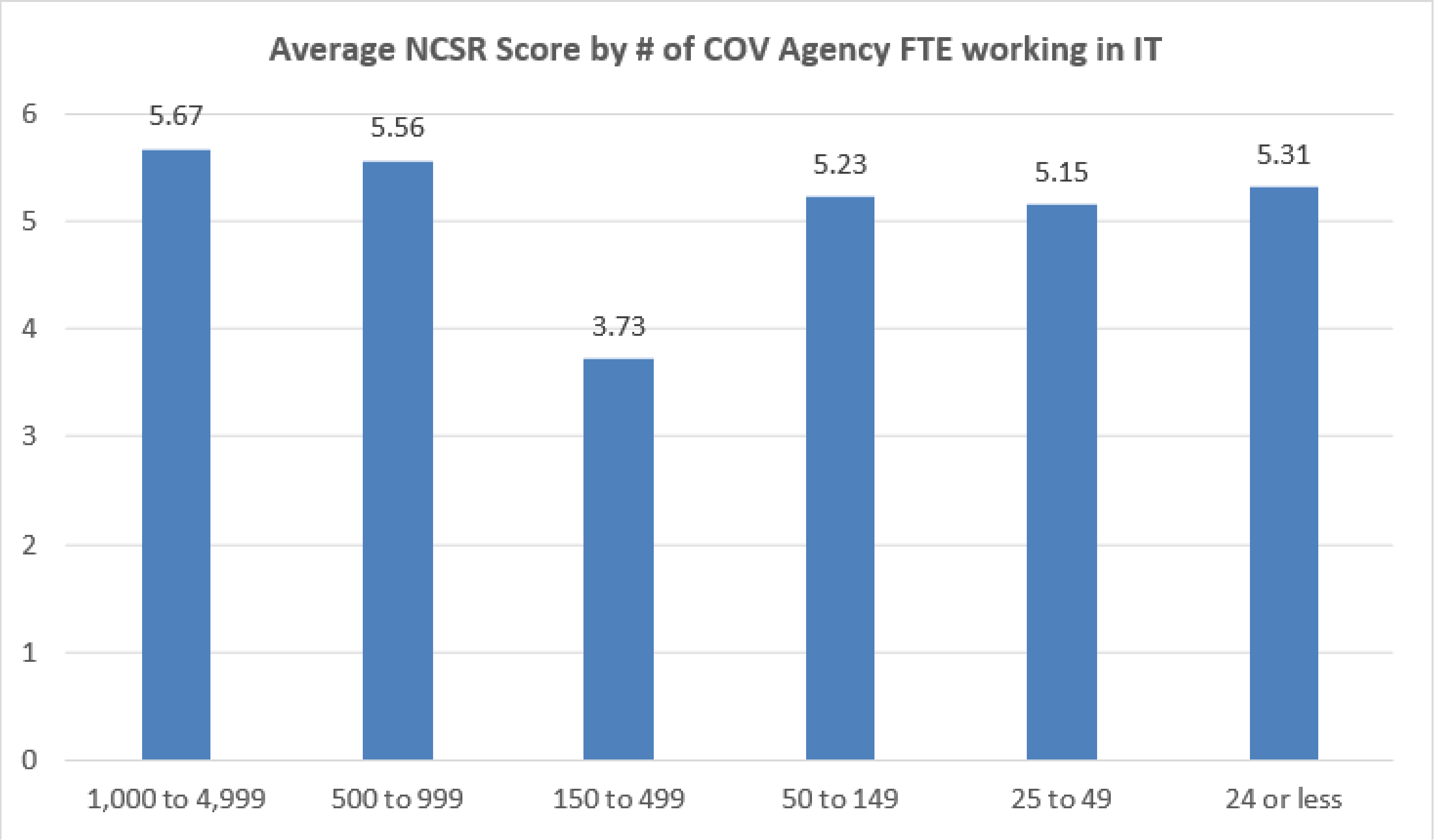


Agencies were also surveyed as to the number of full-time employees whose primary job responsibility is in Information technology. The majority of agencies reported that they have less than 24 employees working in the IT area.



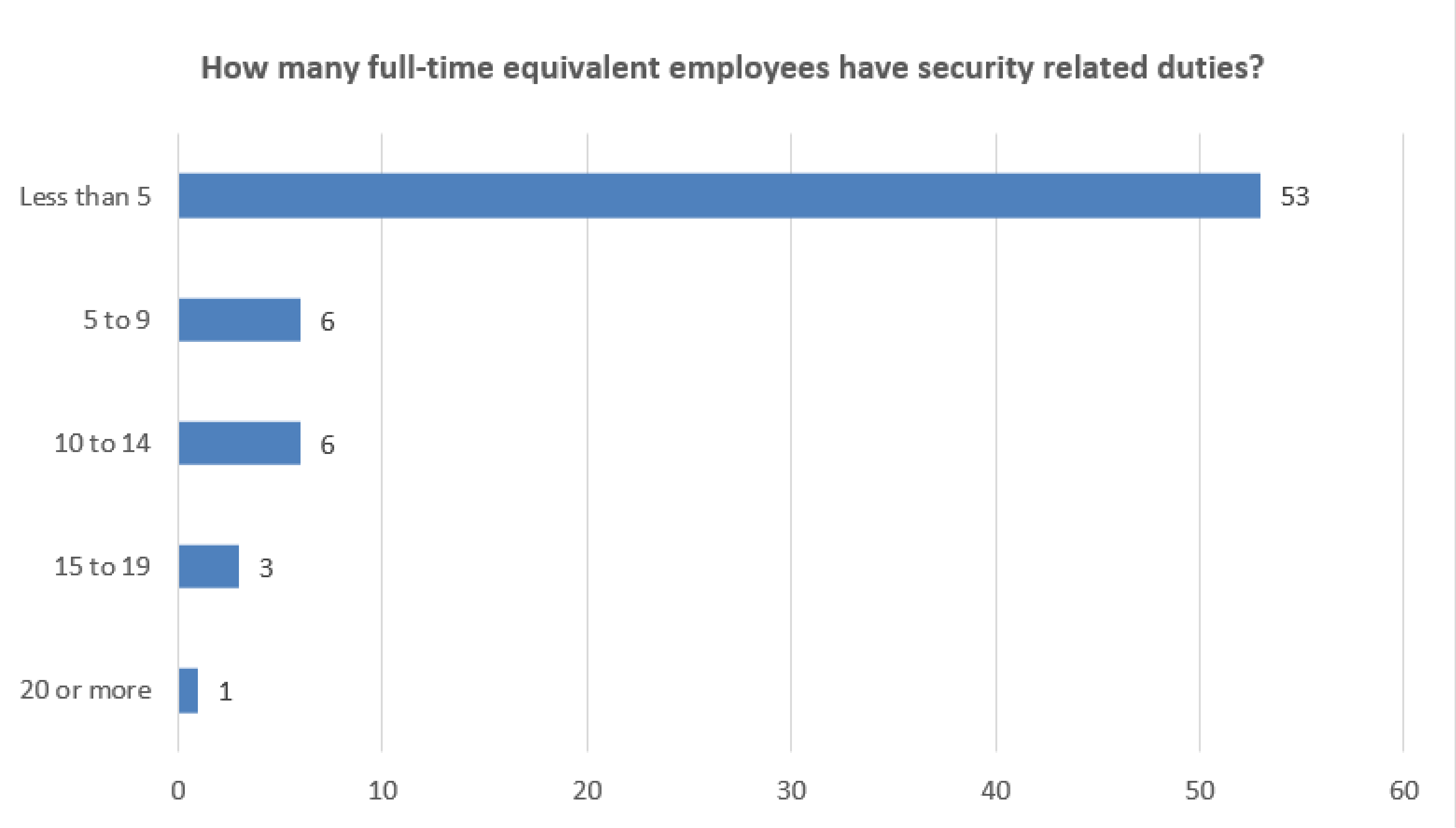
NCSR

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



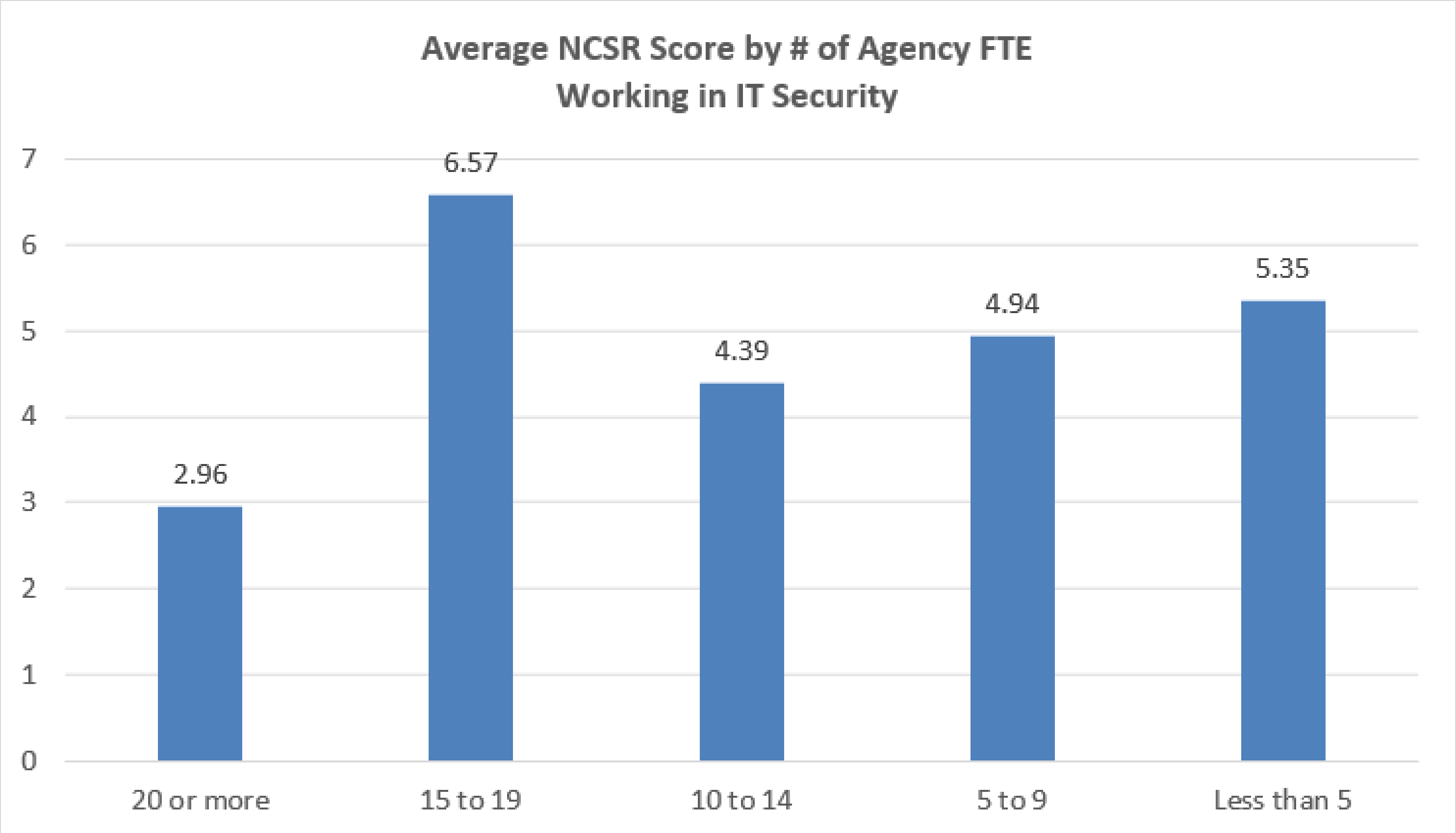
NCSR

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

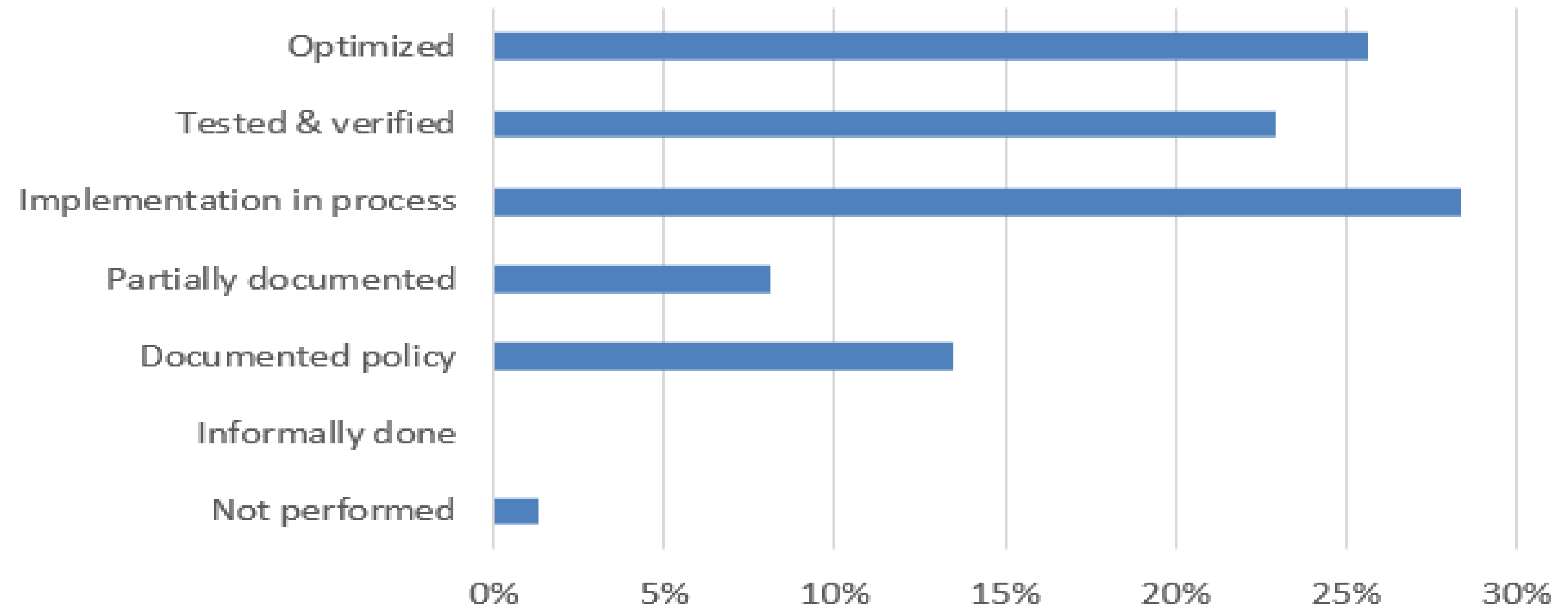


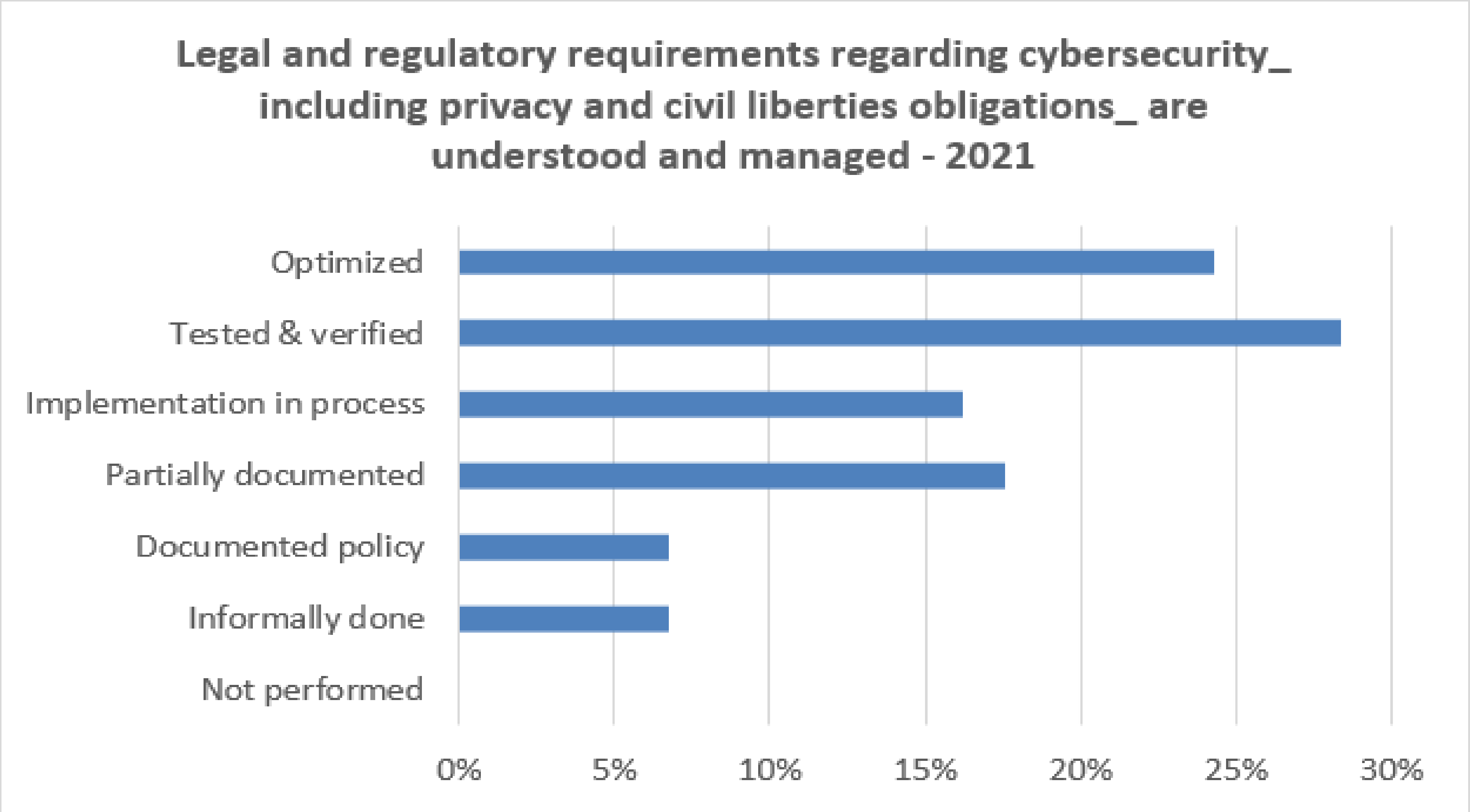
NCSR

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

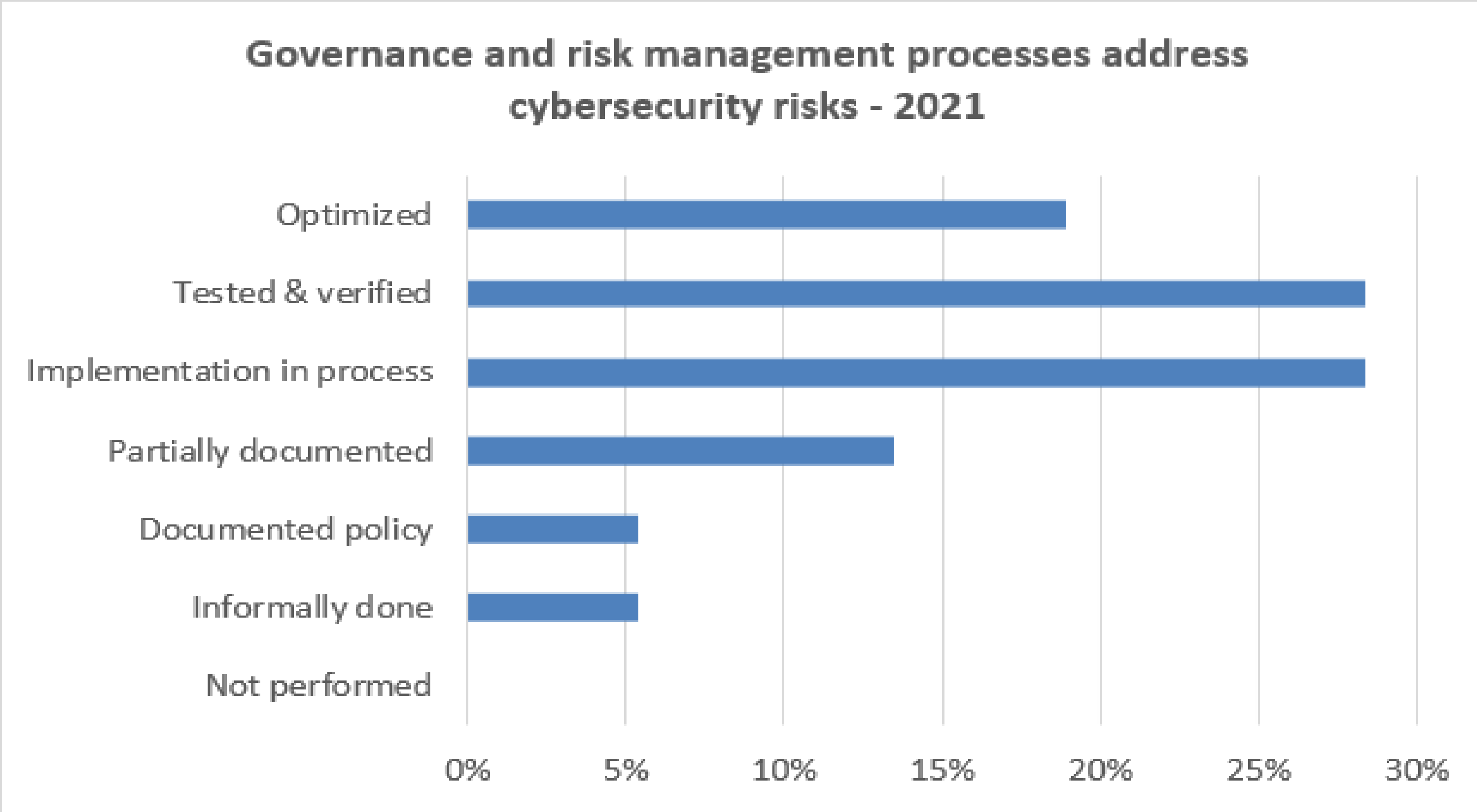


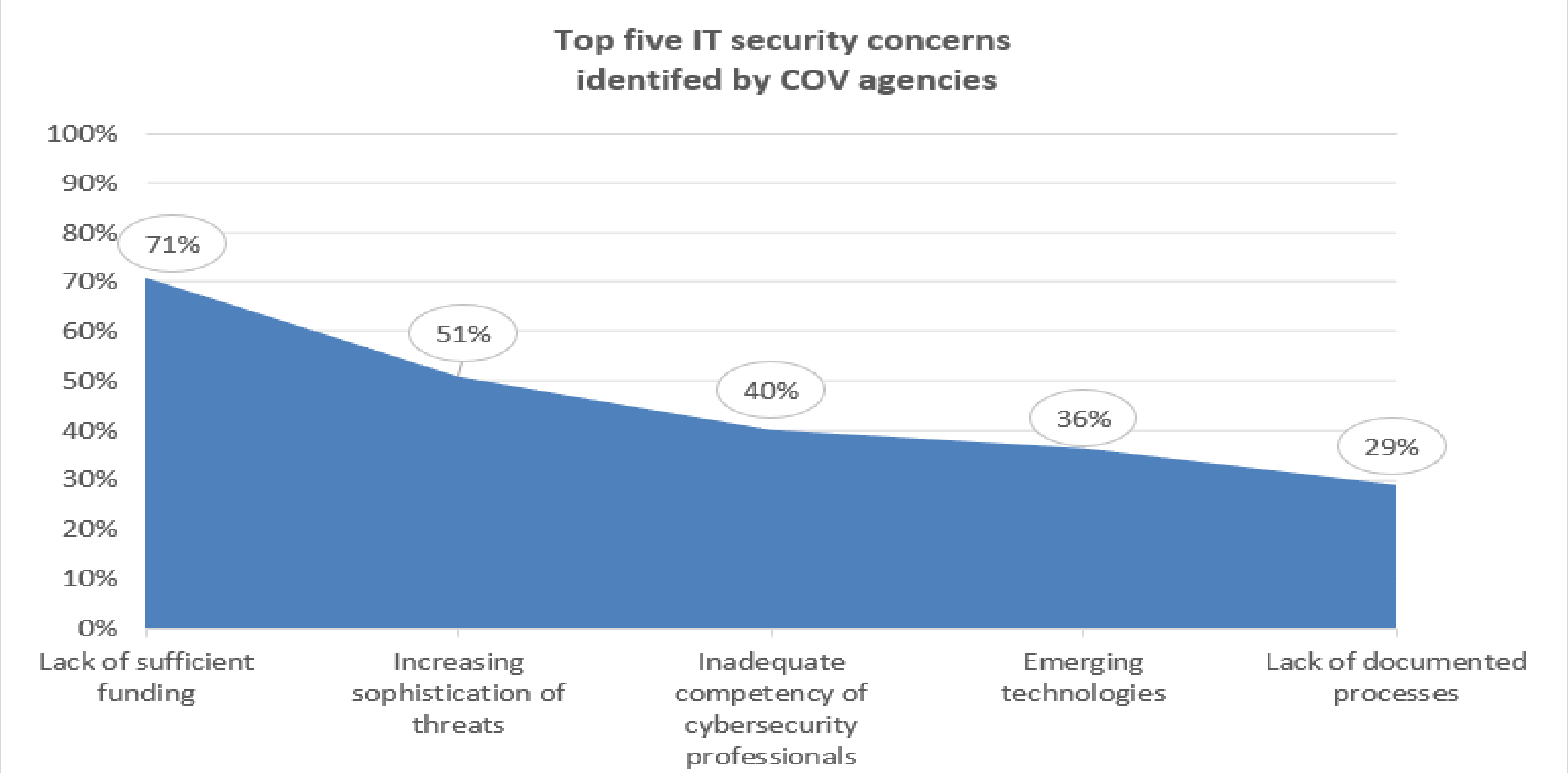
Organizational cybersecurity policy is established and communicated - 2021





Legal and regulatory requirements regarding cybersecurity_ including privacy and civil liberties obligations_ are understood and managed - 2021


Governance and risk management processes address cybersecurity risks - 2021
Optimized
Tested & verified
Implementation in process
Partially documented
Documented policy
Informally done
Not performed
0%
5%
10%
15%
20%
25%
30%


Top five IT security concerns
identifed by COV agencies
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
71%
51%
40%
36%
29%
Lack of sufficient funding
Increasing sophistication of threats
Inadequate competency of cybersecurity professionals
Emerging technologies
Lack of documented processes

SUMMARY

- Keep in mind that the NCSR is a SELF Assessment.
- Please be reasonable when you answer.
- It seems unlikely that with 140+ questions that any agency could reasonably score themselves as a 7 (optimized) for every single question.
- The NCSR provides valuable insight to how your agency measures against other agencies in the Commonwealth and across the country.

QUESTIONS

VIRGINIA
IT AGENCY

COV WIDE PHISHING CAMPAIGN
SEPTEMBER 2022

KATHY BORTLE & JAMES STURDEVANT, SR.

Incident Response Specialists

VITA/CSRM /THREAT MANAGEMENT TEAM

OCTOBER 5TH, 2022

OVERVIEW

OVERVIEW

September 2022 Phishing Campaign (Q3 2022)

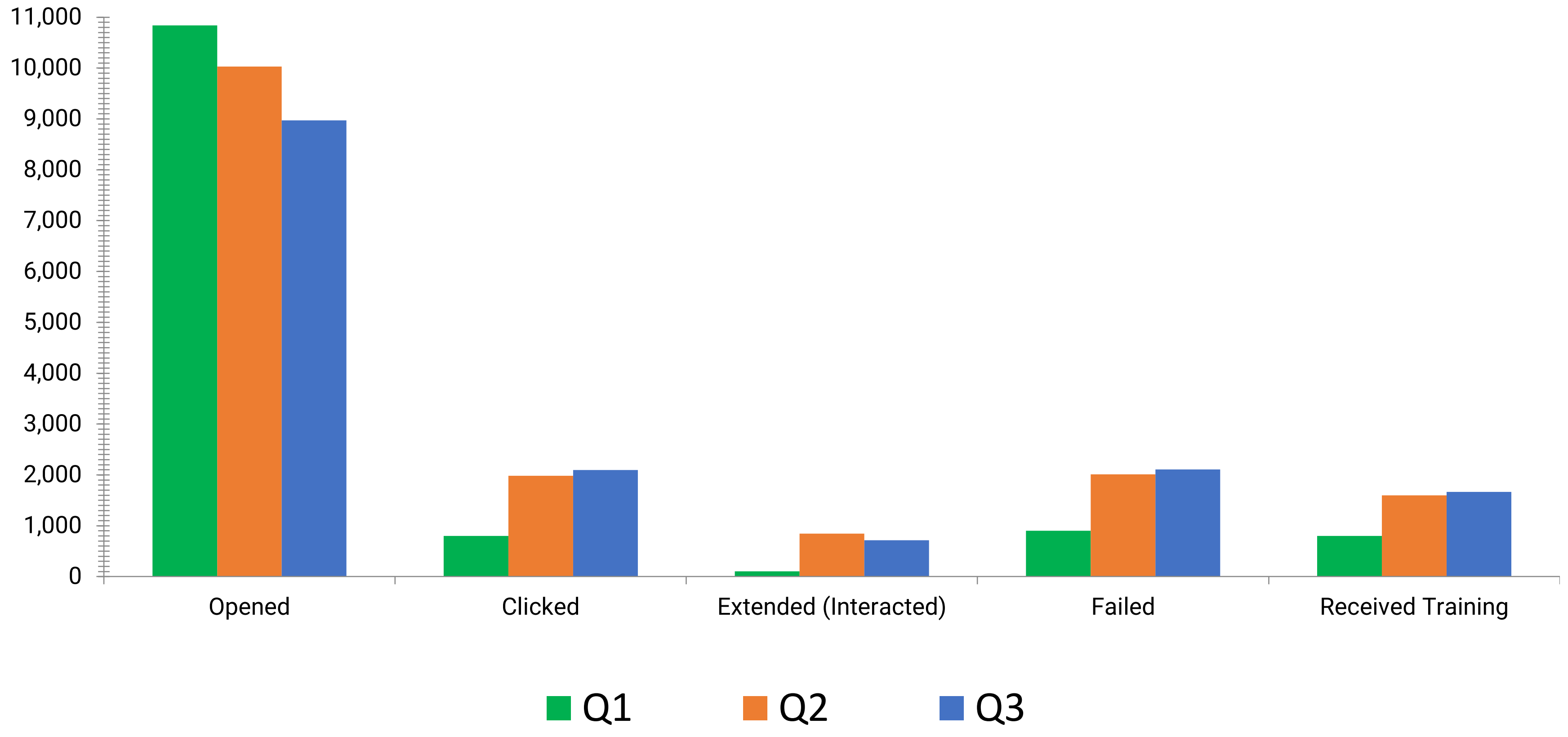
VITA selected 3 messages that should have been relatively easy to identify to set a baseline. These messages were sent to all users with an active email address. The test for each group ran for 3 days after message delivery to collect the results. All FY23 phishing accounts were enabled and all FY22 phishing accounts were disabled. If an entire agency was completed in FY22, then only new employees were phished during FY23.

Before we launched the campaign …..

1. All email domains were verified as whitelisted.
2. All user accounts were verified to be enabled in Active Directory. Any AD account that were disabled due to inactivity or a user leaving, were removed from the campaign.
3. The exhaustive report which provides the actions a user performed is limited to 2,500 rows. This is fine for small agencies. However, if your agency has over 2,500 actions to report, the full details are provided in the CSV export.

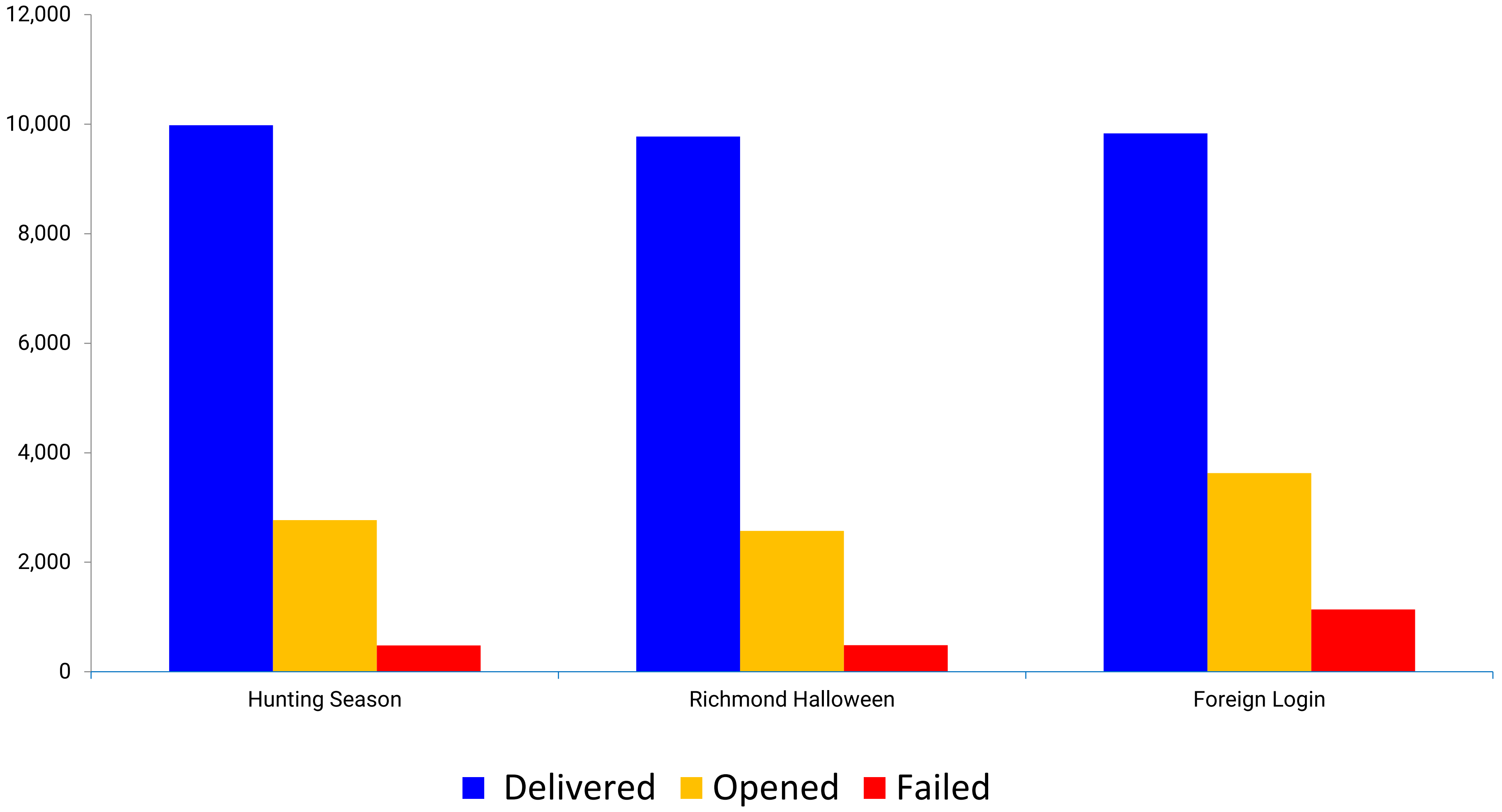
Q3 2022 PHISHING CAMPAIGN RESULTS

COV RESULTS BY ACTION TAKEN
Q1 – Q3 2022

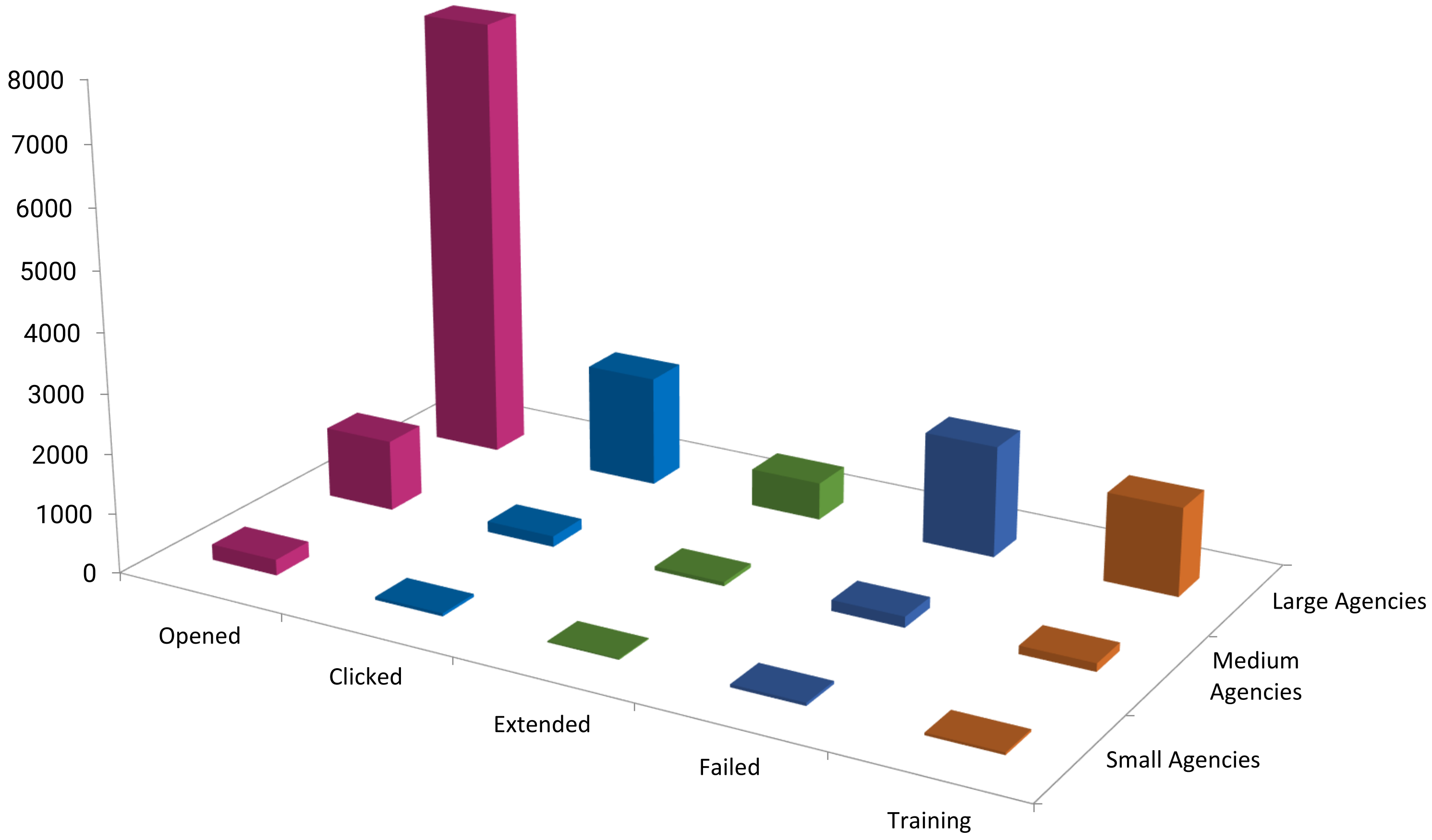


VIRGINIA IT AGENCY

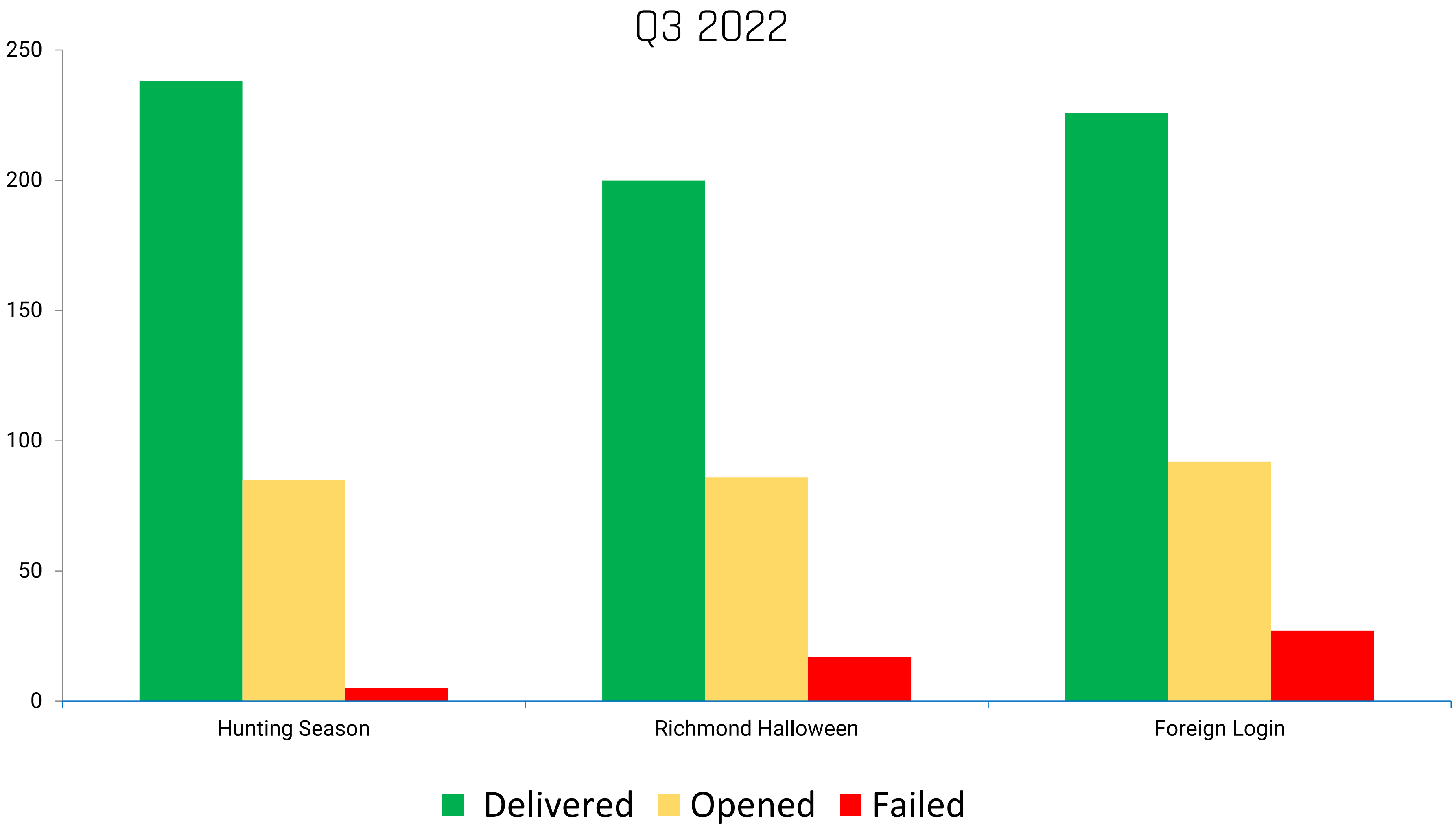
COV RESULTS BY PHISHING MESSAGE
Q3 2022



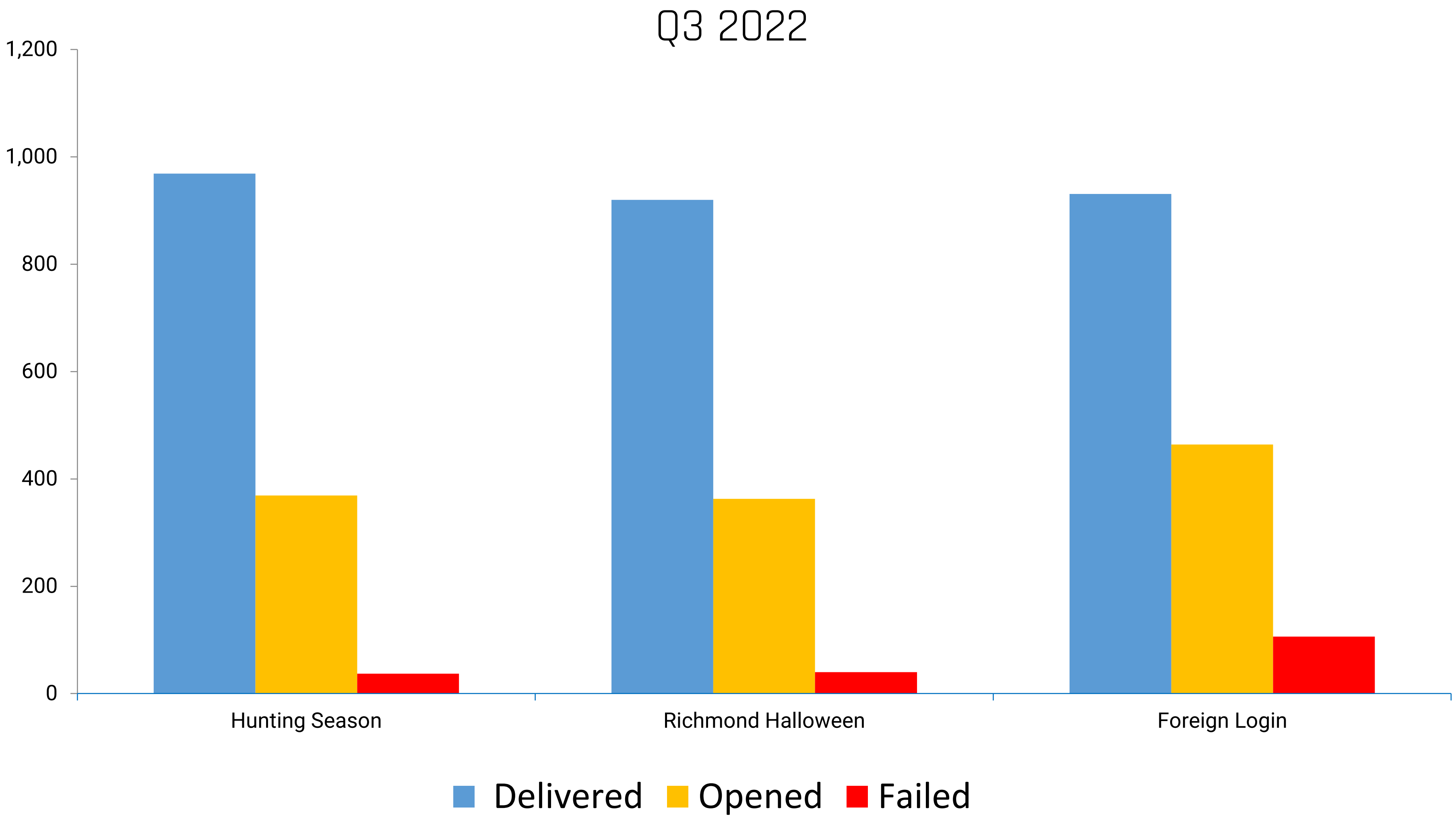
AGENCY RESULTS BY ACTION TAKEN Q3 2022



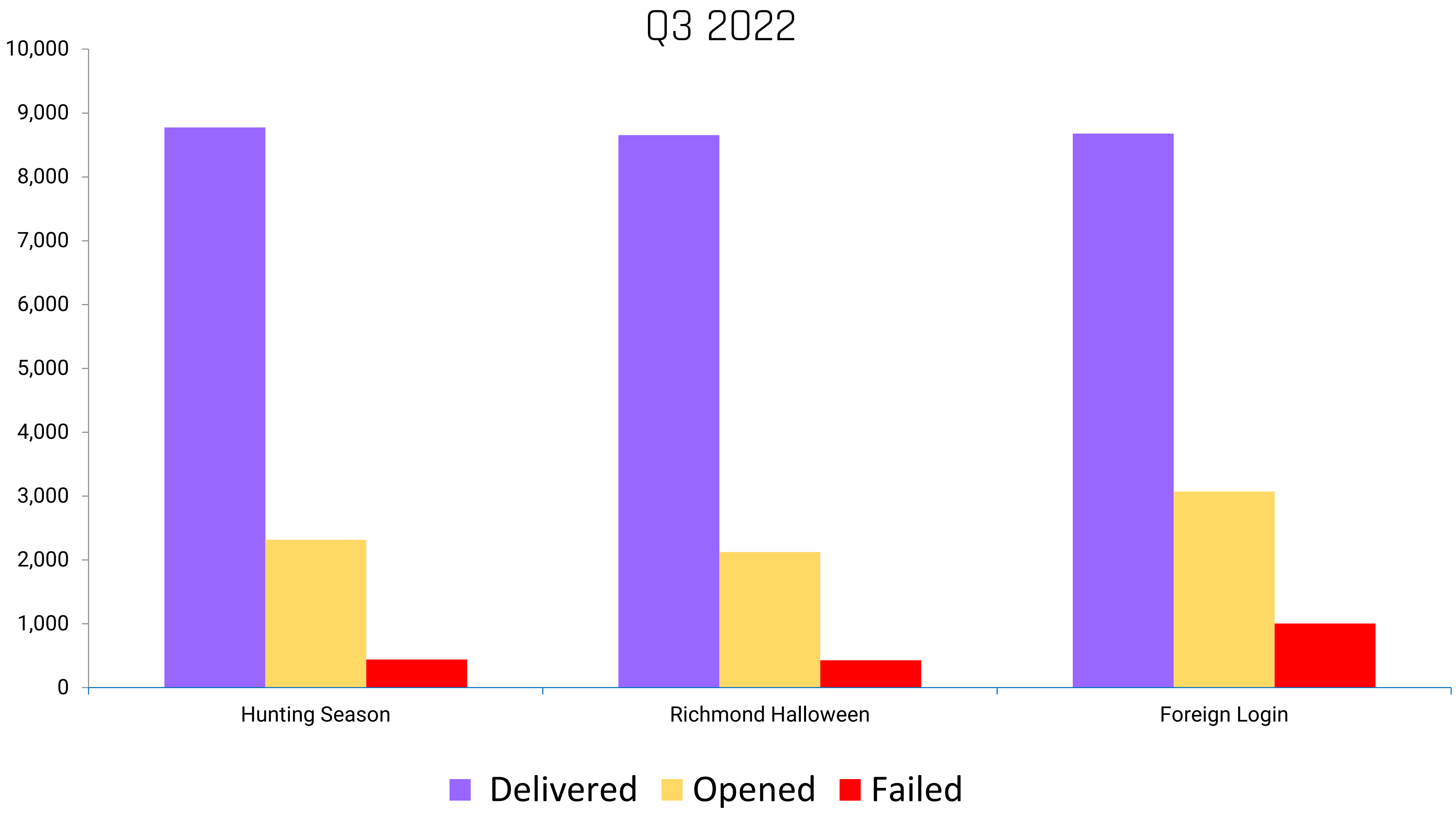
RESULTS BY PHISHING MESSAGE SMALL AGENCIES



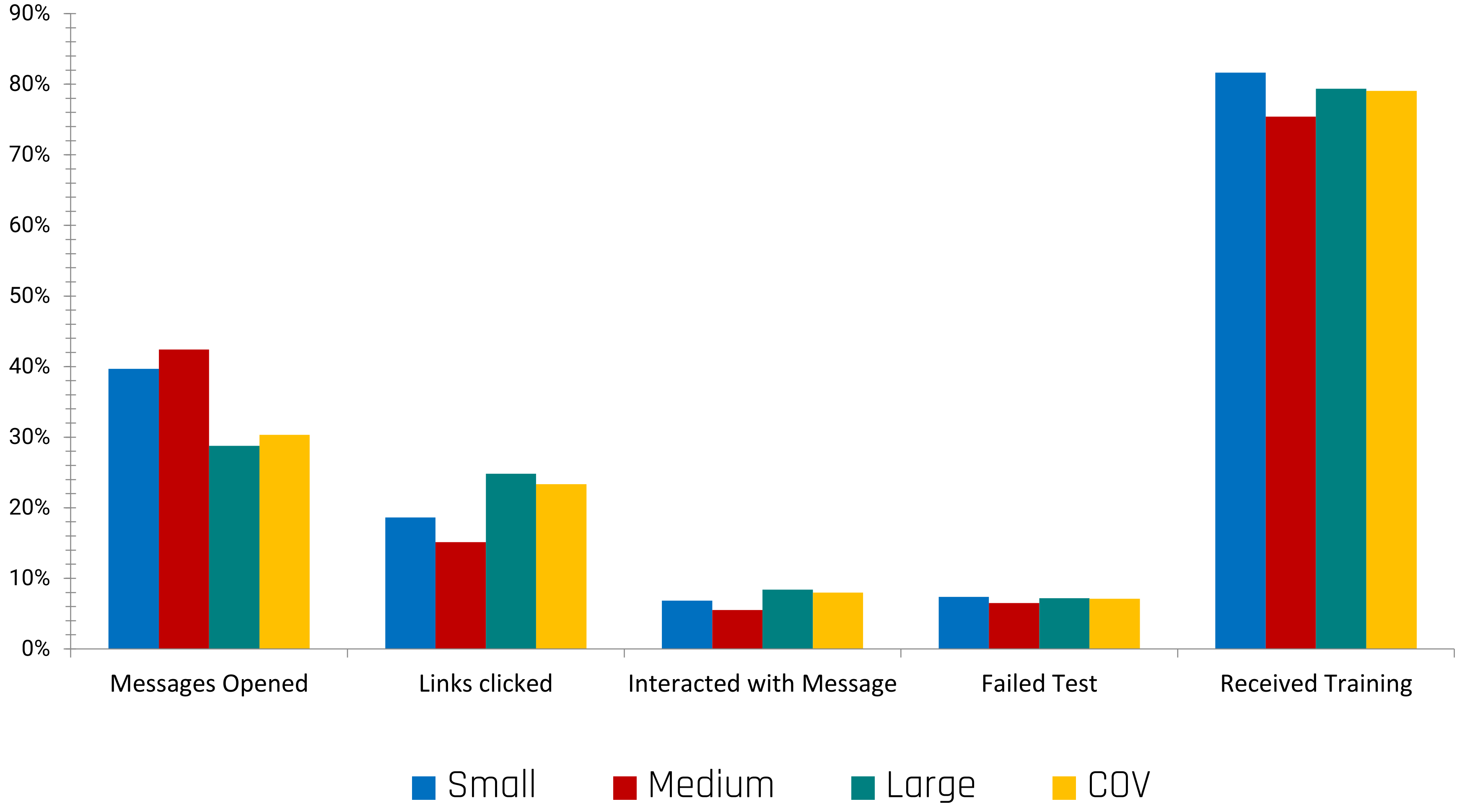
RESULTS BY PHISHING MESSAGE MEDIUM AGENCIES



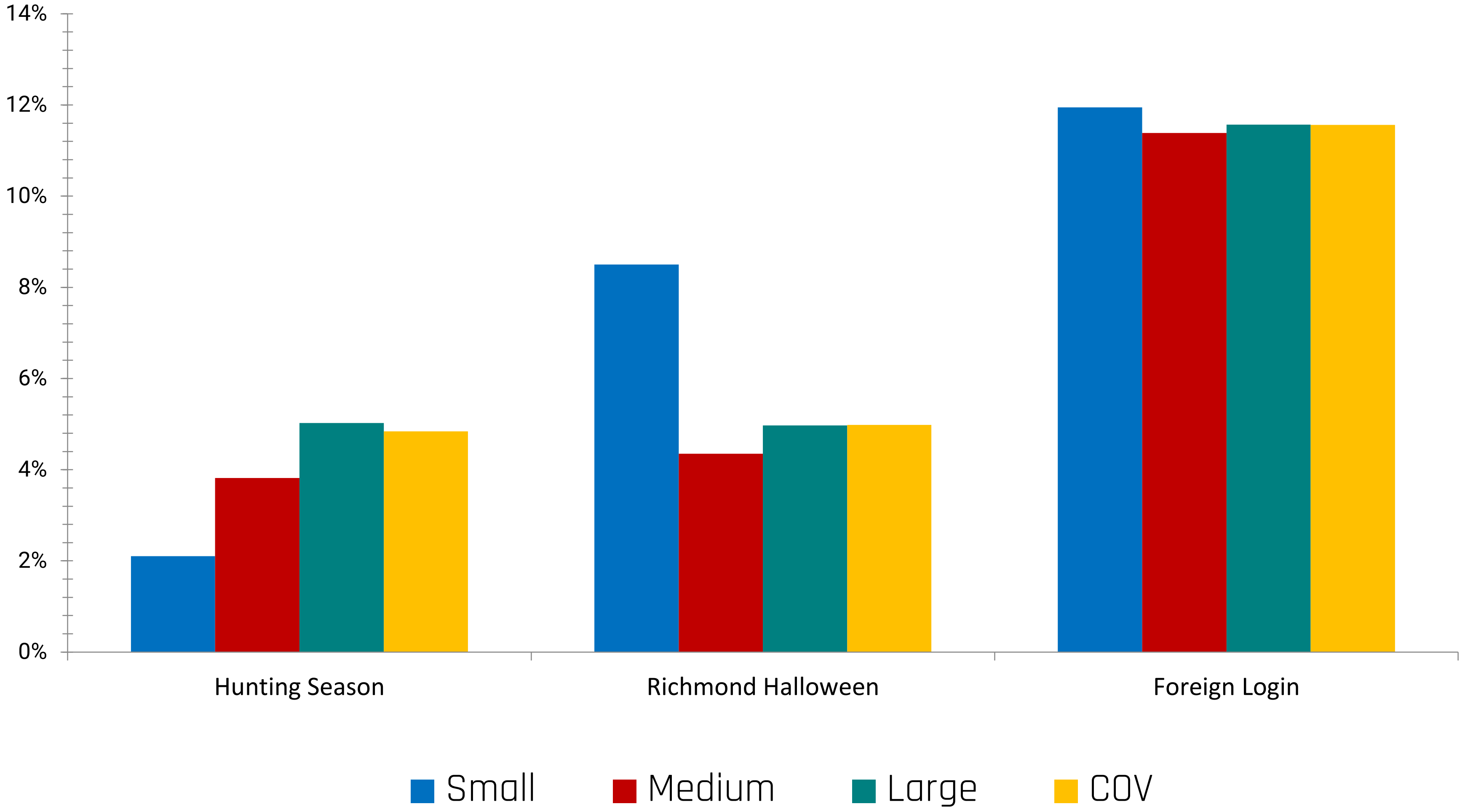
RESULTS BY PHISHING MESSAGE
LARGE AGENCIES



COV VS AGENCY ACTIONS TAKEN
Q3 2022



SUCCESS RATE OF PHISHING MESSAGES Q3 2022



EXAMPLE REPORTS

REPORTING RESULTS

There are three types of reports that CSRM pulls once a phishing campaign has been completed. These are:

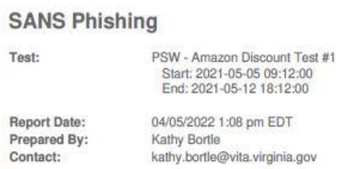
- Full Report
- Exhaustive Report
- Repeat Offenders Report – this report will be available after the user participates in multiple campaigns
- CSV Export - This file will contain all results for that test.

FULLREPORT

INCLUDES:

- TEST SUMMARY
- PHISHING TERM APPENDIX

Full Report

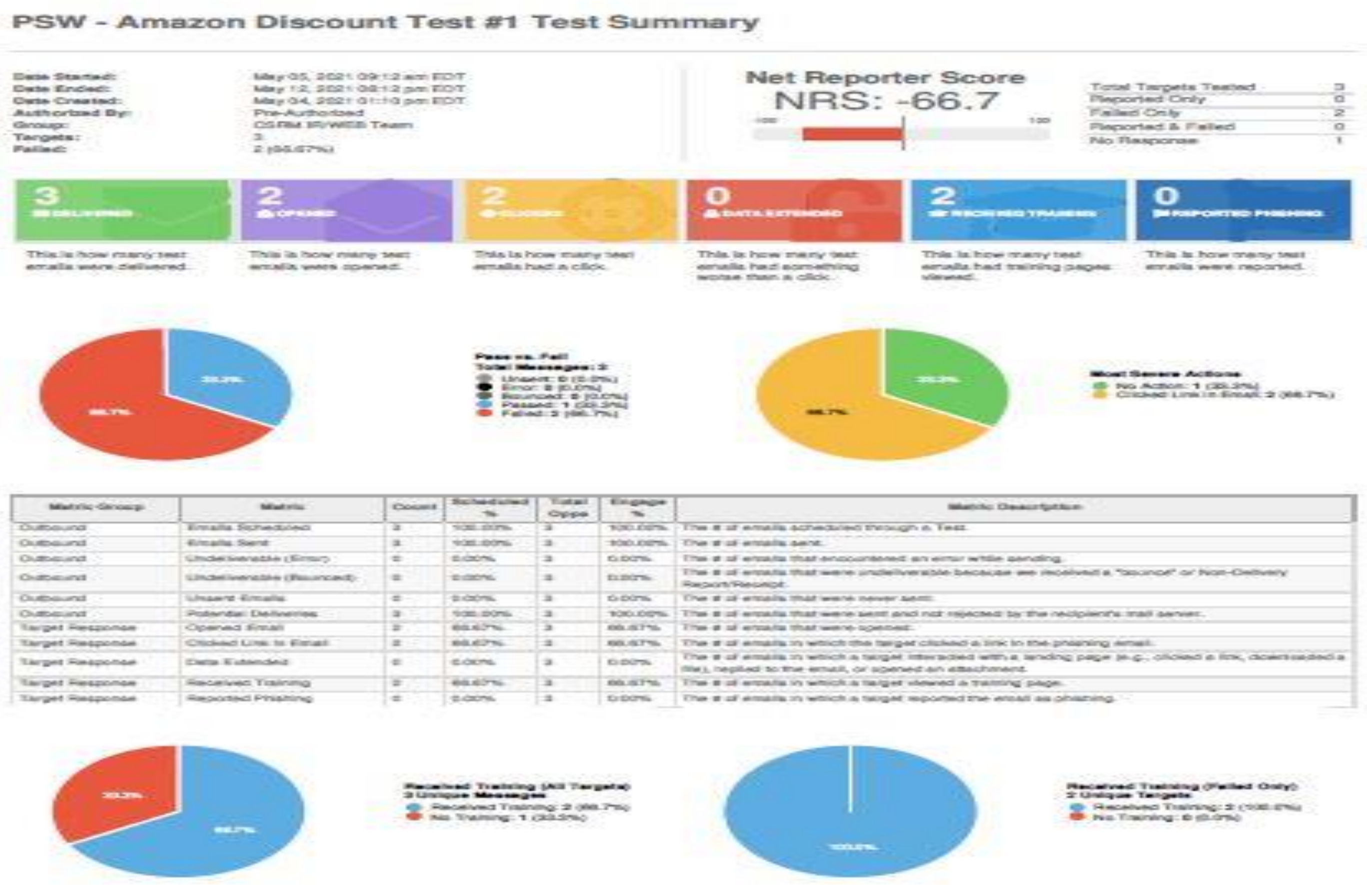


SANS Phishing

Test: PSW - Amazon Discount Test #1
Start: 2021-05-05 09:12:00
End: 2021-05-12 18:12:00

Report Date: 04/05/2022 1:08 pm EDT
Prepared By: Kathy Bortle
Contact: kathy.bortle@vita.virginia.gov

FULL REPORT TEST SUMMARY



PSW - Amazon Discount Test #1 Test Summary

Date Started:	May 05, 2021 09:12 am EDT
Date Ended:	May 12, 2021 08:12 pm EDT
Date Created:	May 04, 2021 01:10 pm EDT
Authorized By:	Pre-Authorized
Group:	CSRM IR/WEB Team
Targets:	3
Failed:	2 (66.67%)

Net Reporter Score

NRS: -66.7

Total Targets Tested	3
Reported Only	0
Failed Only	2
Reported & Failed	0
No Response	1

3 DELIVERED

This is how many test emails were delivered.

2 OPENED

This is how many test emails were opened.

2 CLICKED

This is how many test emails had a click.

0 DATA EXTENDED

This is how many test emails had something worse than a click.

2 RECEIVED TRAINING

This is how many test emails had training pages viewed.

0 REPORTED PHISHING

This is how many test emails were reported.

Pass vs. Fail
Total Messages: 3
- Unsent: 0 (0.0%)
- Error: 0 (0.0%)
- Bounced: 0 (0.0%)
- Passed: 1 (33.3%)
- Failed: 2 (66.7%)

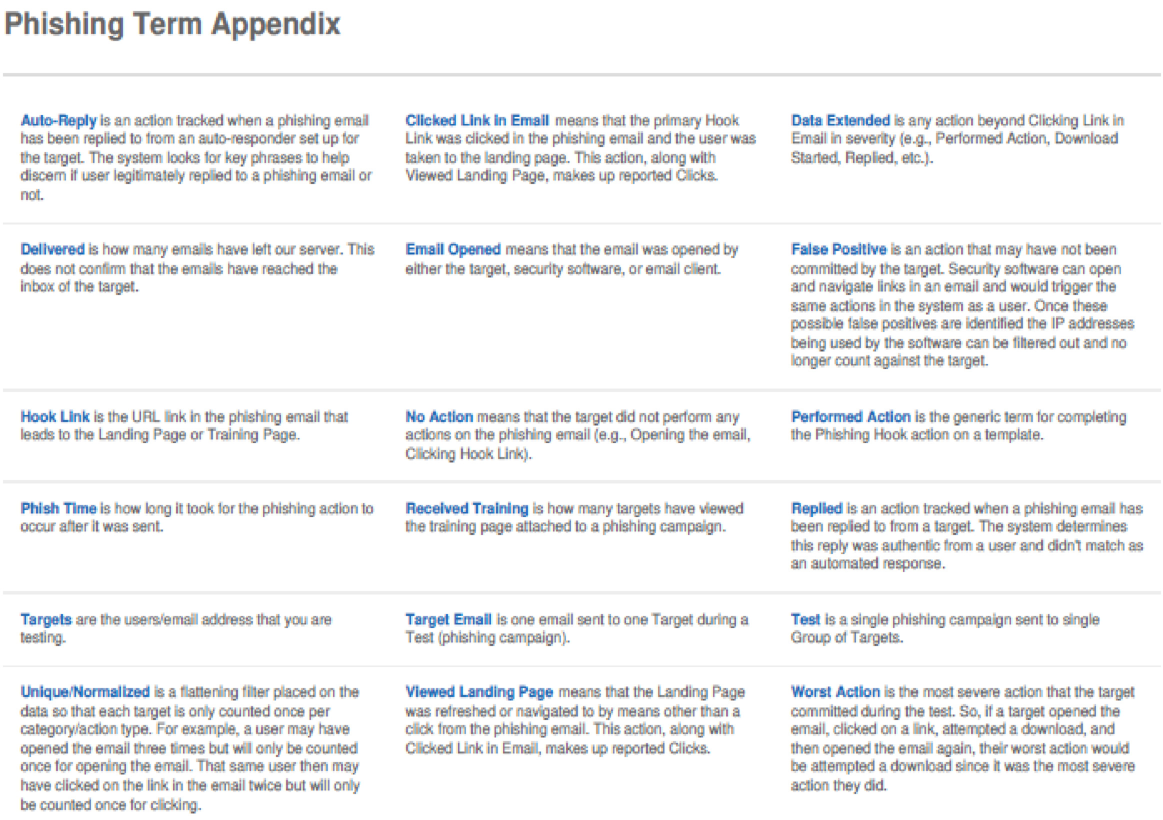
Most Severe Actions
- No Action: 1 (33.3%)
- Clicked Link in Email: 2 (66.7%)

Metric Group	Metric	Count	Scheduled %	Total Opps	Engage %	Metric Description
Outbound	Emails Scheduled	3	100.00%	3	100.00%	The # of emails scheduled through a Test.
Outbound	Emails Sent	3	100.00%	3	100.00%	The # of emails sent.
Outbound	Undeliverable (Error)	0	0.00%	3	0.00%	The # of emails that encountered an error while sending.
Outbound	Undeliverable (Bounced)	0	0.00%	3	0.00%	The # of emails that were undeliverable because we received a "bounce" or Non-Delivery Report/Receipt.
Outbound	Unsent Emails	0	0.00%	3	0.00%	The # of emails that were never sent.
Outbound	Potential Deliveries	3	100.00%	3	100.00%	The # of emails that were sent and not rejected by the recipient's mail server.
Target Response	Opened Email	2	66.67%	3	66.67%	The # of emails that were opened.
Target Response	Clicked Link in Email	2	66.67%	3	66.67%	The # of emails in which the target clicked a link in the phishing email.
Target Response	Data Extended	0	0.00%	3	0.00%	The # of emails in which a target interacted with a landing page (e.g., clicked a link, downloaded a file), replied to the email, or opened an attachment.
Target Response	Received Training	2	66.67%	3	66.67%	The # of emails in which a target viewed a training page.
Target Response	Reported Phishing	0	0.00%	3	0.00%	The # of emails in which a target reported the email as phishing.

Received Training (All Targets)
3 Unique Messages
- Received Training: 2 (66.7%)
- No Training: 1 (33.3%)

Received Training (Failed Only)
2 Unique Targets
- Received Training: 2 (100.0%)
- No Training: 0 (0.0%)

FULL REPORT – PHISHING TERM APPENDIX



Phishing Term Appendix

Auto-Reply is an action tracked when a phishing email has been replied to from an auto-responder set up for the target. The system looks for key phrases to help discern if user legitimately replied to a phishing email or not.

Clicked Link In Email means that the primary Hook Link was clicked in the phishing email and the user was taken to the landing page. This action, along with Viewed Landing Page, makes up reported Clicks.

Data Extended is any action beyond Clicking Link in Email in severity (e.g., Performed Action, Download Started, Replied, etc.).

Delivered is how many emails have left our server. This does not confirm that the emails have reached the inbox of the target.

Email Opened means that the email was opened by either the target, security software, or email client.

False Positive is an action that may have not been committed by the target. Security software can open and navigate links in an email and would trigger the same actions in the system as a user. Once these possible false positives are identified the IP addresses being used by the software can be filtered out and no longer count against the target.

Hook Link is the URL link in the phishing email that leads to the Landing Page or Training Page.

No Action means that the target did not perform any actions on the phishing email (e.g., Opening the email, Clicking Hook Link).

Performed Action is the generic term for completing the Phishing Hook action on a template.

Phish Time is how long it took for the phishing action to occur after it was sent.

Received Training is how many targets have viewed the training page attached to a phishing campaign.

Replied is an action tracked when a phishing email has been replied to from a target. The system determines this reply was authentic from a user and didn't match as an automated response.

Targets are the users/email address that you are testing.

Target Email is one email sent to one Target during a Test (phishing campaign).

Test is a single phishing campaign sent to single Group of Targets.

Unique/Normalized is a flattening filter placed on the data so that each target is only counted once per category/action type. For example, a user may have opened the email three times but will only be counted once for opening the email. That same user then may have clicked on the link in the email twice but will only be counted once for clicking.

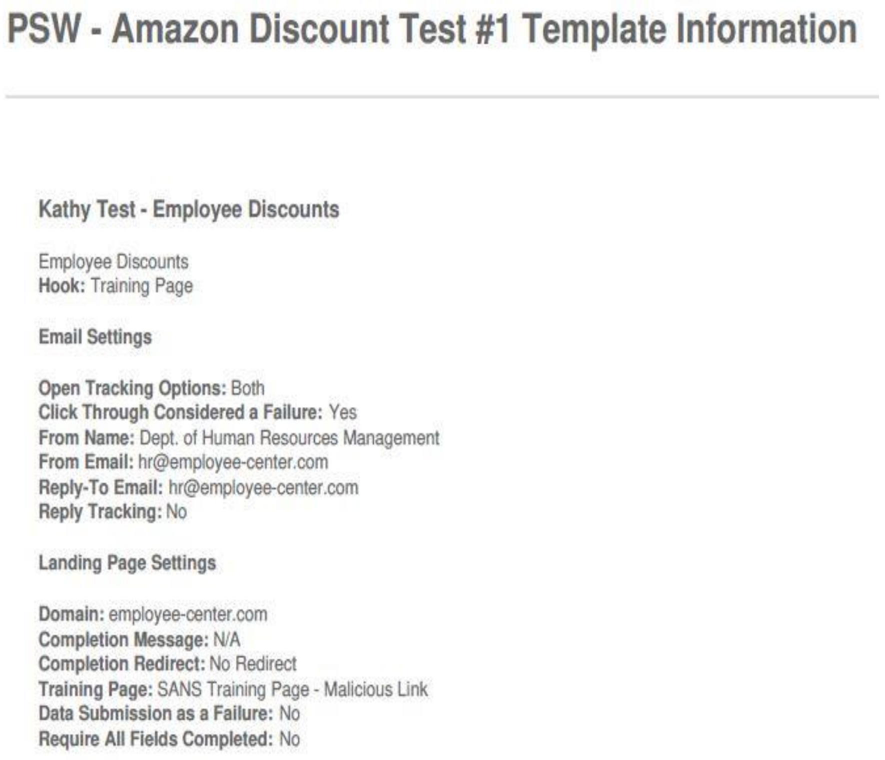
Viewed Landing Page means that the Landing Page was refreshed or navigated to by means other than a click from the phishing email. This action, along with Clicked Link in Email, makes up reported Clicks.

Worst Action is the most severe action that the target committed during the test. So, if a target opened the email, clicked on a link, attempted a download, and then opened the email again, their worst action would be attempted a download since it was the most severe action they did.

EXHAUSTIVE REPORT

INCLUDES:

- TEST SUMMARY (SAME AS FULL REPORT)
- TEMPLATE INFORMATION
- ACTION BREAKDOWN (LIMITED TO 2,500 ROWS)
- IP ADDRESS USER HIT LOCATIONS
- PHISHING TERM APPENDIX



PSW - Amazon Discount Test #1 Template Information

Kathy Test - Employee Discounts

Employee Discounts
Hook: Training Page

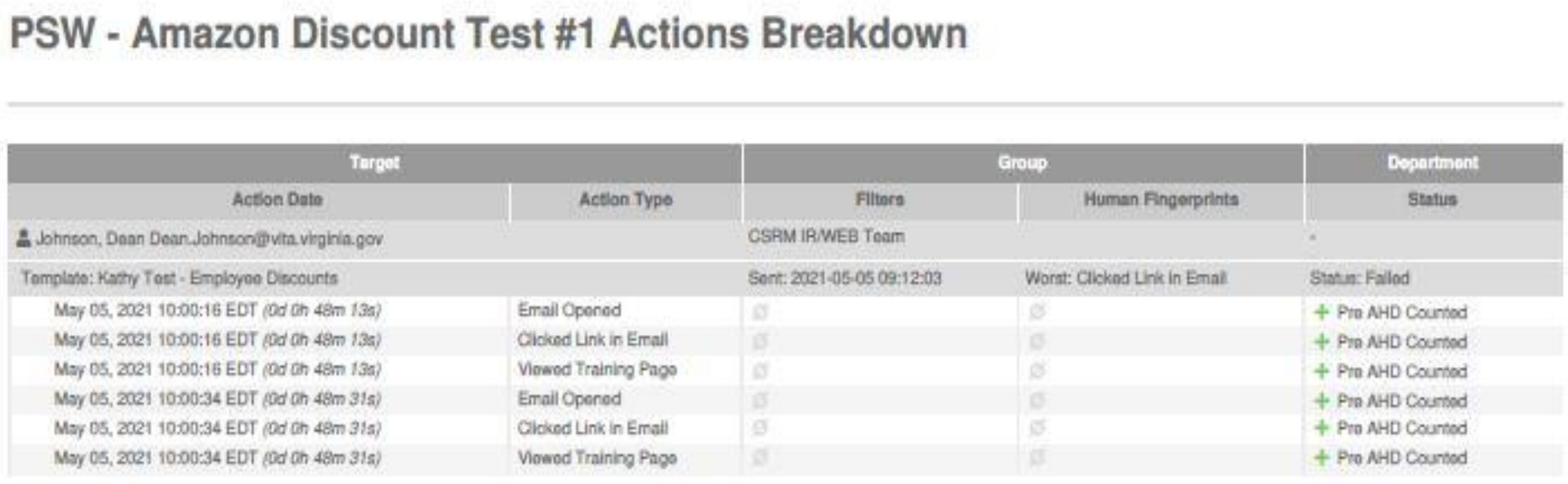
Email Settings

Open Tracking Options: Both
Click Through Considered a Failure: Yes
From Name: Dept. of Human Resources Management
From Email: hr@employee-center.com
Reply-To Email: hr@employee-center.com
Reply Tracking: No

Landing Page Settings

Domain: employee-center.com
Completion Message: N/A
Completion Redirect: No Redirect
Training Page: SANS Training Page - Malicious Link
Data Submission as a Failure: No
Require All Fields Completed: No

EXHAUSTIVE REPORT ACTION BREAKDOWN TABLE*



PSW - Amazon Discount Test #1 Actions Breakdown

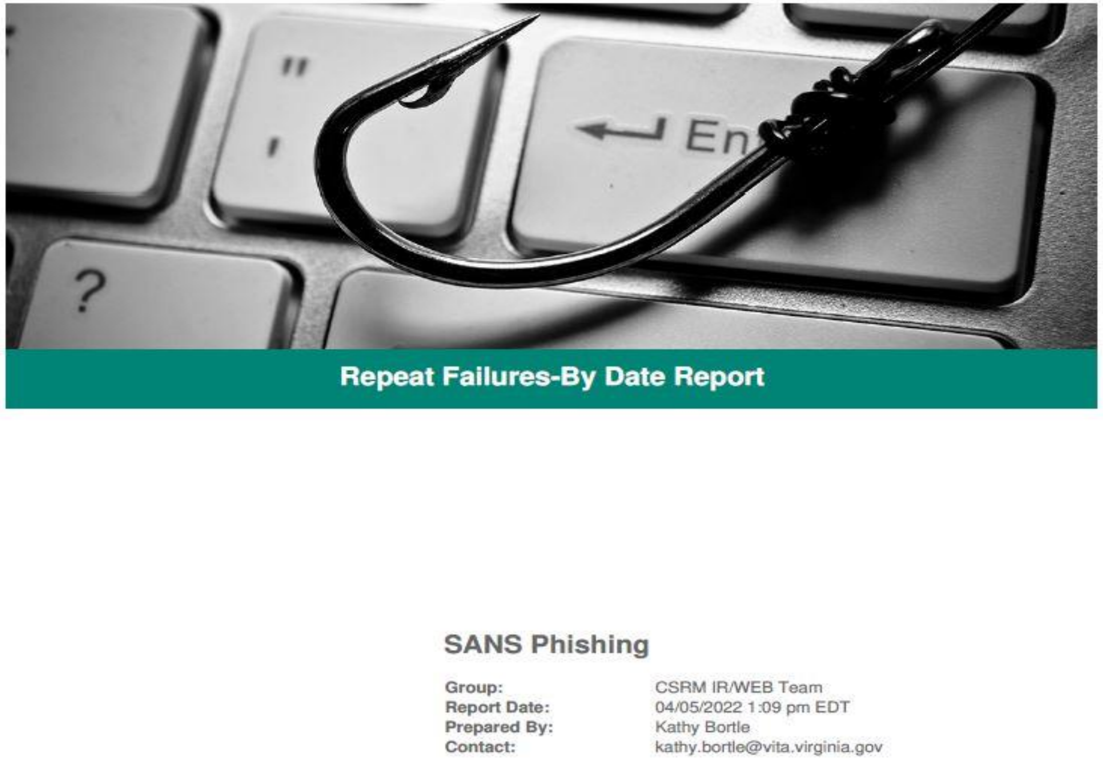
Target		Group		Department
Action Date	Action Type	Filters	Human Fingerprints	Status
Johnson, Dean Dean.Johnson@vita.virginia.gov		CSRM IR/WEB Team		-
Template: Kathy Test - Employee Discounts		Sent: 2021-05-05 09:12:03	Worst: Clicked Link in Email	Status: Failed
May 05, 2021 10:00:16 EDT *(0d 0h 48m 13s)*	Email Opened			+ Pre AHD Counted
May 05, 2021 10:00:16 EDT *(0d 0h 48m 13s)*	Clicked Link in Email			+ Pre AHD Counted
May 05, 2021 10:00:16 EDT *(0d 0h 48m 13s)*	Viewed Training Page			+ Pre AHD Counted
May 05, 2021 10:00:34 EDT *(0d 0h 48m 31s)*	Email Opened			+ Pre AHD Counted
May 05, 2021 10:00:34 EDT *(0d 0h 48m 31s)*	Clicked Link in Email			+ Pre AHD Counted
May 05, 2021 10:00:34 EDT *(0d 0h 48m 31s)*	Viewed Training Page			+ Pre AHD Counted

* Table is limited to 2500 rows

REPEAT OFFENDERS REPORT

INCLUDES:

- REPEAT OFFENDERS
- PHISHING TERM APPENDIX

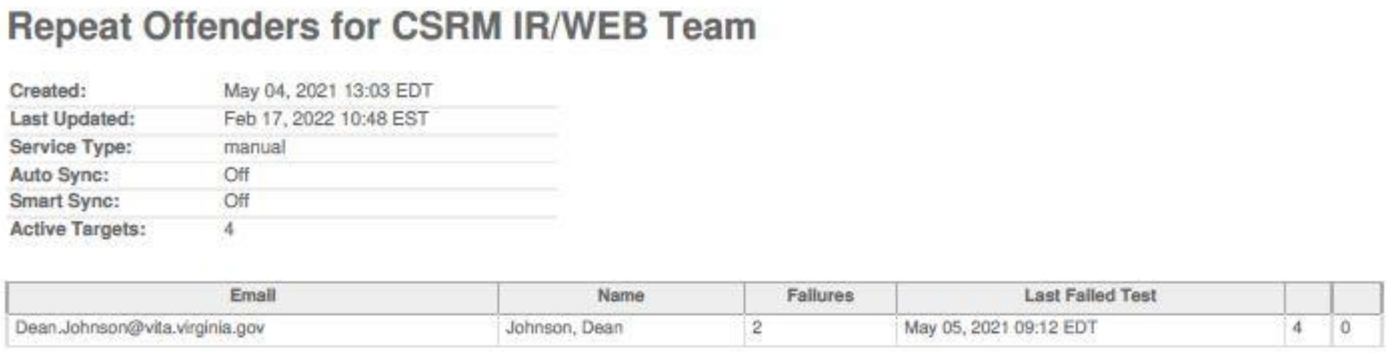


Repeat Failures-By Date Report

SANS Phishing

Group:	CSRM IR/WEB Team
Report Date:	04/05/2022 1:09 pm EDT
Prepared By:	Kathy Bortle
Contact:	kathy.bortle@vita.virginia.gov

REPEAT OFFENDERS REPORT DETAIL

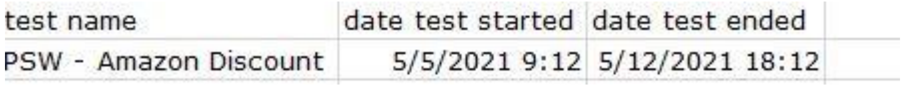


Repeat Offenders for CSRM IR/WEB Team

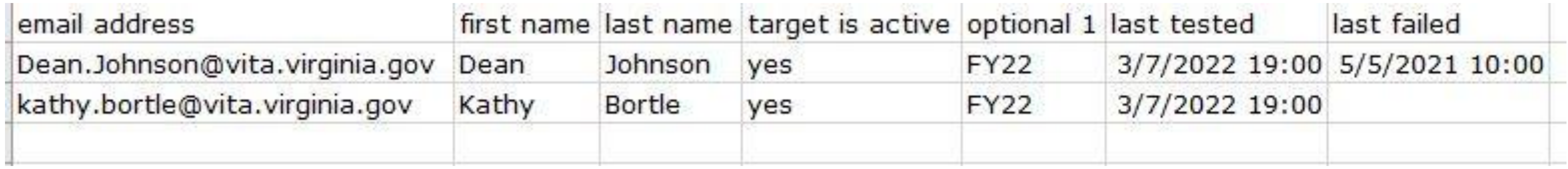
Created:	May 04, 2021 13:03 EDT
Last Updated:	Feb 17, 2022 10:48 EST
Service Type:	manual
Auto Sync:	Off
Smart Sync:	Off
Active Targets:	4

Email	Name	Failures	Last Failed Test		
Dean.Johnson@vita.virginia.gov	Johnson, Dean	2	May 05, 2021 09:12 EDT	4	0

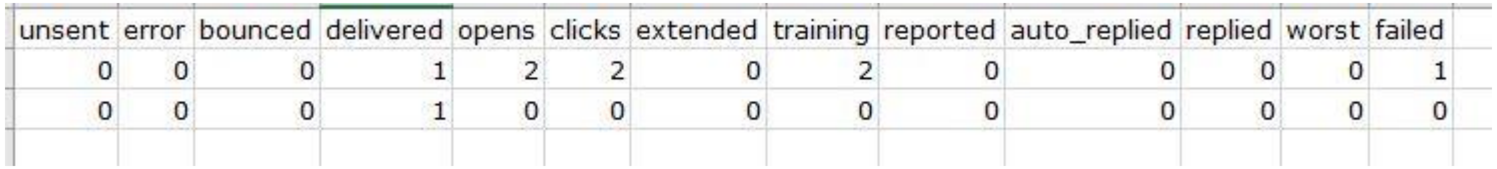
CSV FILE OF FULL RESULTS – IMPORTANT FIELDS



test name	date test started	date test ended
PSW - Amazon Discount	5/5/2021 9:12	5/12/2021 18:12



email address	first name	last name	target is active	optional 1	last tested	last failed
Dean.Johnson@vita.virginia.gov	Dean	Johnson	yes	FY22	3/7/2022 19:00	5/5/2021 10:00
kathy.bortle@vita.virginia.gov	Kathy	Bortle	yes	FY22	3/7/2022 19:00	



unsent	error	bounced	delivered	opens	clicks	extended	training	reported	auto_replied	replied	worst	failed
0	0	0	1	2	2	0	2	0	0	0	0	1
0	0	0	1	0	0	0	0	0	0	0	0	0

GOING FORWARD

QUARTERLY PHISHING CAMPAIGNS

The CSRM Threat Management Team will be performing COV Wide Phishing Campaigns once a quarter.

- The next campaign will be scheduled for December 2022.
- All details for the campaign will be shared with the ISOs, ATOS and the MSI prior to campaign start.
- All account verification will be completed prior to campaign start.
- ISOs will receive results once verified following the campaign.
- Results will include:
  - Full Report
  - Exhaustive Report if user actions are displayed
  - CSV files of all results
  - Repeat Offender reports if applicable

QUESTIONS?

CONTACT INFO

Dean Johnson, Director of Threat Management

Dean.Johnson@vita.Virginia.gov

(804) 510-7093

Kathy Bortle , Incident Response Specialist

Kathy.Borle@vita.Virginia.gov

(804) 510-7055

Jim Sturdevant, Sr., Incident Response Specialist

Jim.Sturdevant@vita.Virginia.gov

(804) 510-7062

VIRGINIA IT AGENCY

COMPLIANCE TESTING - NETWORK

Enforcement Update – October 2022

Darrell Raymond
Atos

Bill Stewart
VITA Service Owner

OCTOBER 2022

AGENDA

- Compliance Testing – Network
    - Reminder of Enforcement Plan
    - Enforcement Goals
    - Status Reporting
    - Questions

COMPLIANCE TESTING NETWORK (NAC)

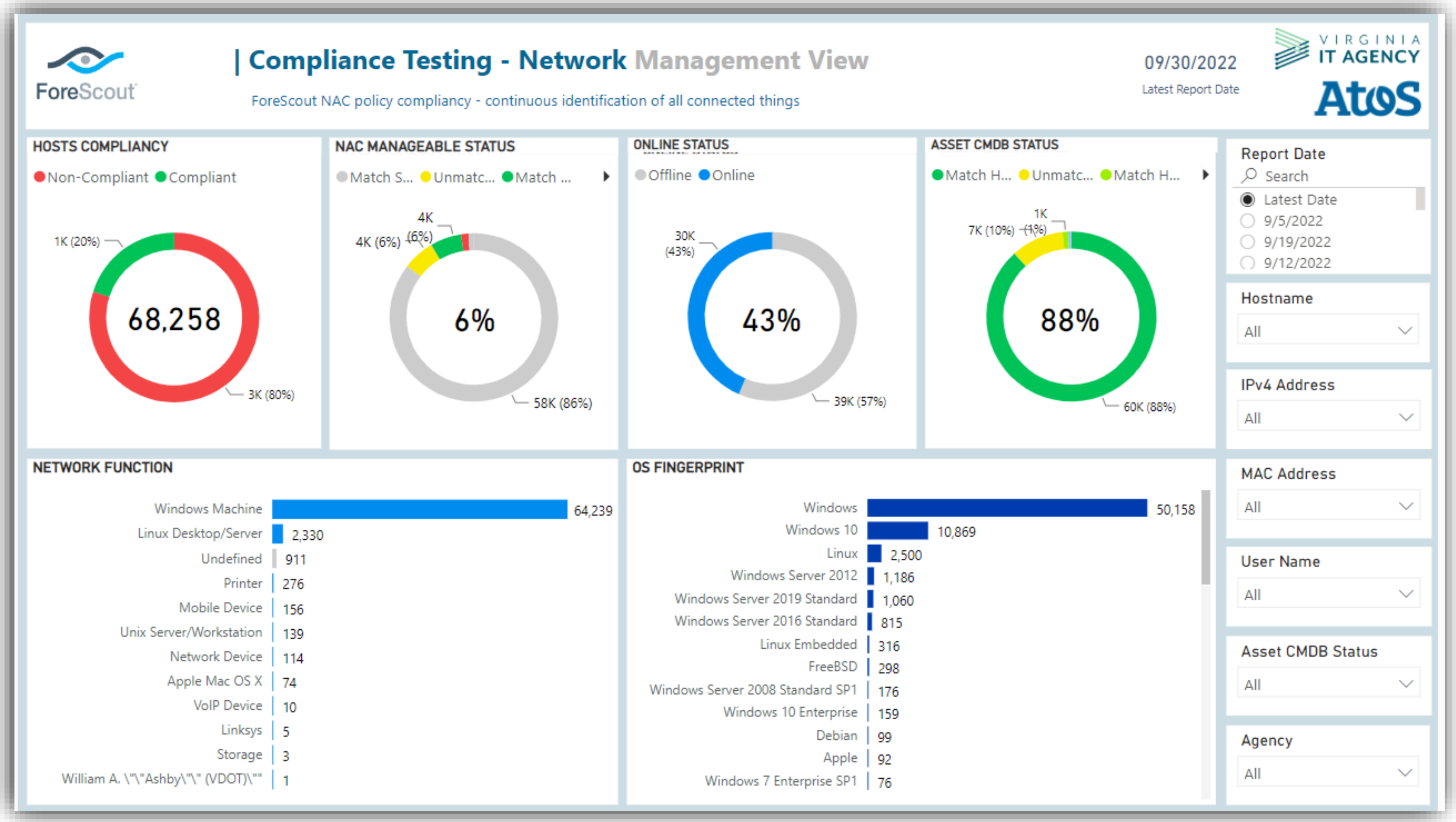
- VITA to phase in enforcement mode- Non-compliant assets will not be able to access network resources
  - Wired networks first
- Initial test will be for CMDB validation.
- All agencies should have access to reports via the security dashboard
- Agency action must be take of machines out of CMDB compliance.

ENFORCEMENT GOALS

- The end goal of Compliance Testing – Network (aka Network Access Control) is to improve the security posture of the Commonwealth by limiting access to the COV network to devices who meet defined security policies:
  - CMDB Compliance – the device is registered in the official CMDB (Agency Responsible)
  - McAfee Agent – workstations will have the McAfee Agent installed
  - Crowdstrike Agent – workstations will have the Crowdstrike Agent installed
  - Nessus Agent – workstations will have the Nessus Agent installed
  - SCCM or Landesk Agent – workstations will have the SCCM or Landesk Agent installed
- Initial enforcement will be on agency wired networks
- Devices that do not meet these requirements will be assigned to a remediation network with no access to COV resources beyond those needed to remediate the device

Information is available in the VITA Security Dashboard

- Summary data on the Management View
- Ability to filter and export on the Drilldown view
- Filters available for Agency, Asset CMDB Status, and more



| Compliance Testing - Network Management View

ForeScout NAC policy compliancy - continuous identification of all connected things

09/30/2022
Latest Report Date

Report Date
Search
● Latest Date
○ 9/5/2022
○ 9/19/2022
○ 9/12/2022

Hostname: All

IPv4 Address: All

MAC Address: All

User Name: All

Asset CMDB Status: All

Agency: All

QUESTIONS?

Thank you!

VIRGINIA IT AGENCY

RISK MANAGEMENT UPDATE

JONATHAN SMITH

Director, Risk Management

ISOAG – OCTOBER 2022

OCT 4, 2022

AGENDA

1. Risk Management Team
2. Incident Response Exercise
3. Nationwide Cybersecurity Review (NCSR)
4. Findings Remediation Effort
5. Organizational Risks and Issues (ORI's)

RISK MANAGEMENT TEAM

Introduction of Team Members

NEW TEAM MEMBER INTRODUCTION

<u>Senior Risk Analysts:</u>

- John Willinger: Started his career in IT with the DOD in 1985 at the Nevada test site, he went on to work with the DOJ working overseas with the DEA in 2000 before he Joined the commonwealth in 2005. John has worked with DBHDS as ISO and AITR, DMAS as their Risk Manager and joined VITA CSRM team in June 2022. Active CISSP since 2011.
- Marjean Adarkwa: Joined VITA in August 2022. She was formerly contracting for the USDA as a Cybersecurity Risk Analyst where she was responsible for ensuring compliance with the USDA Security Policies and Procedures, NIST, FedRAMP and DISA STIGs. Marjean has a Masters (Villanova University) and Bachelors (University at Albany-SUNY) in Accounting as well as CISA (Certified Information Systems Auditor), Open FAIR (Factor Analysis of Information Risk) and CompTIA Security+ certifications.

INCIDENT RESPONSE EXERCISE

Tabletop Exercise – Nov. 3, 2022

OVERVIEW

The COV Annual Tabletop Incident Response (IR) Exercise is an unclassified, adaptable exercise developed by the MSI/MSS for the Commonwealth of Virginia. The main purpose is to evaluate performance of the multisupplier model, promote dialogue around opportunities for continuous improvement, and identify recommendations for improvement for the COV Cybersecurity Incident Response process.

OBJECTIVES

The main objective for this exercise is to uncover strengths and weaknesses within the integrated IR process:

- Evaluate the Service Delivery capability for detecting, responding to, and recovering from simulated, realistic cybersecurity events
- Evaluate Service Delivery communication and responsiveness
- Run the event through the Service Delivery and State Agency Incident Response plans, identify opportunities for alignment, and any gaps in Service Delivery execution
- Provide recommendations for corrective action to VITA-CSRM

EXPECTED OUTCOMES

Conduct a tabletop event where coordination of multiple Suppliers and Service Delivery ensures COV information systems will successfully operate in support of the exercise scenario, and when the managed environment is under attack.

- Demonstrate successful coordination of Multiple Supplier Service Delivery
- Enhance awareness, readiness and coordination within the integrated environment
- Test capability to determine operational impacts of a cyberattack
- Test and exercise participant’s incident response playbooks, incident analysis, incident response plans and incident reporting procedures
- Demonstrate compliance with MSI Security Incident Management Process and VITA Incident Response Playbooks
- Identify Enterprise-wide opportunities for improvement
- Further integration of multi sourcing program between MSI, VITA-CSRM, Service Towers, and the Agencies

EVENT INFORMATION

- When:
  - Exercise: Thursday, Nov 3rd, 2022, from 8am-1pm
  - Hotwash: Friday, Nov 4th, 2022, from 11am-12pm
- Who:
  - Hosted by MSI SIRT team, ATOS Security, and VITA CSRM
  - Participants include representatives from each agency and service tower
- Where:
  - Zoom Meeting will be hosted for coordination
  - Participation from your usual workspaces

EVENT INFORMATION (CONT'D)

How to participate:

An email has been sent out weekly since 9/14 to last year's participants, you can respond to one of these emails stating you would like to participate (if your agency hasn't done so already)

If you haven't received the weekly notification, please send an email to MSI-Security-Operations@saic.com stating that your agency/tower would like to participate in this year's event

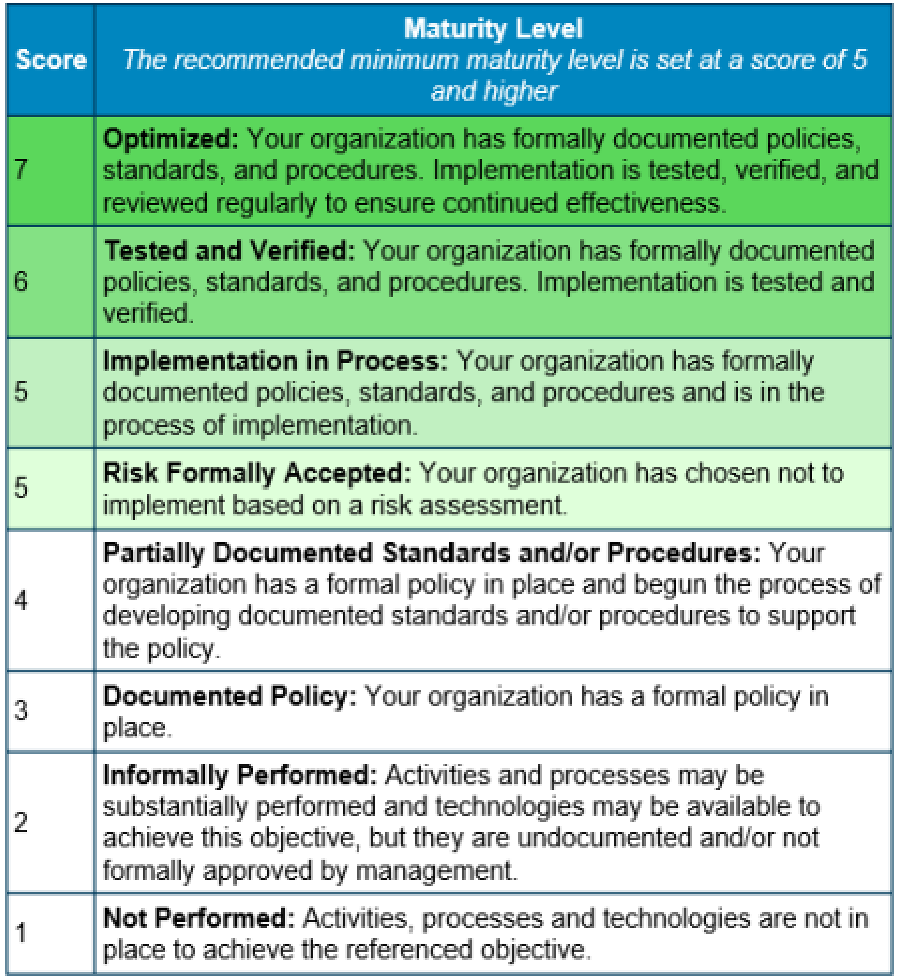
Cut-off date for registration: Thursday, Oct 27th, 2022

NATIONWIDE CYBERSECURITY REVIEW

Oct. 1, 2022 – Feb. 28, 2023

OVERVIEW

The NCSR is a no-cost, anonymous, maturity based, annual self-assessment. All states (and agencies), local governments (and departments), tribal nations, and territorial (SLTT) governments are encouraged to participate. It is designed to measure gaps and capabilities of SLTT governments' cybersecurity programs and is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).



Score	**Maturity Level** *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 tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and 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.

BENEFITS

- Receive metrics specific to your organization to identify gaps and develop a benchmark to gauge year-to-year progress, as well as anonymously measure your results against your peers.
- Attain reporting and resources that can help you prioritize next steps towards desired cybersecurity improvement. For HIPAA compliant agencies, translate your NCSR scores to the HIPAA Security Rule scores of an automatic self-assessment tool.
- Gain access to a repository of informative references, such as NIST 800-53, COBIT and the CIS Controls that can assist in managing cybersecurity risk.
- Fulfill the NCSR assessment requirement for the Homeland Security Grant Program (HSGP). Additional information located here: https://www.fema.gov/homeland-security-grant-program.

REGISTRATION

- CSRM is working with CIS to enroll Commonwealth Executive Branch and Independent agencies
- You should be receiving registration confirmation emails soon
- Login URL: https://cis.my.logicmanager.com/login
- Users will be need to select “Reset Password” to complete the registration process

FINDINGS REMEDIATIONS

Audit and Risk findings in Archer

OPEN RISK AND AUDIT FINDINGS

Risk Findings

- 1965 Open risk findings
  - 1643 (84%) of the open risk findings are more than 1 year old
  - *1140 (69%) of agency risk findings more than a year old with a status of "Not started"*

Audit Findings

- 1942 Open audit findings
  - 1356 (70%) open audit findings more than 1 year old
  - *505 (37%) of agency audit findings more than a year old with a status of "Not started"*

WHAT CAN WE DO?

Review and update open findings

- Verify continued validity
- Has a finding remediation response been entered into Archer?
- Is the status for the finding accurate (not started, underway, awaiting review, etc)?
- Have quarterly updates been submitted and updated in Archer?

Having difficulties within Archer? Contact you CSRM analyst or CommonwealthSecurity@vita.virginia.gov

ORGANIZATIONAL RISKS & ISSUES

ORI’s in Archer

WHAT IS AN ORI?

Organizational risk and issue findings identified within the enterprise or agency environments that will require business requirements to address them within IT Strategic Plans

- Program risks/issues
    - Agency audit program
    - Agency security/risk program
    - Vulnerability management program
- End-of-Life software/hardware
    - Enterprise Architecture
- Shadow IT identified
- Other

WHAT DO I DO WITH AN ORI FINDING

ORI findings shall be treated as other findings in Archer

- Maintain status of the finding (not started, underway, submitted for closure, etc.)
- Remediation plan and remediation activities maintained and updated in Archer
- Submit/enter quarterly updates to the remediation efforts until closure

Note: During the IT Strategic Planning Process, open ORI's will require agencies to address the risk or issue within their IT strategic plan with the creation of a business requirement for technology

QUESTIONS?

Please reach out to the Risk Management Team if you have any additional questions:

Jonathan Smith, Dir Risk Management – jonathan.m.smith@vita.virginia.gov

John Willinger, Sr. Risk Analyst – john.willinger@vita.virginia.gov

Marjean Adarkwa, Sr. Risk Analyst - marjean.adarkwa@vita.virginia.gov

Andrew Wirz, Archer Sys Admin - andrew.wirz@vita.virginia.gov

VIRGINIA IT AGENCY

CORRECTIVE ACTION PLANNING

Mark McCreary, CISA, CISSP, CISM

Centralized IT Security Audit Service
Director

CORRECTIVE ACTION PLANNING

- IT Security Audit Standard
- Reporting Audit Results
- Corrective Action Plan Template/Elements
- Security Exceptions
- Follow-up Activities

IT SECURITY AUDIT STANDARD (SEC502)

- Current version is 502.4
- Found on VITA’s website:

  https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

- Requires IT Security Audits of each Sensitive System every three-years.
- Audits measure compliance with the applicable requirements of IT Security Standard 501.

IT SECURITY AUDIT REPORTS

All IT security audits must follow an established auditing framework. In general, internal auditors will follow the Institute of Internal Auditors (IIA) framework and external auditors will follow Generally Accepted Government Auditing Standards (GAGAS).

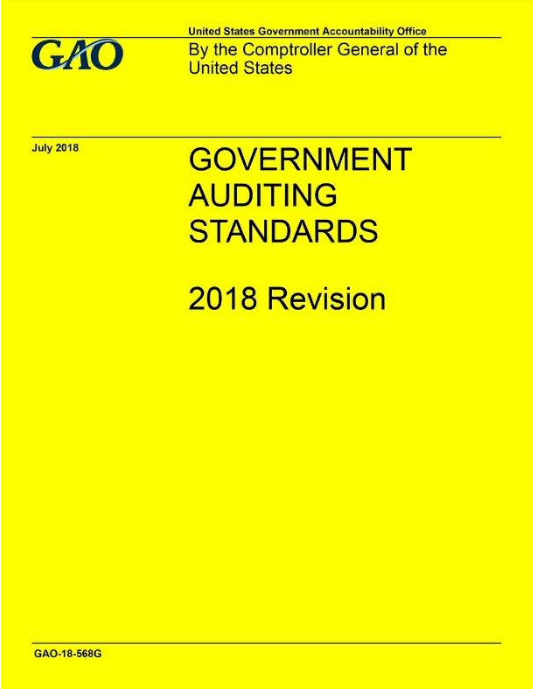
INTERNATIONAL PROFESSIONAL PRACTICES FRAMEWORK (IPPF)®

Mission of Internal Audit | Core Principles | Definition of Internal Auditing | Code of Ethics | Standards | Implementation Guidance | Supplemental Guidance

2017 EDITION

The Institute of Internal Auditors Global

The official audit report submitted needs to include an attestation as to the audit standard used (i.e. yellow or red book or other approved framework).



GAO

United States Government Accountability Office
By the Comptroller General of the United States

July 2018

GOVERNMENT AUDITING STANDARDS

2018 Revision

GAO-18-568G

REPORTING AUDIT RESULTS

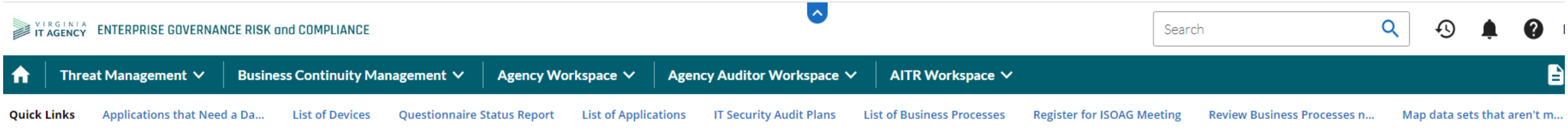
The Agency Head or designee shall submit to the CISO the following information:

A record of all completed IT Security Audits conducted by or on behalf of the Agency, including the official audit report (in accordance with auditing standards), all findings, and whether the Agency concurs or does not concur with each. IT Security Audits submitted to VITA must be reflected in the IT Security Audit Plan.

CORRECTIVE ACTION PLAN TEMPLATE

Agencies are required to submit Corrective Action Plans using the eGRC (Archer) system using the elements from the Audit Remediation Plan template found at:

www.vita.virginia.gov/it-governance/itrm-policies-standards/#securityPSGs


VIRGINIA IT AGENCY
ENTERPRISE GOVERNANCE RISK and COMPLIANCE
Search
Threat Management
Business Continuity Management
Agency Workspace
Agency Auditor Workspace
AITR Workspace
Quick Links
Applications that Need a Da...
List of Devices
Questionnaire Status Report
List of Applications
IT Security Audit Plans
List of Business Processes
Register for ISOAG Meeting
Review Business Processes n...
Map data sets that aren't m...

INITIAL CORRECTIVE ACTION PLAN ELEMENTS

Develop Corrective Action Plans with the following elements:

1. Finding Name/Title
2. Finding Description
3. Affected Applications
4. Policy Section
5. Magnitude of Impact
6. Probability of Occurrence
7. Submit Date
8. Remediation Overview
9. Estimated Completion Date
10. Responsible Person
11. Status
12. Exception on File (Yes/No)

MAGNITUDE OF IMPACT

Magnitude of Impact	Impact Definition
High	Occurrence of the risk: (1) May result in human death or serious injury. (2) May result in the loss of major COV tangible assets, resources, or sensitive data. (3) May significantly harm, or impede the COV's mission, reputation, or interest.
Moderate	Occurrence of the risk: (1) May result in human injury. (2) May result in the costly loss of COV tangible assets or resources. (3) May violate, harm, or impede the COV's mission, reputation, or interest.
Low	Occurrence of the risk: (1) May result in the loss of some tangible COV assets or resources. (2) May noticeably affect the COV's mission, reputation, or interest.

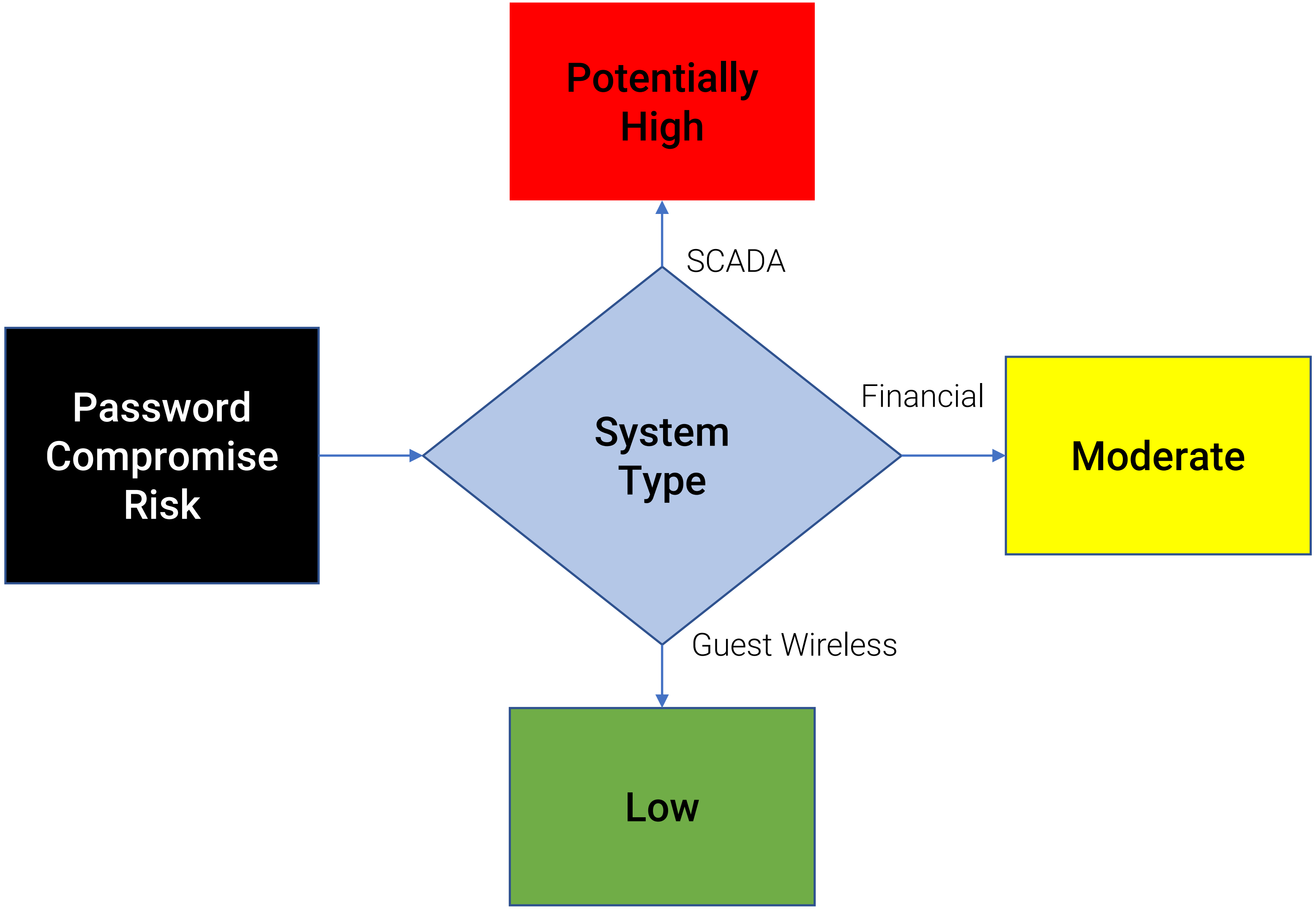
MAGNITUDE OF IMPACT

Magnitude of Impact

=

HIGH

MAGNITUDE OF IMPACT



PROBABILITY OF OCCURRENCE

Effectiveness of Controls	Probability of Occurrence (Natural or Environmental Threats) or Threat Motivation and Capability (Human Threats)		
	Low	Moderate	High
Low	Moderate	High	High
Moderate	Low	Moderate	High
High	Low	Low	Moderate

Values may change based on control effectiveness.

PROBABILITY OF OCCURRENCE

“NASA knows of no asteroid or comet currently on a collision course with Earth, so the probability of a major collision is quite small. In fact, as best as we can tell, no large object is likely to strike the Earth any time in the next several hundred years.”

EFFECTIVENESS OF CONTROLS

After 10 months flying in space, NASA's Double Asteroid Redirection Test (DART) – the world's first planetary defense technology demonstration – successfully impacted its asteroid target, the agency's first attempt to move an asteroid in space.

PROBABILITY OF OCCURRENCE

	Effectiveness Of Controls	Probability of Occurrence (Natural or Environmental Threats) or Threat Motivation and Capability (Human Threats)		
		Low	Moderate	High
Simple Passwords	Low	Moderate	High	High
Complex Passwords	Moderate	Low	Moderate	High
Multi-Factor Auth	High	Low	Low	Moderate

OVERALL FINDING RISK

Probability of Occurrence	Magnitude of Impact		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate
Low	Low	Low	Low

Overall Finding Risk = *Criticality* field in Archer

Helps prioritize findings based on risk.

- Remediation Overview - Documents the step(s) necessary to achieve compliance and/or mitigate risk.
- Estimated completion date
- Responsible Person
- Status

LET'S MAKE A DEAL

SECURITY EXCEPTIONS

- Security Exception on File (Y/N)

- Agencies should request Security Exceptions once they become aware of a control deficiency (awareness is not limited to Audit Findings).

- Once control deficiencies are identified, Corrective Action Plans exceeding 90-days require a Security Exception.

FOLLOW-UP ACTIVITIES

Submit Corrective Action Plan status quarterly, *within 30 days after the end of each quarter*, until all corrective actions are completed.

All Corrective Action Plans and Quarterly Updates submitted must have Agency Head approval and any modification to a Corrective Action Plan must be reported.

QUESTIONS

Contact information

Email: Mark.McCreary@vita.virginia.gov

Phone: (804) 510-7095

UPCOMING EVENTS

VASCAN

VASCAN 2022 (*Securing the Transformation*)
Hosted by VCU Technology Services

When: Thursday, **October 6th and Friday, October 7th**
Where: Delta Hotel Richmond Downtown, 555 E Canal St. Richmond, VA - parking in the hotel garage is INCLUDED for Thursday & Friday.
Contact: Hope Adams, VASCAN Conference Coordinator, adamsh@vcu.edu
Website: vascan.vcu.edu

Registration Link: https://wm.irisregistration.com/Site/VASCAN22ATTEND
Registration Costs:
- Conference Only = $150.00
- Conference + Training = $400.00

Conference cost includes all sessions, breakfast, lunch, breaks, parking and evening networking event. CPEs will be available for sessions.

Training Details:
Tactical Windows Forensics, Presented By TrustedSec
Length: 8 hours - Friday, October 7, 2022 (8am - 5pm)

NOV 5TH ISOAG MEETING

SPEAKERS:

DAVID RAYMOND / VA CYBER RANGE

PATRICK DOHERTY & TRACEY NORRIS / CROWDSTRIKE

CHRIS MCCALL / EXTRAHOP

ERIC HUNTER / VITA

VIRGINIA IT AGENCY

MEETING ADJOURNED