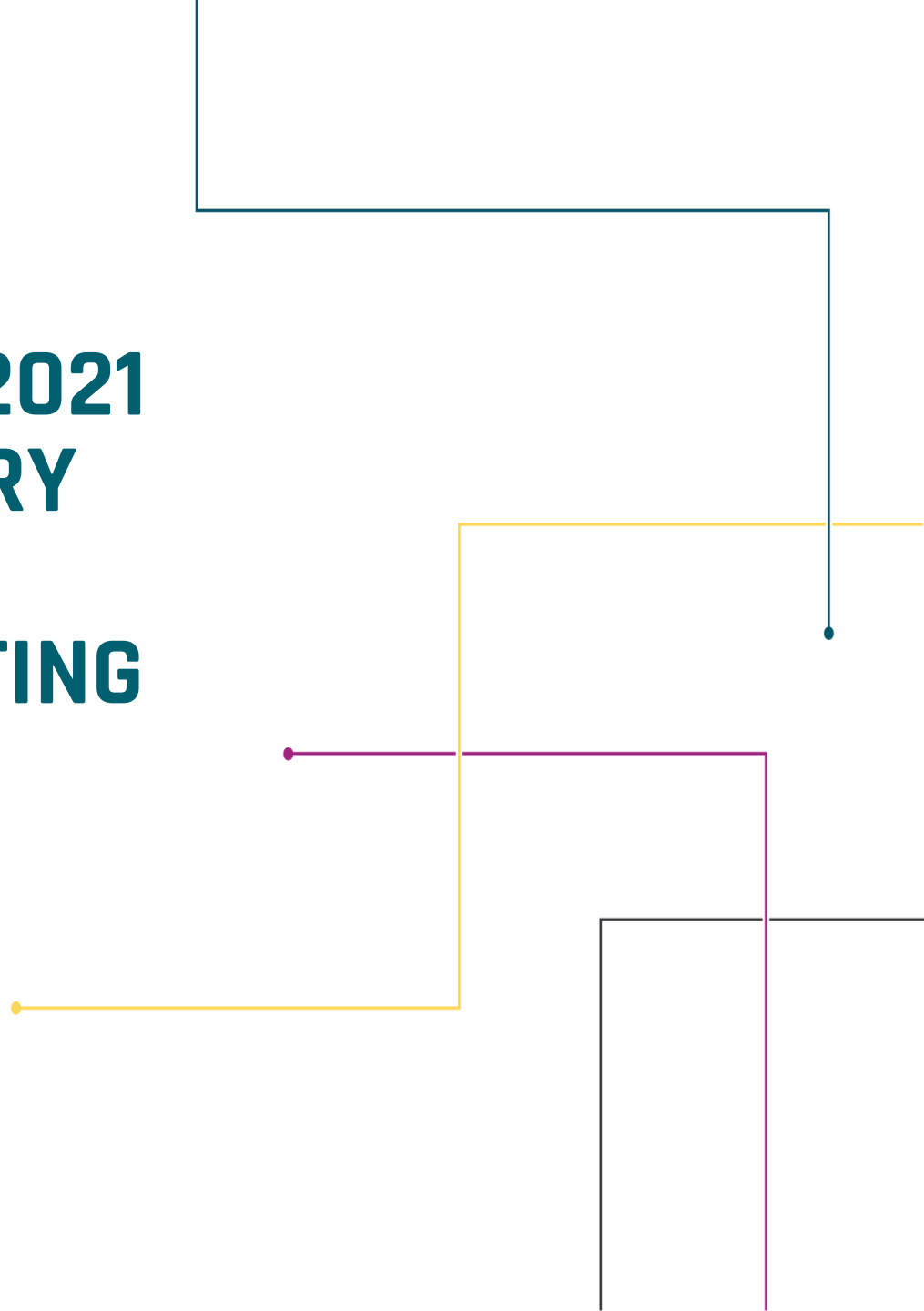




OCTOBER 6, 2021 MANDATORY ISOAG MEETING



AGENDA



- **WELCOME / INTRODUCTION: MIKE WATSON**
- **VITA/CSRM PHISHING SERVICE: KATHY BORTLE/JIM STURDEVANT**
- **RISK MANAGEMENT UPDATE: JON SMITH**
- **NCSR UPDATE: TYLER SCARLOTTA/CI SECURITY MSISAC**
- **CONTINGENCY PLANNING TABLETOP EXERCISE: ZACH WILTON/SAIC**
- **ARCHER SECURITY EXCEPTION PROCESS: LOURDES LUNSFORD**
- **CENTRALIZED AUDIT SERVICES UPDATE: MARK MCCREARY**
- **SECURITY AWARENESS UPDATE/CYBERSECURITY AWARENESS MONTH: TINA GAINES**
- **IT SECURITY GOVERNANCE UPDATE: ED MILLER**
- **UPCOMING EVENTS**
- **ADJOURN**



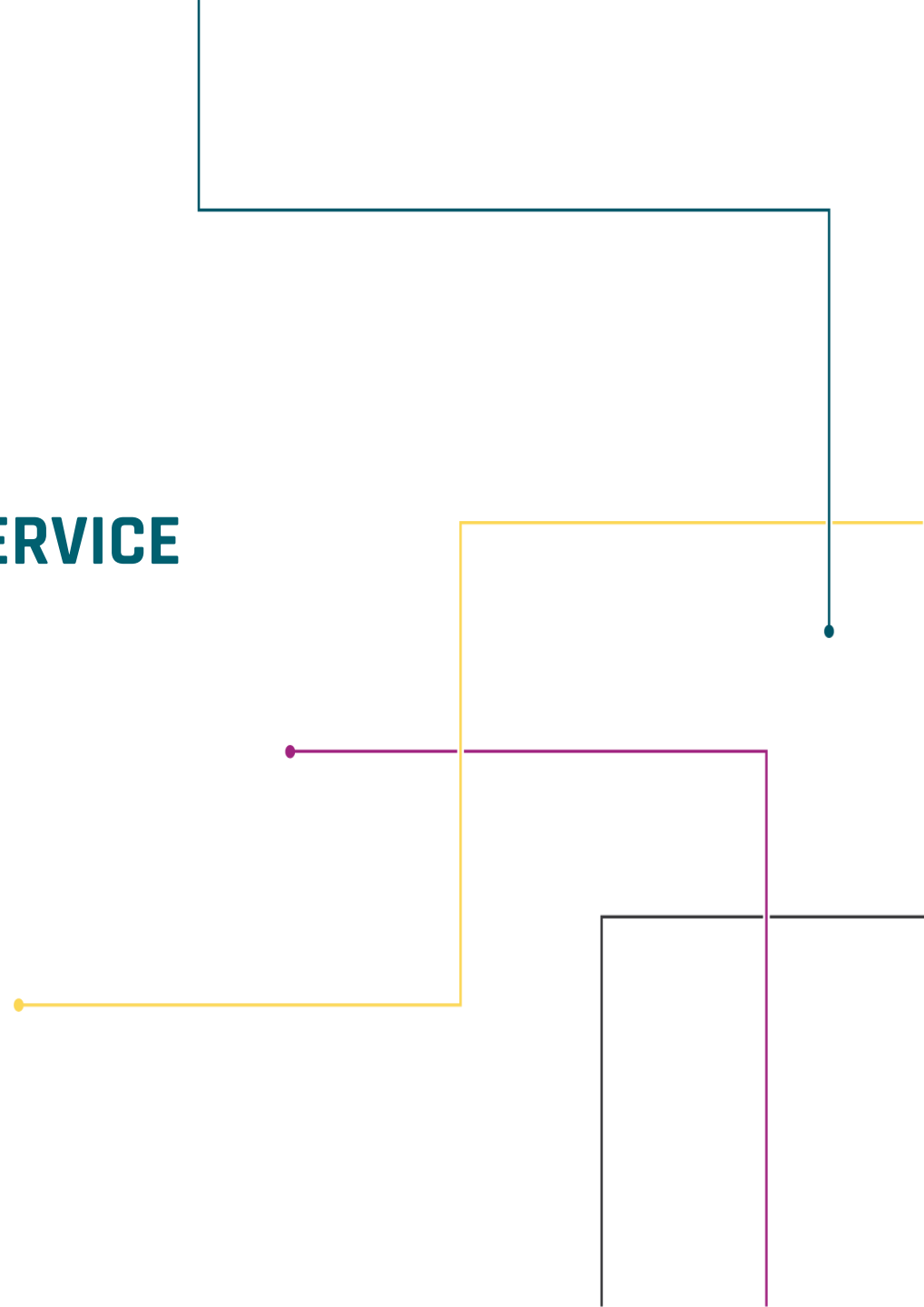
VITA/CSRM PHISHING SERVICE

KATHY BORTLE & JAMES STURDEVANT, SR.

Incident Response Specialists

VITA/CSRM /THREAT MANAGEMENT TEAM

OCTOBER 6, 2021



BACKGROUND



BACKGROUND

- VITA started hosting phishing campaigns to assist agencies with training their users on how to recognize a phishing message in a safe controlled environment.
- At the time, VITA had purchased an add-on option to Metasploit to handle the campaigns. While the tool was very flexible, the reporting was rather lacking. If multiple agencies were phished at the same time, all results would have to be manually reviewed and correlated to provide user data to each agency. This was a very time consuming task and limited the number of campaigns that could be done in a year.
- Due to the increase in Ransomware attacks, the Virginia Legislature directed VITA to perform phishing campaigns across the Commonwealth and provided a budget for the tools for six years.
- VITA evaluated multiple phishing tools and decided to purchase the SANS phishing tool. It is much easier to use and allows flexibility in reporting results.

MEETING SECURITY REQUIREMENTS



REQUIREMENTS

- VITA has 33,000 phishing licenses a year to phish the Commonwealth's approximate 65,000 users.
- In order for agencies to maintain compliance with SEC 525, the VITA/CSRM/threat management team will phish half of the agency each year.
- Example: If an agency has 500 users - they would be able to phish 250 users years 1, 3 and 5 and the other 250 users years 2,4, and 6.
- Agencies will need to provide VITA/CSRM with the names of employees that they want to phish that year. Once an employee has been assigned a phishing license, they can be phished multiple times during the year.
- At the end of the two year cycle, all employees should have been phished at least once.

HOW TO GET STARTED

The background is a solid teal color. On the right side, there are several yellow lines that form a stepped, staircase-like pattern. These lines start from the top right and move downwards and to the left in a series of horizontal and vertical segments. Some of these segments end with a small yellow dot.

STEPS TO CREATE A PHISHING CAMPAIGN

1. Send an email with your contact information to VITA security requesting a phishing campaign

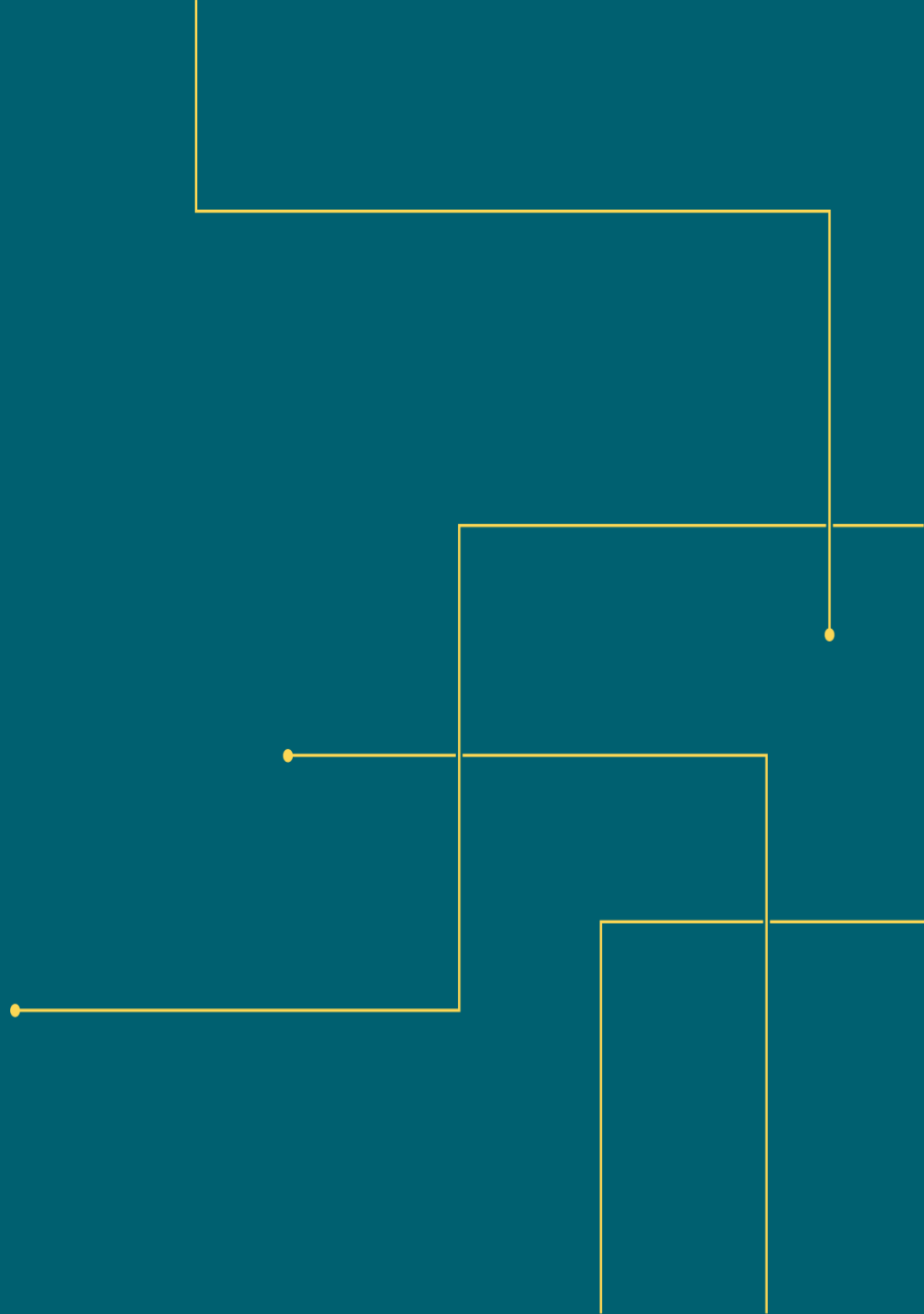
Email: CommonwealthSecurity@vita.virginia.gov

2. VITA/CSRM/threat management team will reach out to you to discuss developing the campaign.
3. The first step will be to create a template for the campaign. You will discuss what you want the phishing message to look like – type of industry, recent news topics, has an attachment, has links for filling out forms, etc.
4. The team will take this information and develop a template for the campaign.
5. Once the template is created, they will send sample phish messages to you so that you can see what it will look like and how it will work.
6. After a final version of the template is agreed, we are ready to setup the campaign and schedule it.

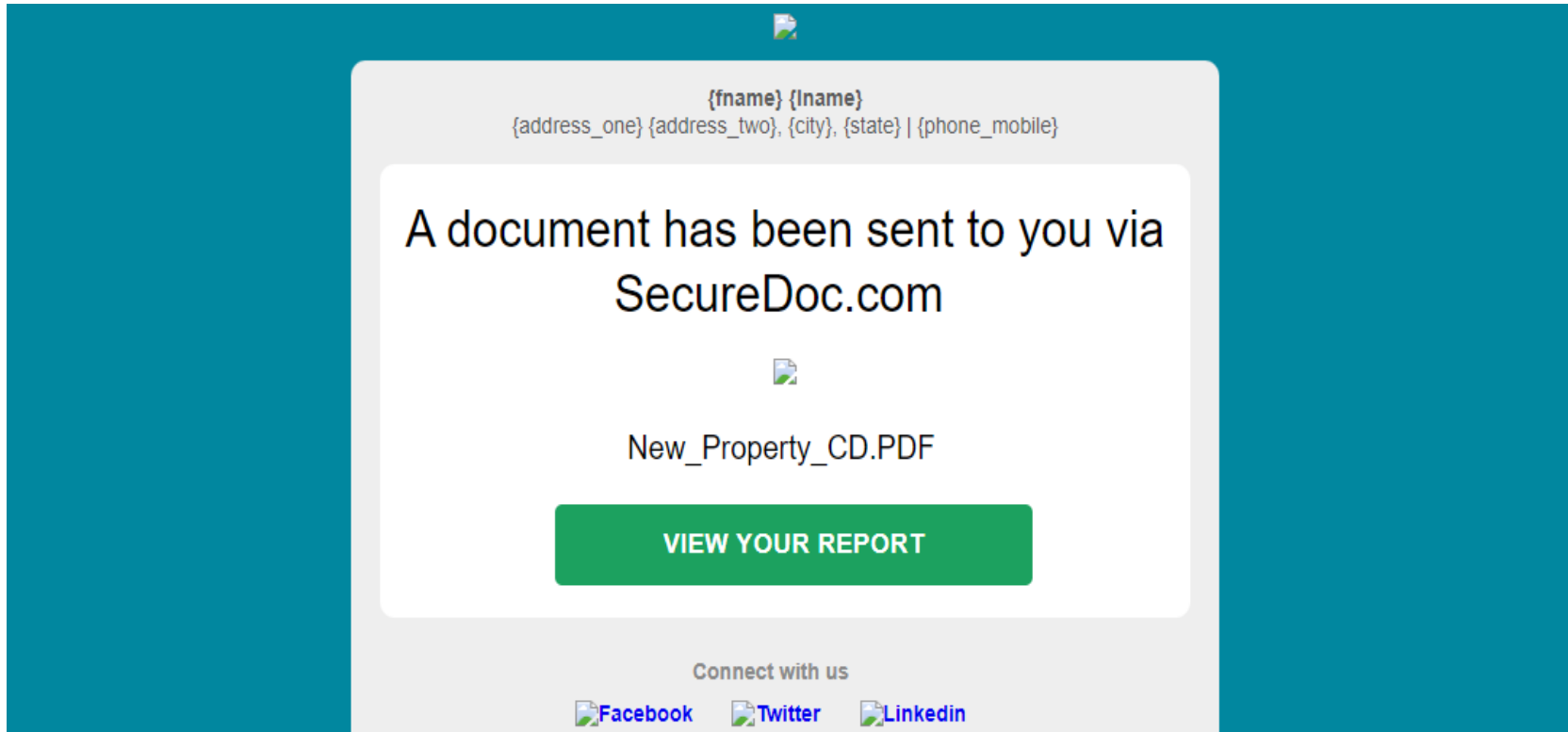
STEPS TO CREATE A PHISHING CAMPAIGN (CONT.)

7. To setup the campaign, the team will need to know the following:
 - First & last names of the users to be phished
 - Email addresses of the users to be phished
 - How long do you want the campaign to run (max is normally three days)
 - When do you want the campaign to start (date/time)
 - When do you want the campaign to run (hours, days, etc.)
8. The threat management team will use this information to setup the campaign and let you know when it is ready.
9. The campaign will be launched at the agreed date/time.
10. When the campaign is finished, the threat management team will pull the campaign results and provide it to you for review.
11. If you wish to re-test your users or run additional campaign, please return to step one of the process by sending another email to VITA security.

EXAMPLES



INFECTED ATTACHMENT

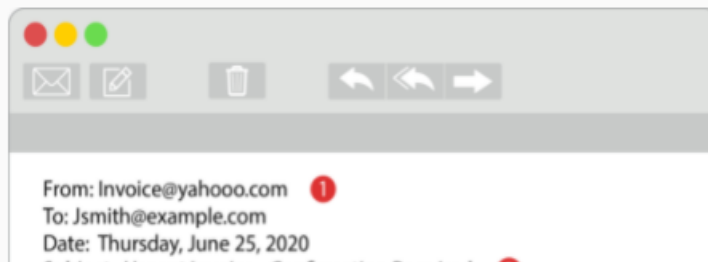


INFECTED ATTACHMENT

Whoops... You just got phished!

You are receiving this training page because you clicked on a link during an *authorized* phishing simulation. Infected attachments are a primary way an adversary attempts to make you fall victim to an attack.

We're here to help you recognize the signs of a phishing attack



- 1 Appears to be an official email but comes from a personal email account
- 2 Strong sense of urgency
- 3 Generic greeting
- 4 Unexpected attachment

MALICIOUS LINKS

{fname},

We attempted to update or patch your laptop to Office 365 but encountered several errors. In order to resolve these corporate risk issues, we need you to perform a few diagnostic checks on your system. You can find instructions to do this by downloading the PDF.

We require you to do this by the end of the day so the upgrade can run smoothly overnight. NOTE: If you experience trouble with the attachment, [click here](#).

Kind Regards,

Application Admin

IT Department

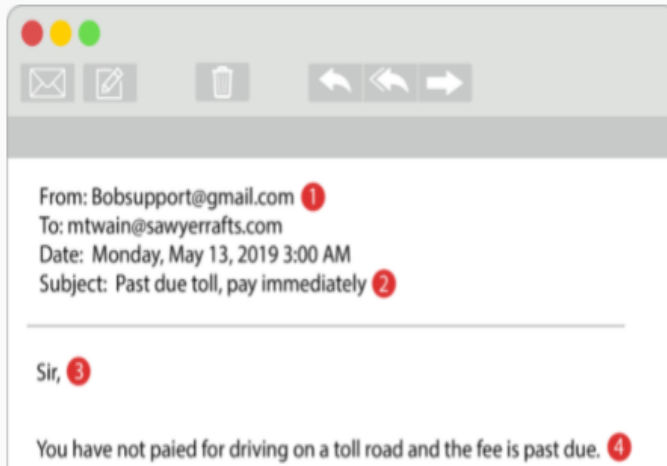


MALICIOUS LINKS

You are receiving this training page because you clicked on a link during an *authorized* phishing simulation.

Malicious links are a primary way an adversary attempts to make you fall victim to an attack.

We're here to help you recognize the signs of a phishing attack



- 1 It appears to come from a personal email account
- 2 The subject of the email has a strong sense of urgency or even curiosity
- 3 It has a generic greeting, such as "Sir," "Miss," or "Valued customer"
- 4 It has grammatical errors
- 5 Words or phrases have a strong sense of urgency, pressuring you into quick decisions
- 6 Includes a link or domain you do not recognize or are

CREDENTIAL HARVESTING - LOGIN REQUEST



Archive of Google data requested

You're getting this email because there's been a request to create an archive of your Google data.

If you didn't make this request, someone may be trying to access your Google account. Check recent activity in your account and take steps to secure it.

Requests can be scheduled in advance.

[Check activity](#)

CREDENTIAL HARVESTING - LOGIN FORM



One Account. All of Google.

Sign in with your Google Account

A light gray rectangular box contains a user profile icon (a gray circle with a person silhouette), an "Email:" label, a white text input field, and a blue "Next" button.

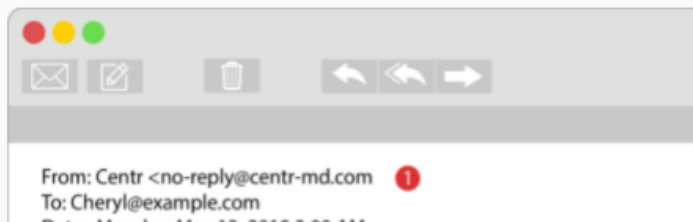
CREDENTIAL HARVESTING

Whoops... You just got phished!

You are receiving this training page because you clicked on and subsequently entered data during an *authorized* phishing simulation.

Credential harvesting is a method that adversaries use to trick you into giving them your login and password.

We're here to help you recognize the signs of a phishing attack



- 1 Do you know the sender?
- 2 Do you have an account with this organization?
- 3 Sense of urgency
- 4 When hovering over the link, does the link or domain look familiar?

CREDENTIAL HARVESTING – REPLY TO

To {fname} {lname}:

Please be advised that, effective immediately, we have terminated your corporate VPN access due to repeated violation of our Acceptable Use Policy. We regret having to take this action, but after numerous warnings regarding inappropriate use and access from unauthorized locations and devices, we have seen no change in your usage pattern. The manner in which you use our VPN service jeopardizes {company}'s reputation and security as safety of our customers' information.

If you believe that you received this message in error or are not responsible for inappropriate use, please reply to this email with your {company} VPN username and password for further investigation.

Sincerely,

{company} IT Department

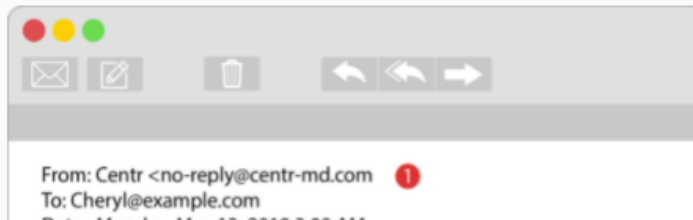
CREDENTIAL HARVESTING

Whoops... You just got phished!

You are receiving this training page because you clicked on and subsequently entered data during an *authorized* phishing simulation.

Credential harvesting is a method that adversaries use to trick you into giving them your login and password.

We're here to help you recognize the signs of a phishing attack



- 1 Do you know the sender?
- 2 Do you have an account with this organization?
- 3 Sense of urgency
- 4 When hovering over the link, does the link or domain look familiar?

EXAMPLE REPORTS



REPORTING RESULTS

There are multiple types of reports that can be pulled once a phishing campaign has been completed. These include:

- Executive report (test summary)
- Failed only report
- Actions report
- Exhaustive report (includes details of template used)
- Repeat offenders report – this report will be available after the user participates in multiple campaigns

All reports include a phishing term appendix

EXECUTIVE REPORT

INCLUDES:

- TEST SUMMARY
- PHISHING TERM APPENDIX

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: The Authorized
Group: CS/PM SV/WEB Team
Targets: 3
Failed: 2 (66.7%)

Net Reporter Score
NRS: -66.7

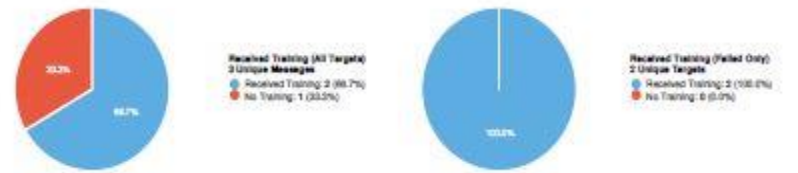
Total Targets Trained: 3
 Reported Only: 0
 Failed Only: 2
 Reported & Failed: 0
 No Response: 1

3 DELIVERED
2 OPENED
2 CLICKED
0 DATA EXTENDED
2 RECEIVED TRAINING
0 REPORTED PHISHING

This is how many test emails were delivered.
 This is how many test emails were opened.
 This is how many test emails had a click.
 This is how many test emails had something worse than a click.
 This is how many test emails had training pages viewed.
 This is how many test emails were reported.



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 (i.e., 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.



EXECUTIVE REPORT

INCLUDES:

- TEST SUMMARY
- 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.

FAILED ONLY REPORT

INCLUDES:

- **TEST SUMMARY (FILTERED)**
- **ACTION BREAKDOWN (FAILED TARGETS ONLY)**
- **IP ADDRESS USER HIT LOCATIONS (FILTERED)**
- **PHISHING TERM APPENDIX**

PSW - Amazon Discount Test #1 Actions Breakdown (Failed Targets Only)

Target		Group		Department	
Action Date	Phish Time	Action Type	IP Address	Browser	OS
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	Clicked Link in Email	IP: 73.40.64.100	Google Chrome	Mac
May 05, 2021 10:00:16 EDT	0d 0h 48m 13s	Viewed Training Page	IP: 73.40.64.100	Google Chrome	Mac
May 05, 2021 10:00:34 EDT	0d 0h 48m 31s	Clicked Link in Email	IP: 63.117.215.9	Google Chrome	Windows
May 05, 2021 10:00:34 EDT	0d 0h 48m 31s	Viewed Training Page	IP: 63.117.215.9	Google Chrome	Windows
Lindsay, Kyle kyle.lindsay@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 09:40:02 EDT	0d 0h 27m 59s	Clicked Link in Email	IP: 73.40.64.100	Google Chrome	Mac
May 05, 2021 09:40:02 EDT	0d 0h 27m 59s	Viewed Training Page	IP: 73.40.64.100	Google Chrome	Mac

ACTION BREAKDOWN REPORT

INCLUDES:

- ACTION BREAKDOWN
- IP ADDRESS USER HIT LOCATIONS
- PHISHING TERM APPENDIX

PSW - Amazon Discount Test #1 Actions Breakdown

Target		Group		Department	
Action Date	Phish Time	Action Type	IP Address	Browser	OS
Johnson, Dean (dean.johnson@vita.virginia.gov)		CSR/IRWEB Team			
Template: Kathy Test - Employee Discounts		Sent: 2021-05-05 09:12:03		Worst: Clicked Link in Email	
May 05, 2021 10:00:16 EDT	0d 0h 48m 13s	Email Opened	73.40.64.100	Google Chrome	Mac
May 05, 2021 10:00:16 EDT	0d 0h 48m 13s	Clicked Link in Email	73.40.64.100	Google Chrome	Mac
May 05, 2021 10:00:16 EDT	0d 0h 48m 13s	Viewed Training Page	73.40.64.100	Google Chrome	Mac
May 05, 2021 10:00:34 EDT	0d 0h 48m 31s	Email Opened	63.117.215.9	Google Chrome	Windows
May 05, 2021 10:00:34 EDT	0d 0h 48m 31s	Clicked Link in Email	63.117.215.9	Google Chrome	Windows
May 05, 2021 10:00:34 EDT	0d 0h 48m 31s	Viewed Training Page	63.117.215.9	Google Chrome	Windows
Lindsay, Kyle (kyle.lindsay@vita.virginia.gov)		CSR/IRWEB Team			
Template: Kathy Test - Employee Discounts		Sent: 2021-05-05 09:12:03		Worst: Clicked Link in Email	
May 05, 2021 09:40:02 EDT	0d 0h 27m 59s	Email Opened	73.40.64.100	Google Chrome	Mac
May 05, 2021 09:40:02 EDT	0d 0h 27m 59s	Clicked Link in Email	73.40.64.100	Google Chrome	Mac
May 05, 2021 09:40:02 EDT	0d 0h 27m 59s	Viewed Training Page	73.40.64.100	Google Chrome	Mac

EXHAUSTIVE REPORT

INCLUDES:

- TEST SUMMARY
- TEMPLATE INFORMATION
- ACTION BREAKDOWN
- 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

REPEAT OFFENDERS REPORT

INCLUDES:

- REPEAT OFFENDERS
- PHISHING TERM APPENDIX

Repeat Offenders for CSRM IR/WEB Team

Created:	May 04, 2021 13:03 EDT
Last Updated:	May 04, 2021 13:03 EDT
Service Type:	None
Auto Sync:	Off
Smart Sync:	Off
Active Targets:	3

Email	Name	Failures	Last Failed Test		
dean.johnson@vita.virginia.gov	Johnson, Dean	2	May 05, 2021 09:12 EDT	4	0
kyle.lindsay@vita.virginia.gov	Lindsay, Kyle	3	May 05, 2021 17:45 EDT	4	1



QUESTIONS?

CONTACT INFO

Dean Johnson, Director of Threat Management

Dean.Johnson@vita.virginia.gov

804-416-8785

Kathy Bortle, Incident Response Specialist

Kathy.Bortle@vita.virginia.gov

804-416-6061

Jim Sturdevant, Sr., Incident Response Specialist

Jim.Sturdevant@vita.virginia.gov

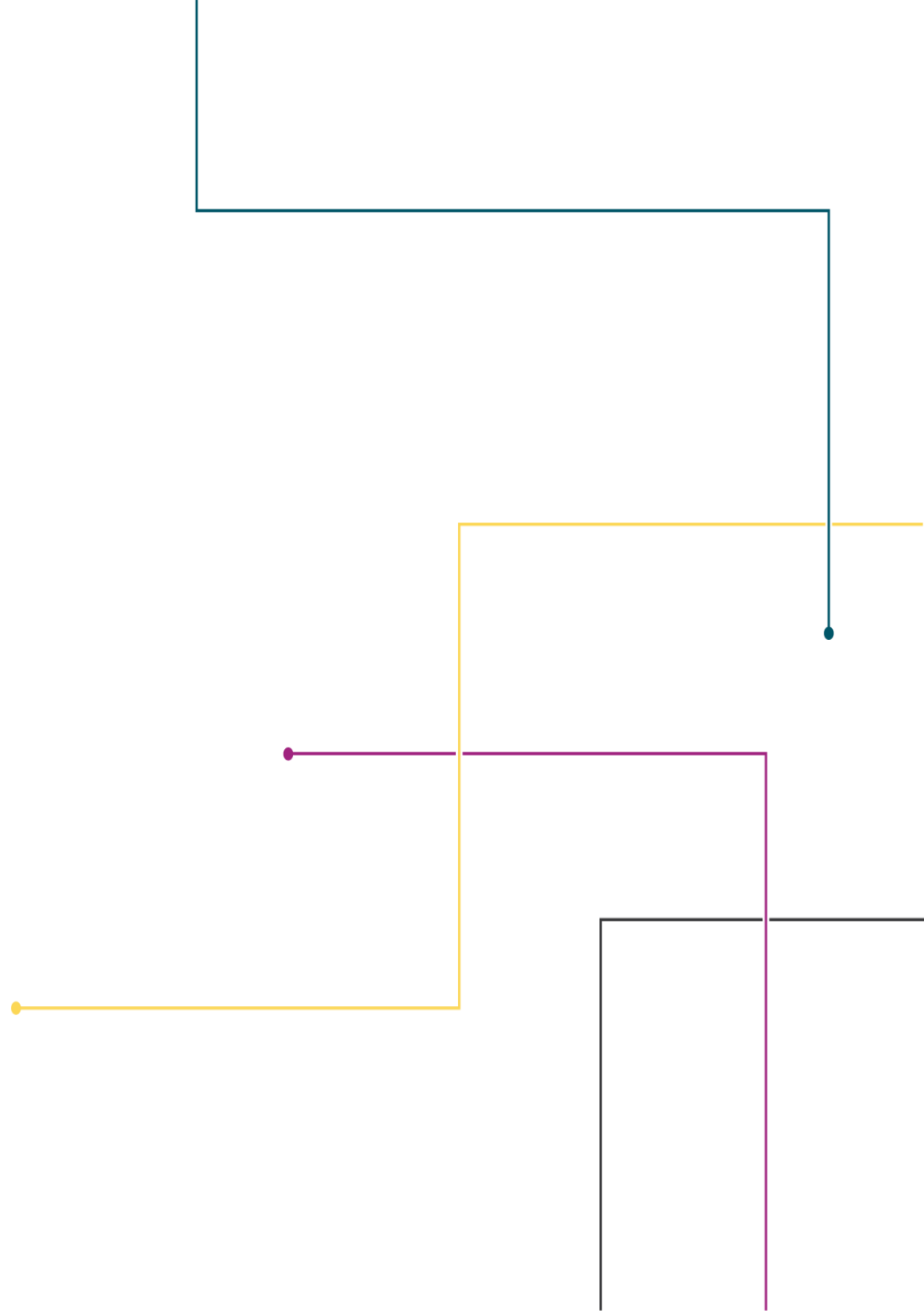
804-416-6038



RISK MANAGEMENT UPDATE

COMMONWEALTH SECURITY AND RISK
MANAGEMENT

OCTOBER 6, 2021



AGENDA

- SEC 520 Risk Management Standard updates
- NCSR
- COV Incident Response Tabletop Exercise
- Cyber Storm VIII

SEC 520 RISK MANAGEMENT STANDARD

- Updated language to section 2.0 - Quantitative Risk, changing the “Center for Internet Security” to “18 CIS Controls”
- Section 4.4 IT System and Data Sensitivity updated to match/align with SEC501
- Section 4.4.2, 2. updated to required data set template to be attached to system security plan - *new requirement*
- Section 4.7.2 update to the Vulnerability Scanning Requirements
- Updated Appendix A, Risk Management Framework Core, to match the new 18 CIS Controls
- ORCA ~November 1, 2021
- Publish ~January 2022

NATIONWIDE CYBER SECURITY REVIEW

- Maturity based self assessment of your agency's cybersecurity and risk management programs
- Based on the NIST Cybersecurity Framework
- Sponsored by DHS and MSISAC
- New application - No longer in Archer
- 141 Questions
- Designed to take approximately one hour to complete
- Agency participation is included in the Annual Report for Information Security
- A communication with instructions has been sent out to agency ISO's from the MSISAC (October 1, 2021)
- Follow on presentation by Tyler Scarlotta /CI Security/MSISAC

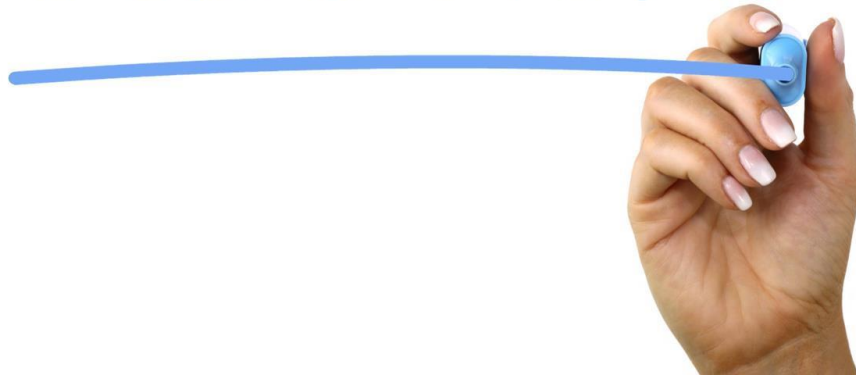
COMMONWEALTH INCIDENT RESPONSE TABLETOP EXERCISE

- Tabletop Exercise – October 28, 2021
 - All day exercise
 - Remote/Virtual
- Hot Wash – October 29, 2021
- CSRM will provide Certificate of participation
- Follow on presentation by Zack Wilson/SAIC

CYBER STORM VIII – SPRING 2022

- Cyber Storm is the Cybersecurity and Infrastructure Security Agency’s (CISA) biennial capstone cyber exercise. Each exercise includes thousands of distributed participants and traditionally takes place over the course of a week
- CISA sponsored exercise focused on policy, procedure, information sharing, coordination, and decision-making (i.e., no actual attacks)
- Provides a venue to simulate discovery of and response to a large-scale, coordinated significant cyber incident
- Players participate from their actual work locations and receive exercise “injects” that describe scenario impacts to their organization and respond according to policy and procedure
- Exercise date: To be announced (Spring 2022)
- To participate, please email commonwealthsecurity@vita.virginia.gov

QUESTIONS



jonathan.m.smith@vita.virginia.gov



Overview & Benefits of the Nationwide Cybersecurity Review (NCSR)

MS-ISAC Presenters: Tyler Scarlotta & Emily Sochia

Nationwide Cybersecurity Review (NCSR)

Background:

- No-Cost, Anonymous, Annual Self-Assessment
- Measures the gaps and capabilities of State, Local, Tribal, and Territorial governments' cybersecurity programs
- Based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

Benefits:

- Obtain reporting that can be communicated with key stakeholders and utilized to prioritize the “next steps” towards cybersecurity improvement.
- Measure your results anonymously against your peers.

Question Set & Maturity Scale

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
Detect	Protective Technology	PR.PT
	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
Respond	Detection Processes	DE.DP
	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
Recover	Improvements	RS.IM
	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

NIST Cybersecurity Framework

<https://www.nist.gov/cyberframework/framework>

SCORE	MATURITY LEVEL	The recommended minimum maturity level is set at a score of 5, indicated by the red horizontal line below
7	Optimized	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	Tested and Verified	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	Implementation in Process	Your organization has an activity or process defined within documented policies, standards, and/or procedures. Your organization is in the process of implementing and aligning the documentation to a formal security framework and/or methodology.
4	Partially Documented Standards and/or Procedures	Your organization has a formal policy in place and has 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 that has been approved by senior management.
2	Informally Done	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 senior management.
1	Not Performed	Activities, processes, and technologies are not in place to achieve the referenced objective.

TLP:WHITE

General User Guide

- Detailed instructions for navigating the NCSR can be found in the General User Guide: <https://learn.cisecurity.org/ncsr-user-guide>.



TLP:WHITE

2021 NCSR Updates

- 2021 assessment opened for participation on October 1st
- An end-user associated with an organization in the NCSR portal is the only person viewing the specific organization's results.
- The NCSR has moved to a new platform: LogicManager
- You can access your data and automated reports throughout the year.

How to Login?

- All current Nationwide Cybersecurity Review (NCSR) users can now login at <https://cis.my.logicmanager.com/>
- Click “Get a new password” and enter your email

LogicManager™

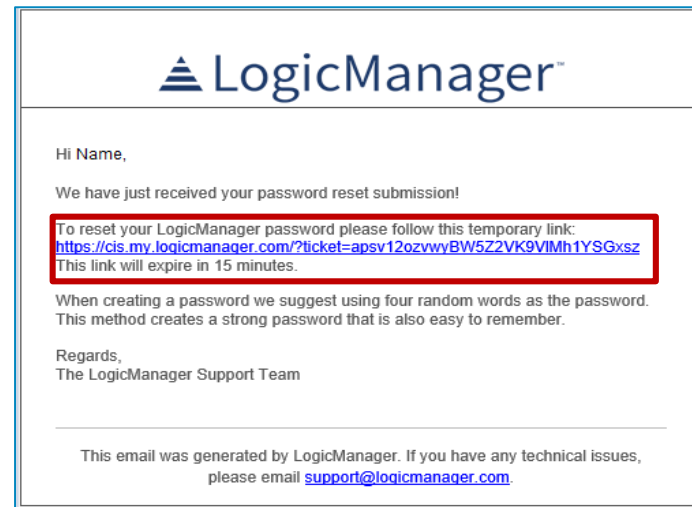
Email Address

Password

LOG IN

Get a new password

Sign up for an account



NCSR Portal Home Screen

The screenshot displays the NCSR Portal Home Screen. At the top, there is a navigation bar with the MS-ISAC logo and menu items: Taxonomy, Plans, Library, Report Portal, and Solution Center. A 'Chat with support' button is visible in the top right corner. Below the navigation bar, the page title is 'LogicManager Home'. A welcome message reads 'Welcome to the Nationwide Cybersecurity Review!'. A search bar is present above a table. The table contains one row of data:

TASK NAME	SOURCE	STATUS	DUE DATE
2021 Nationwide Cybersecurity Review (NCSR)	MS-ISAC TEST ORGANIZATION	New	02/20/2022

Below the table, there is a 'Task by Status' section with a donut chart. The chart is labeled 'ALL TIME' and shows a single red segment, indicating that all tasks are in the 'New' status.

TLP:WHITE

NCSR Portal Home Screen

- Please do not click the following options that are at the top of the NCSR portal:



- For all questions on the NCSR please contact ncsr@cisecurity.org or (518) 266 - 2466

Navigating the NCSR

Your Task List ⋮

🔍 Search

TASK NAME	SOURCE	DUE DATE ▲
→ 2021 Nationwide Cybersecurity Review (NCSR)	MS-ISAC TEST ORGANIZATION	02/28/2022

⏪ < 1 / 1 > ⏩

TLP:WHITE

Taking the NCSR

Questionnaire Tabs with Questions Listed:

▼ Demographics Questions

These Demographic questions do not impact your score but do provide us with additional context to the responses you are providing. The grant specific questions are related to the Homeland Security Grant Program (HSGP). As outlined in the Fiscal Year 2020 HSGP Notice of Funding Opportunity (NOFO), the NCSR is a requirement for organizations receiving funding through the HSGP, specifically the State Homeland Security Grant Program (SHSP) and the Urban Area Security Initiative (UASI).

If you have any questions, please reference the NCSR guidance materials below:

- NCSR FAQ Guide
[NCSR FAQ Guide.pdf](#)
- NCSR Maturity Levels & Response Scale
[NCSR Maturity Levels & Response Scale.pdf](#)
- NCSR Question Set - Help Text Clarification
[NCSR Question Clarification.xlsx](#)

2021 Nationwide Cybersecurity Review (NCSR)

Task Details Demographics Questions Identify Protect Detect Respond Recover Automation Questions Post-Survey Questions Optional: End User Comme... Optional: End User Comme... Optional: End User Comme... Optional: End Use

Category: Identify - Asset Management

Category Description: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

ID.AM-1: Physical devices and systems within the organization are inventoried. ©

Taking the NCSR

- Responding to a question:

The screenshot shows a web interface with a navigation bar at the top containing 'Profile', 'Assessment', 'References', 'Related Tasks', and 'Documents'. A 'Profile Actions' dropdown menu is visible in the top right corner. The main content area displays 'Category: Identify - Asset Management' and a 'Category Description: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.' Below this is a question: 'ID.AM-1: Physical devices and systems within the organization are inventoried.*'. A 'select option' dropdown menu is open, showing a list of options: 'Optimized', 'Tested and Verified', 'Implementation in Process', 'Partially Documented Standards and/or Procedures', 'Documented Policy', 'Informally Done', and 'Not Performed'. The 'Optimized' option is currently selected and highlighted in a darker grey.

Documenting Notes

- At the end of the assessment, there are “Optional: End User Comments” for each section
- This allows the end-user to enter and save notes on that specific question.

Optional: End User Comments - Identify

Comments/Notes: ID.AM-1: Physical devices and systems within the organization are inventoried.
Enter text

Comments/Notes: ID.AM-2: Software platforms and applications within the organization are inventoried
Enter text

Comments/Notes: ID.AM-3: Organizational communication and data flows are mapped
Enter text

Comments/Notes: ID.AM-4: External information systems are catalogued
Enter text

Comments/Notes: ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value
Enter text

TLP:WHITE

Help Text – Question Clarification

- A question mark icon is located to the right of a specific question, giving clarification on the question:

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders* ⓘ

Select option

ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process* ⓘ

Select option

Category: Identify - Supply Chain Risk Management

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, man

Select option

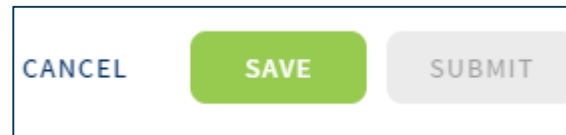
Ask Yourself: Are contractors, suppliers, or third party hosts categorized and prioritized based on the organization's security needs?

Tracking Progress & Submitting NCSR

- Home screen section – Task Status:

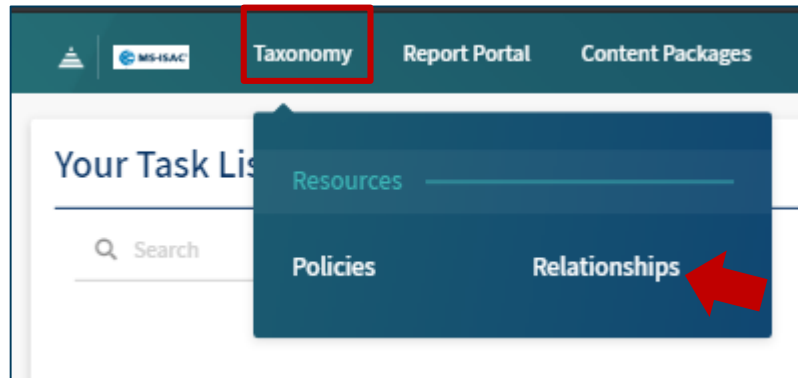


- Lower right-hand corner of your NCSR task view:



Viewing Your Assessment

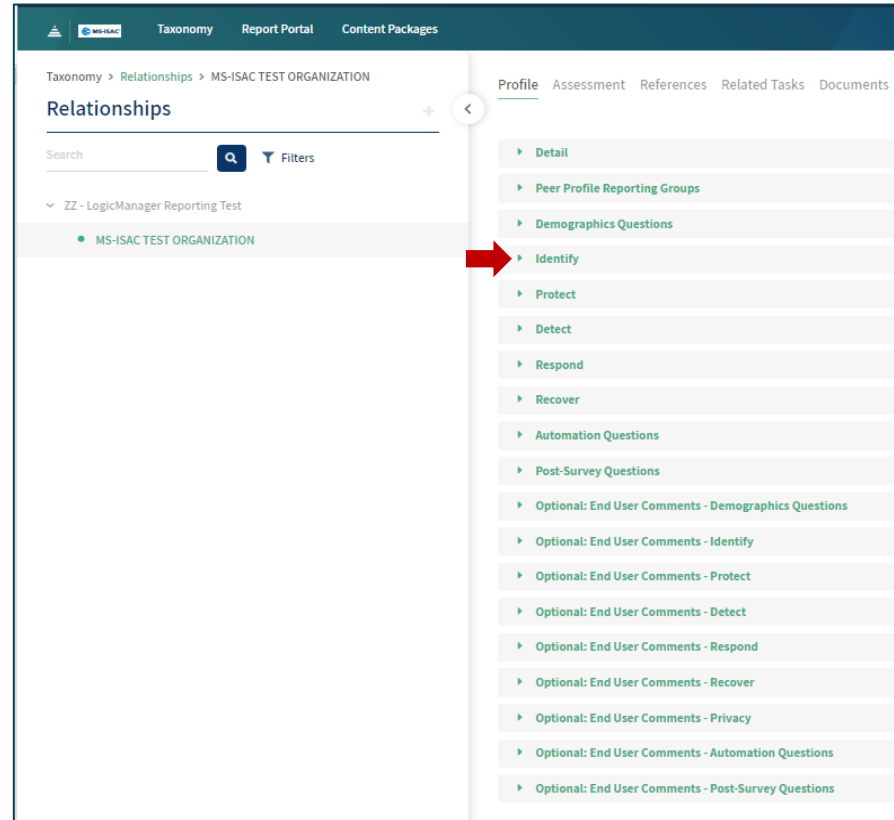
- To view your current year's assessment and responses, select the "Taxonomy" section in the top left of the screen and then select "Relationships":



TLP:WHITE

Viewing Your Assessment

- You will then be brought to your organization's information entered within the current NCSR assessment.



TLP:WHITE

Viewing & Exporting Your Assessment

- From this section, you can view all of your responses:

▼ Identify

Category: Identify - Asset Management 🔒

Category Description: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. ⓘ

ID.AM-1: Physical devices and systems within the organization are inventoried.* ⓘ ⓘ
Partially Documented Standards and/or Procedures

ID.AM-2: Software platforms and applications within the organization are inventoried.* ⓘ ⓘ
Implementation in Process

ID.AM-3: Organizational communication and data flows are mapped.* ⓘ ⓘ
Implementation in Process

ID.AM-4: External information systems are catalogued.* ⓘ ⓘ
Implementation in Process

- You can also export to PDF, using “Profile Actions”:

Profile Actions ▼

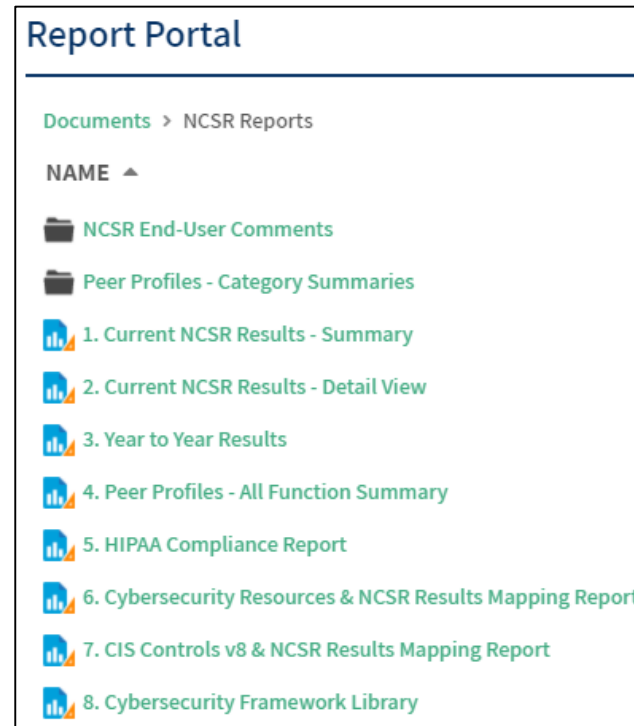
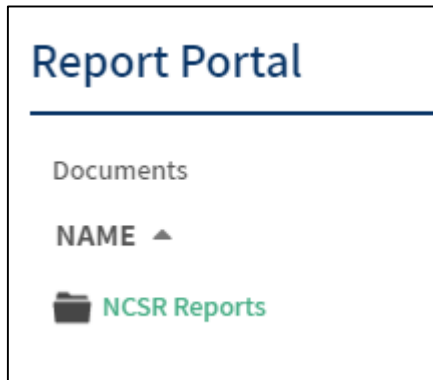
- New Profile Task
- Field History
- Copy Profile Field Values
- Export to PDF

Assessment Completed, What Next?

1. Access NCSR Reports in the NCSR Portal
2. Utilize Resources to Assess Results
3. Identify Areas for Improvement
4. Make the Plan

Reports Available in the Report Portal

End-User Reports Listed on NCSR Portal Home:



TLP:WHITE

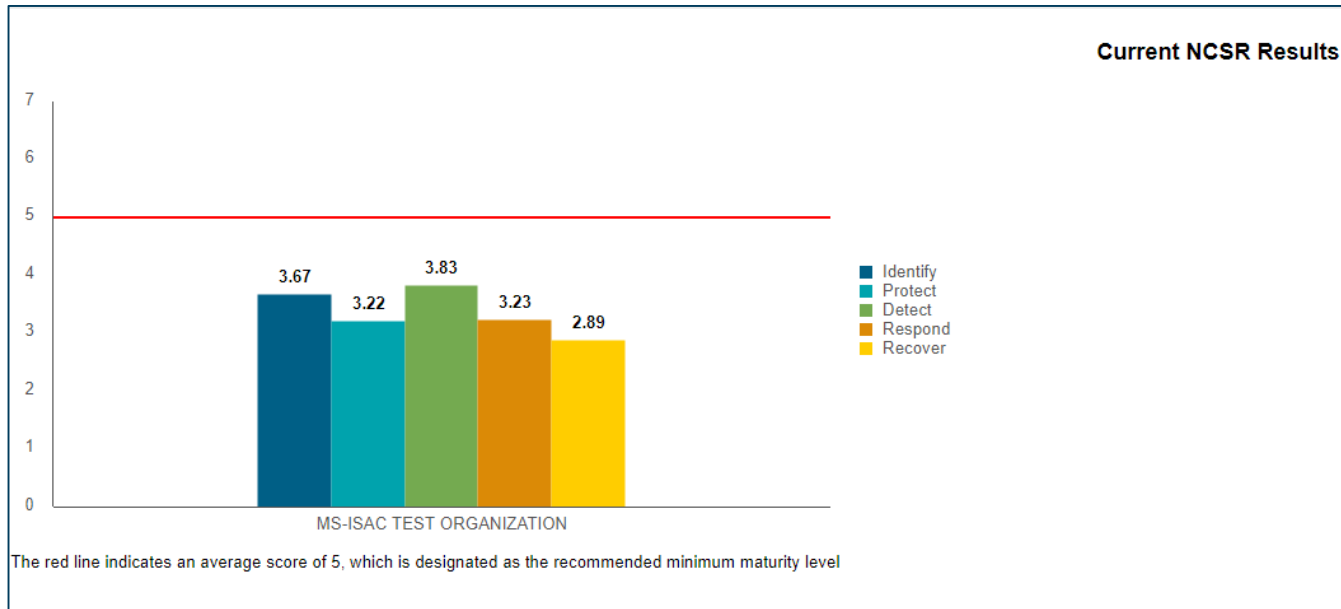
Report: Current NCSR Results

- From this screen, you can select your organization from the drop down
- You will only be able to view your own organization's information

The screenshot shows a web interface titled "Parameters". Under the "Organization" section, there is a dropdown menu labeled "Organization Name". The dropdown is open, showing a list with "MS-ISAC TEST ORGANIZATION" selected and highlighted in blue. Below the dropdown are four buttons: "Cancel", "Back", "Next", and "Finish". A red arrow points to the "Finish" button.

Report: Current NCSR Results - Summary

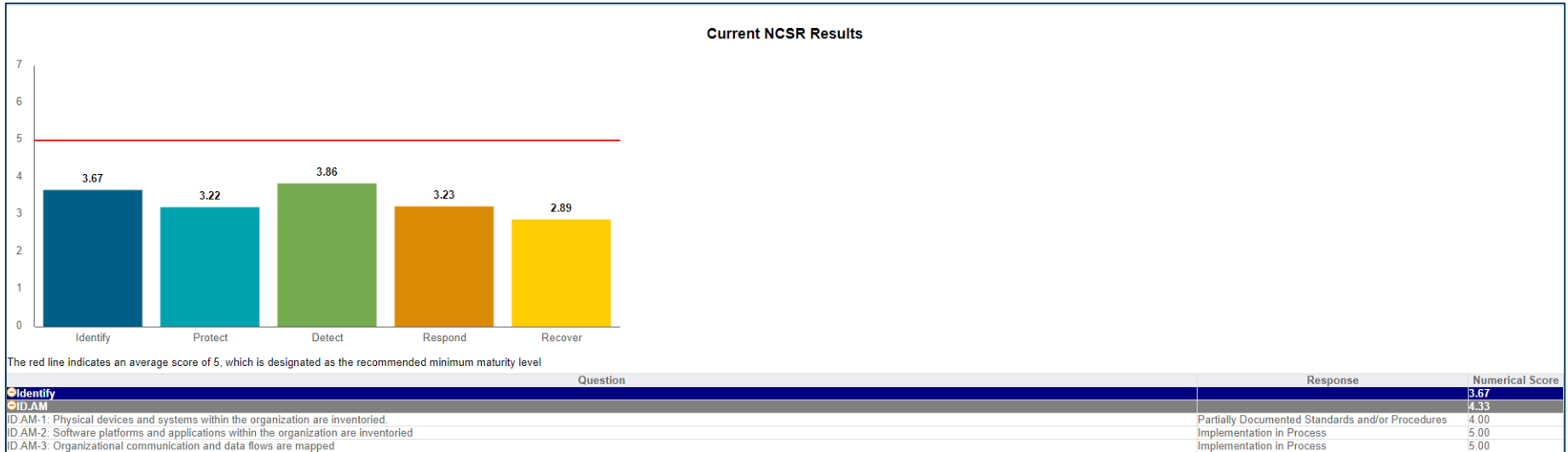
Displays average score within Identify, Protect, Detect, Respond, & Recover Functions:



TLP:WHITE

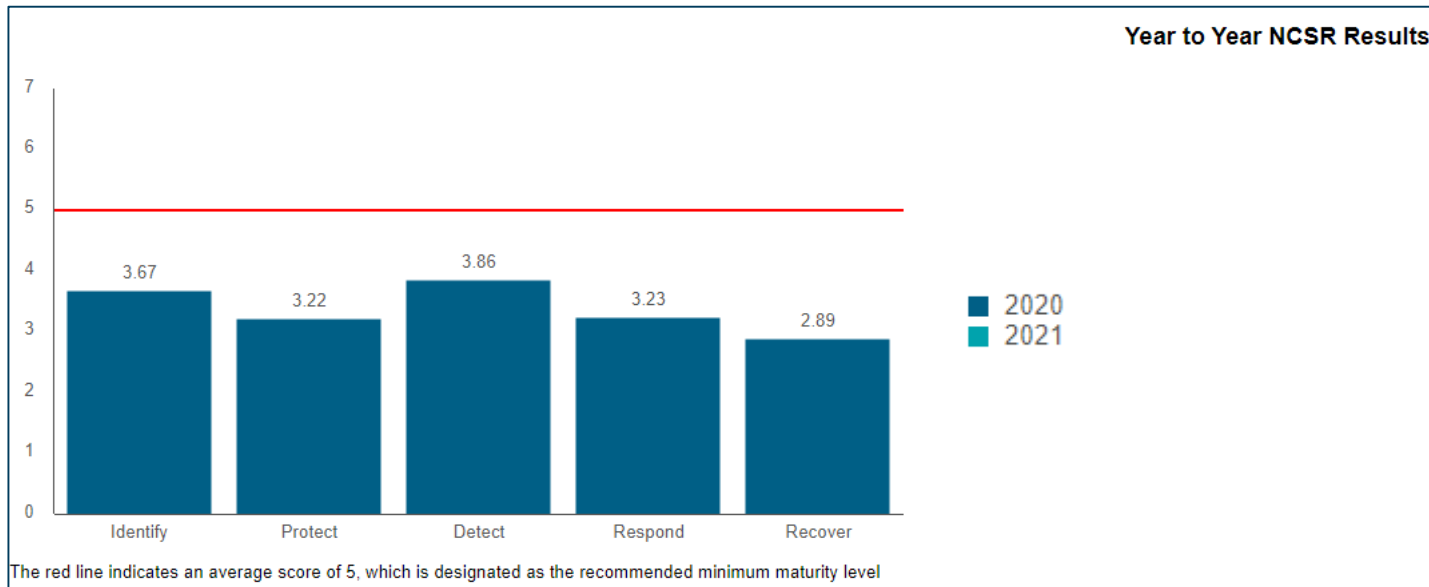
Report: Current NCSR Results – Detail View

- You can also review your results by NIST CSF subcategory:



Report: Year-to-Year Results

- Displays the average scores of the functions, for each year of participation:



TLP:WHITE

Report: HIPAA Compliance Report

- Displays the alignment of HIPAA Security Rules to the NIST CSF subcategories, as well as your NCSR answer for the applicable NIST CSF subcategory:

HIPAA to NIST Alignment		
HIPAA Security Rule	NIST CSF	Response
HIPAA Security Rule §164.310(a)(2)(ii)	Crosswalked to NIST CSF (DE.CM-7)	I scored: Informally Done
HIPAA Security Rule §164.310(a)(2)(ii)	Crosswalked to NIST CSF (DE.CM-2)	I scored: Documented Policy

Report: CIS Controls v8 & NCSR Mapping

- CIS Controls v8 Report example in the NCSR platform:

CIS Control/Sub Control	CIS Control/Sub Control	Applicable Implementation Group(s)	NCSR Question/NIST CSF Subcategory	NCSR Answer Submitted	NCSR Answer Numeric Score
01.01: Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Implementation Group 1	Crosswalked to NIST CSF (ID.AM-1)	Not Performed	1

TLP:WHITE

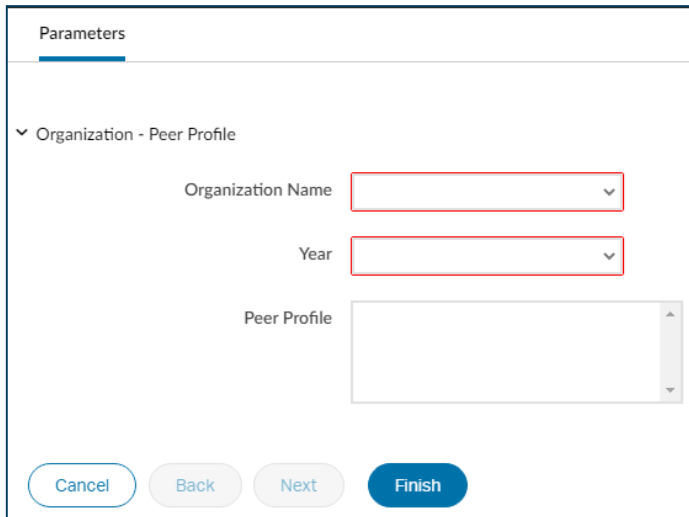
Report: Cybersecurity Resources & NCSR Mapping

- Cybersecurity Resources Report example in the NCSR platform:

Cybersecurity Resource	Link to Resources Documents	NCSR Question/NIST CSF Subcategory	NCSR Answer Submitted	NCSR Answer Numeric Score
Policy Template: Access Control Policy	Link	ID.AM-1: Physical devices and systems within the organization are inventoried	Not Performed	1
Open Source: OpenVAS	Link	ID.AM-1: Physical devices and systems within the organization are inventoried	Not Performed	1

Reports: Peer Profiles by Function or Category

- The “Peer Profile” Reports will be available in March 2022.
- Your applicable peer profiles will appear in the box shown below
- If you are associated with many peer profiles, you can select to view them all at once, or one at a time



Parameters

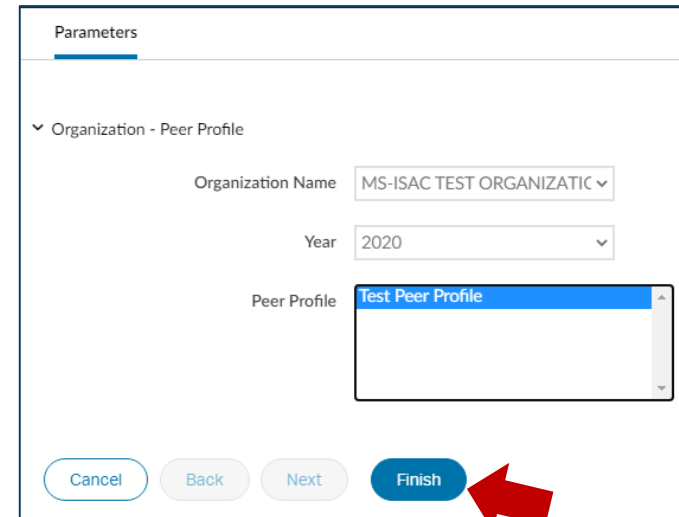
Organization - Peer Profile

Organization Name

Year

Peer Profile

Cancel Back Next Finish



Parameters

Organization - Peer Profile

Organization Name MS-ISAC TEST ORGANIZATIC

Year 2020

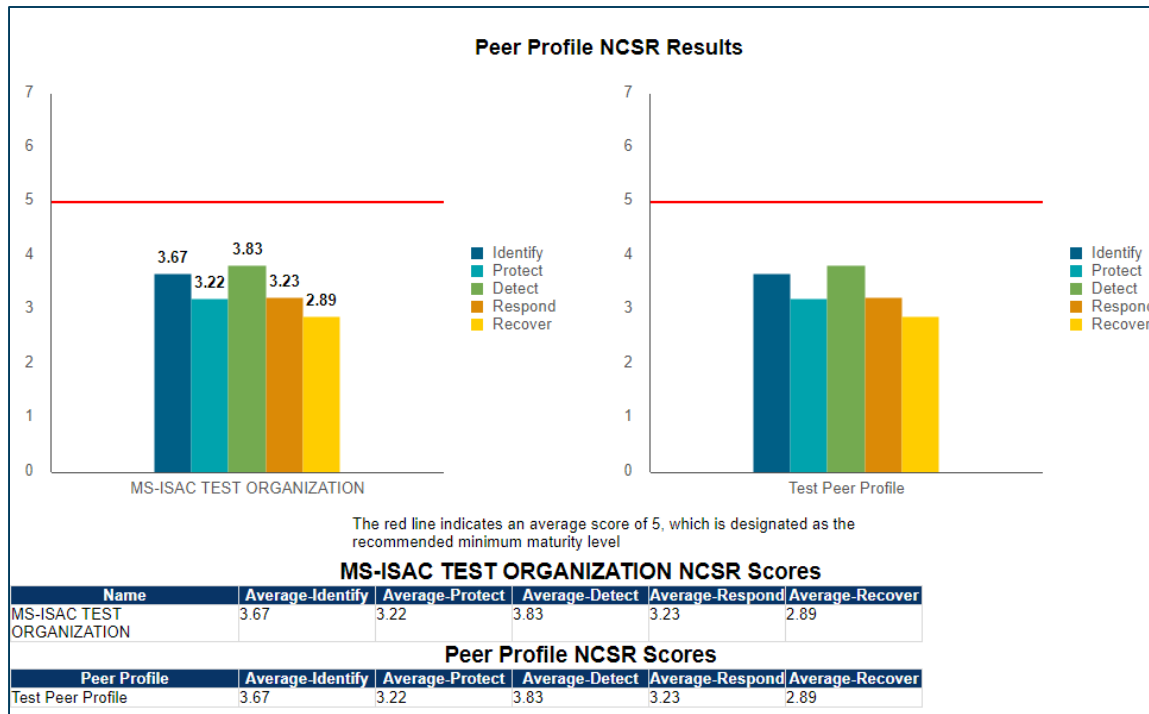
Peer Profile Test Peer Profile

Cancel Back Next Finish

TLP:WHITE

Report: Peer Profiles – All Function Summary

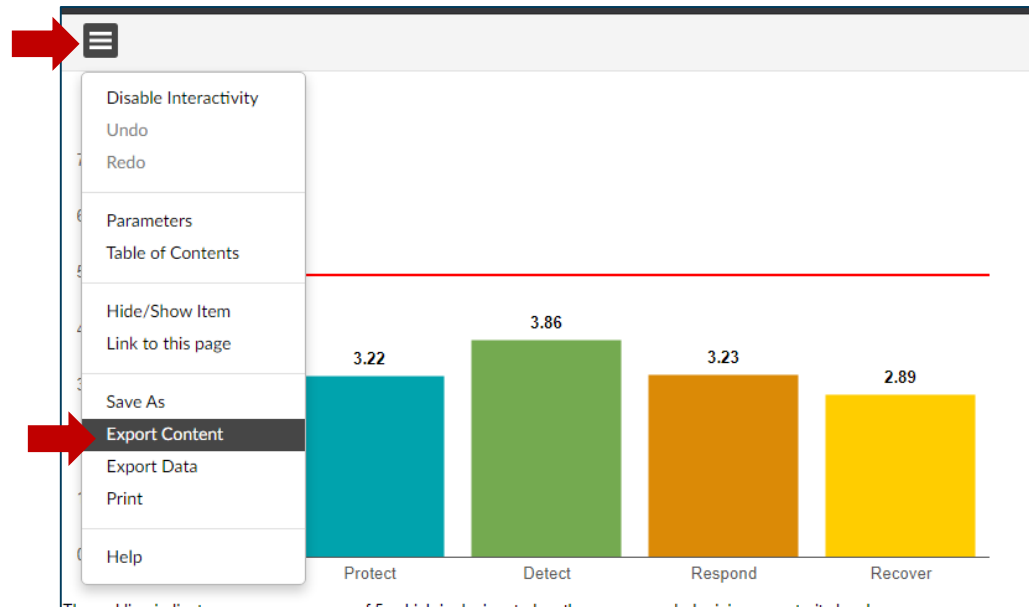
- Displays your organization’s average scores by function, compared to an anonymized overall average of the peer group(s) you are associated with:



TLP:WHITE

Displaying a Report

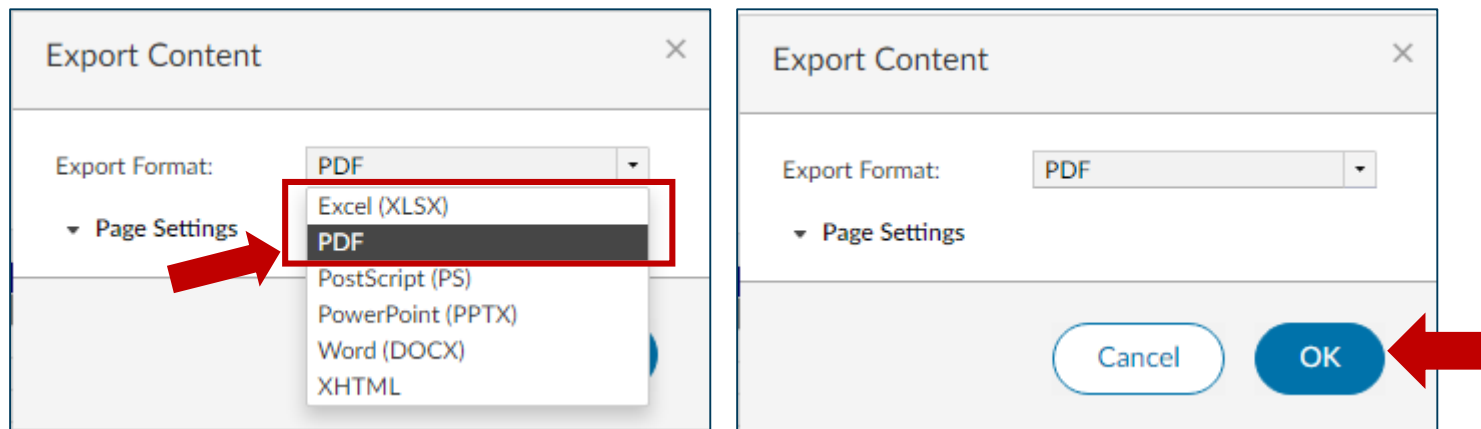
- When viewing any of the reports on a dashboard, there is a three horizontal line icon in the upper left corner of the report. After selecting that three line icon, an option for “Export Content” will appear.



TLP:WHITE

Exporting a Report

- After selecting the “Export Content” option, the following options will appear
- Select the format applicable for your organization and select “OK”. Your report will then be available.



TLP:WHITE

End-User Resources

- Located Here: <https://www.cisecurity.org/ms-isac/services/ncsr/>

✓ NCSR Reporting Templates

- CIS Controls Version 8 – NCSR Results Mapping Template
- Cybersecurity Resources Mapped to NIST CSF - NCSR Results Template
- NCSR-Data-Reporting-Template

✓ Metrics Workgroup Reference Guides

- NIST CSF Policy Template Guide 2020
- Cybersecurity Resources Guide
- Supply Chain Cybersecurity Resources Guide
- First Steps Within a Cybersecurity Program
- Risk Assessment Guide
- The NCSR & Your HIPAA Security Rule Assessment

TLP:WHITE



Multi-State Information Sharing & Analysis Center (MS-ISAC)

Contact: NCSR@cisecurity.org

MSI Tabletop Exercise 2021

Zachary D. Wilton
SAIC MSI Security Incident Response

Agenda

- Overview
- Objectives
- Expected Outcomes



Overview

The MSI Annual Tabletop Exercise is an unclassified, adaptable exercise developed by the MSI for the Platform, and 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.



Objectives

- **The Main Objective for this Tabletop is to uncover Strengths within SAIC Multisourcing Services:**
 - Evaluate the Service Delivery capability for detecting, responding to, and recovering from simulated, realistic 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-CSR



Expected Outcomes

- **Expected outcome from this event is to 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
 - Ensure COV information systems will successfully operate in support of the exercise scenario
 - Enhance awareness, readiness and coordination
 - Test capability to determine operational impacts of a cyberattack
 - Test participant's exercise playbooks, incident analysis, incident response plans and procedures, and incident reporting
 - Demonstrate compliance with MSI Security Incident Management Process SMM 4.1.5.7 and VITA Playbooks
 - Identify Enterprise-wide opportunities for improvement
 - Further integration of multi sourcing program between MSI, VITA-CSR, Service Towers, and the Agencies



ARCHER SECURITY EXCEPTION

LOURDES LUNSFORD

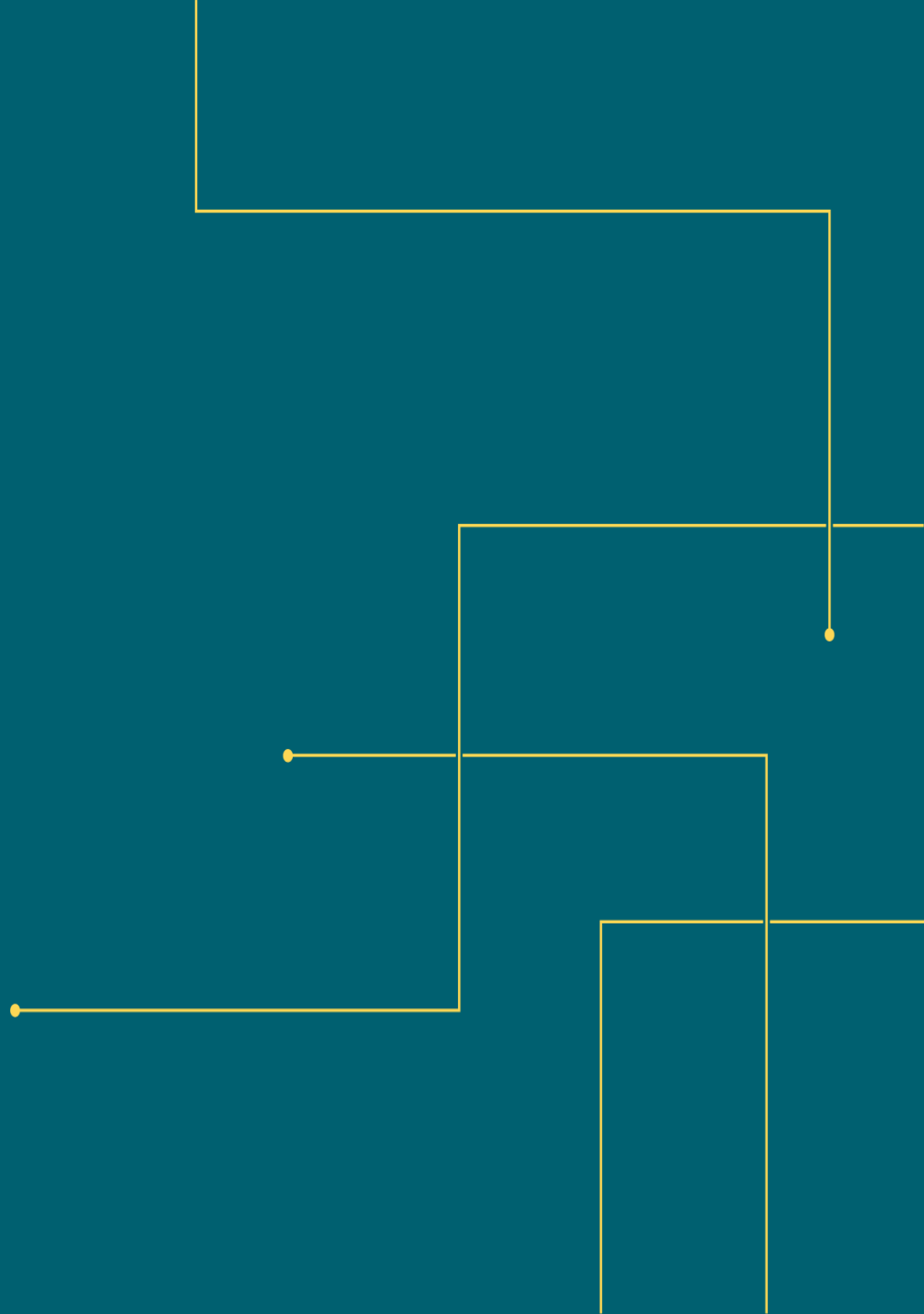
Security Architect

ISOAG

10/05/2021

OVERVIEW

- Security Exception Review
- Security Exception Live Demo



Navigate to the Exception Request



Maria De Lou...

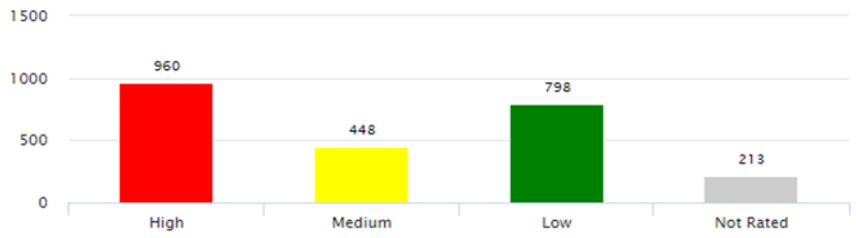
- Home
- Risk Management
- Enterprise Management
- Incident Management
- Threat Management
- Agency Workspace
- Reports

- Quick Links
- Applications that Need a Da...
- List of Devices
- Questionnaire Status Report
- List of Applications
- IT Security Audit Plans
- List of Business Processes

AGENCY EXECUTIVE DASHBOARD

Agency Applications

Applications by Criticality Rating



Risk Assessment Questionnaire

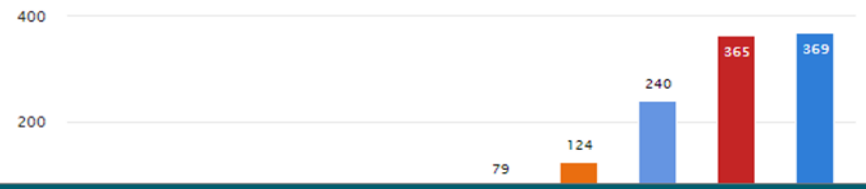
- Risk Assessment Questionnaire - New Record
- Risk Assessment Questionnaire - Records

Exceptions iVIEW

- Exception Requests - New Record
- Exception Requests - Records

Agency Exceptions Reports

Exceptions by Status



javascript:\$nff(/foundation/ExtRedirect.aspx?hash=newrecord/eyJjb250ZW50SWQjOjAsImFwcGxpY2F0aW9uSWQjOjgzfQ==)

ENTER THE NEW RECORD INFORMATION



Exception Requests: Add New Record

Exception Declaration | Review and Approvals | Extension Request

ABOUT

GENERAL INFORMATION

Exception ID:	* Agency: <input type="text"/>
* Submission Status: <input type="text" value="Draft"/>	Overall Status: Draft
Submit Date: <input type="text"/>	Expiration Date:
<small>The requested duration of the exception should not exceed twelve months.</small>	Days to Expiration:
Requested Expiration Date: <input type="text"/>	Initial Creation Date:
Agency Contact: <input type="text"/>	


ENTER THE NEW RECORD INFORMATION




Exception Requests: Add New Record

Associated Policies:

EXCEPTION DECLARATION

 * Exception Description:

Provide details of the exception description

 Business and Technical Justification:

Provide the technical justification or limitations in relation to the exception.

ENTER THE NEW RECORD INFORMATION



Risk Management

Enterprise Management

Incident Management

Threat Management



Reports

Exception Requests: Add New Record

SAVE

SAVE AND CLOSE



Business Impact and Risks:

Provide all the risks identified through the risk assessment.

Residual Risk:

Any residual risk after the compensating controls are identified must be listed here.

AFFECTED APPLICATIONS

Affected Applications:

... Add

ENTER THE NEW RECORD INFORMATION



Exception Requests: Add New Record

AFFECTED APPLICATIONS

Affected Applications:

ASSOCIATED FINDINGS

Associated Findings:

COMPENSATING CONTROLS

Select the control procedures that will compensate for the exception.

Compensating Controls:

Additional Compensating Controls:

Add the compensating controls the agency plans to implement to reduce the identified risks.

ENTER THE NEW RECORD INFORMATION



Exception Requests: Add New Record

SAVE SAVE AND CLOSE

AFFECTED DEVICES

Affected Devices: Add

EXCEPTION REQUEST ATTACHMENTS

Name	Size	Type	Upload Date
------	------	------	-------------

No Records Found Attach any documentation relevant to the exception

AGENCY HEAD APPROVAL

Name	Size	Type	Upload Date
------	------	------	-------------

No Records Found

HISTORY

* Required

CHANGE SUBMISSION STATUS

When the new record is completed and ready for Architectural review change the Submission Status to “Submit for Review” and SAVE.

The screenshot shows the 'Add New Record' form for 'Exception Requests'. The top navigation bar includes 'Agency Workspace', 'AITR Workspace', 'Policy Management', 'Schedule Management', and 'Agency Auditor Workspace'. The form has tabs for 'Exception Declaration', 'Review and Approvals', and 'Extension Request'. Under 'GENERAL INFORMATION', the 'Submission Status' dropdown is highlighted in yellow and set to 'Submit for Review'. Other fields include 'Submit Date' (7/25/2019), 'Agency Contact' (Ed Miller), 'Architect Type' (CSRM Security Architecture and Operations), and 'Exception Type' (SEC 501). On the right, 'Agency' is 'Virginia Information Technologies Agency', 'Overall Status' is 'Draft', and 'Expiration Date' is empty.

An email is sent to the Architectural team.

- During the Architectural review the Security Architecture team, Operations team and ISOs will discuss the exception and finalize the exception for Agency Head approval.
- The Exception status will be changed to “Ready for Agency Head Approval” the agency ISO will receive a notification email.

- ISO can print the “Exception Request Template” for AH Signature from the EXPORT option within the exception record.

EXC-453 Exception Requests

The screenshot displays the user interface for an exception request record (EXC-453). At the top, there is a navigation bar with options: NEW, COPY, SAVE, SAVE AND CLOSE, EDIT, DELETE, and an 'EXPORT' button highlighted in yellow. Below this, the record details are shown, including the Agency (Alcoholic Beverage Control), Overall Status (In Architecture Review), and Submission Status (Submit for Review). A modal window titled 'Exception Requests: Export Options' is open, showing a list of report templates and export options. The 'Exception Request Template' option is highlighted in yellow. The export options include Rich Text File, Adobe PDF, Microsoft Excel, CSV, and HTML File. The interface also shows a sidebar with navigation options: ISO, ITAudit, RO, and ITAUDIT.

NEW COPY SAVE SAVE AND CLOSE EDIT DELETE

Record 2 of 17

RELATED RECALCULATE EXPORT

Initial Creation Date: 4/16/2019 9:34 AM Last Updated: 8/14/2019 2:41 PM

Exception Declaration Review and Approvals Extension Request

ABOUT

GENERAL INFORMATION

Exception ID: EXC-453 Agency: [Alcoholic Beverage Control](#)

Submission Status: [Submit for Review](#) Overall Status: [In Architecture Review](#)

Submit Date: 4/16/2019 Expiration Date:

Risk Rating: Days to Expiration:

Agency Contact: [Amy Luffey](#)

Architect Type: CSRM Security Architecture and Operations

Exception Type: SEC 501

EXCEPTION DECLARATION

Exception Description: testing all values

Business Justification: testing all values

Business Impact and Risks: testing all values

AFFECTED APPLICATIONS

Affected Applications: [Account Central](#)

ASSOCIATED FINDINGS

Associated Findings: EMDL1004

Exception Requests: Export Options

Report Templates

- Report templates integrate record data with predefined Mail Merge functionality using Microsoft Word.
- Exception Request Template**

Export Options

- The data export features enables you to export records to an external data file. The file format options are described below.
- Rich Text File**: Generates a file in Rich Text format intended for use in most standard word processors.
- Adobe PDF**: Generates a PDF file, which can be shared, viewed and printed by any user on any system using Adobe Reader (a free program) or Adobe Acrobat.
- Microsoft Excel**: Generates a file in Microsoft Excel format.
- CSV**: Generates a comma-separated text file intended for use in any application that can read text files.
- HTML File**: Generates an HTML file that users can view in any web browser. Users can also open the file in an HTML editor, a text editor or any other application that can read text files.

ISO ITAudit RO ITAUDIT

- Agency Head Approval can also be obtained by emailing the Agency Head. The email must include the following exception information:

✓ Agency	✓ Associated Policies
✓ Submit Date	✓ Exception Description
✓ Agency Contact	✓ Business Justification
✓ Exception Type	✓ Business Impact and Risks

- Agency Head will email back approval to ISO, acknowledging and accepting all the risks.

Remember emails must be encrypted!!!!



- Update Exception record by attaching the Agency Head approval (Signed form or email)

▼ AGENCY HEAD APPROVAL

Name	Size	Type	Upload Date	Add New
No Records Found				Add New

- Change Submission Status to “Submit for Approval”

* Submission Status:

- Architectural team is notified by email and the exception is routed for CSRM review
- CSRM completes review and CSRM Review Status is updated to either Approved or Denied

CSRM Review Status:

Explanation of Denial:

No Selection
Awaiting Review
Approved
Denied
Returned to Reviewer

- ISO receives an email notification with either Approval or Denial.

LIVE DEMO

<https://test.itgrcs.vita.virginia.gov/apps/ArcherApp/Home.aspx>





CENTRALIZED IT SECURITY AUDIT SERVICE

Mark McCreary, CISA, CISSP, CISM

Director

October 6, 2021



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ Risk-Based Audits
- ❖ Benefits from Using the Service
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding





➤ Current version is 502.4

➤ Found on VITA's website:

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





- IT Security Audit Standard (SEC502) requires audits of each Sensitive System every three-years.
- Measures compliance with the applicable requirements of IT Security Standard 501.
- Also includes other Federal regulations or COV Standards as applicable.

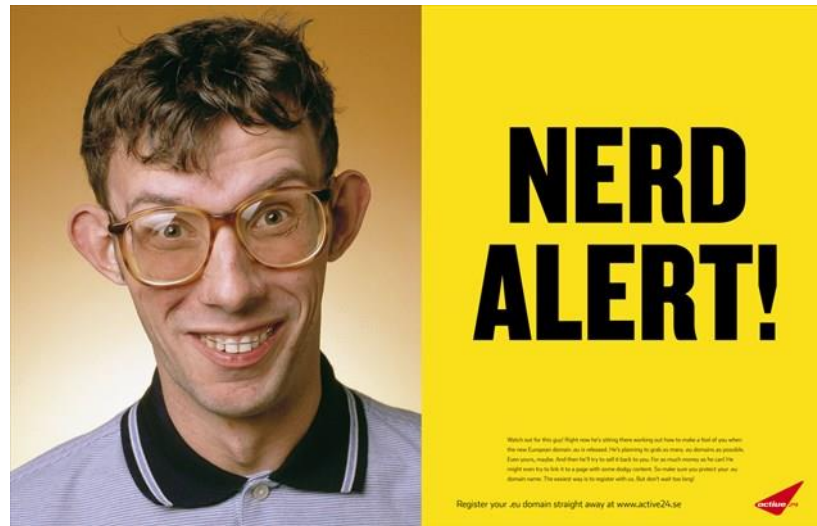


- ❖ IT Security Audit Standard
- ❖ **Centralized IT Security Audit Service**
- ❖ Risk-Based Audits
- ❖ Benefits from Using the Service
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding





Our A-Team



Our A-Team

Mike Dorris, CPA, CISA, Sr. IT Security Auditor

Nat Chusing, IT Security Auditor

Autumn Mashore, SEC +, IT Security Auditor

Matt Steinbach, IT Security Auditor



- Conduct Risk-Based IT Security Audits
- Help identify appropriate Corrective Action Plans
- Help with annual Audit Plan Submission



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ **Risk-Based Audits**
- ❖ Benefits from Using the Service
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding





Focus on High-Risk Areas/Activities



Determine High-Risk Areas By:

- Evaluating *Pre-Audit Internal Control Questionnaire(s)*

- Evaluating results of other audits or reviews
 - System and Organization Controls (SOC) Reports
 - Prior Audit Reports, Outstanding Findings



- Reviewing Security Exceptions
- Evaluating additional controls for Hosted Applications
 - Uses SEC525, some controls more restrictive than SEC501
 - Emphasis placed primarily on areas the agency controls, for example, Access Controls and Contingency Planning
 - ECOS Assessments/Oversight



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ Risk-Based Audits
- ❖ **Benefits from Using the Service**
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding





- Familiar with Commonwealth Security Standards and VITA Operations
- More cost-effective than private firms as DPB sets rates
- Knowledge retention
- Helps provide awareness to Agency Heads of IT security control weaknesses





Audit Compliance Grade

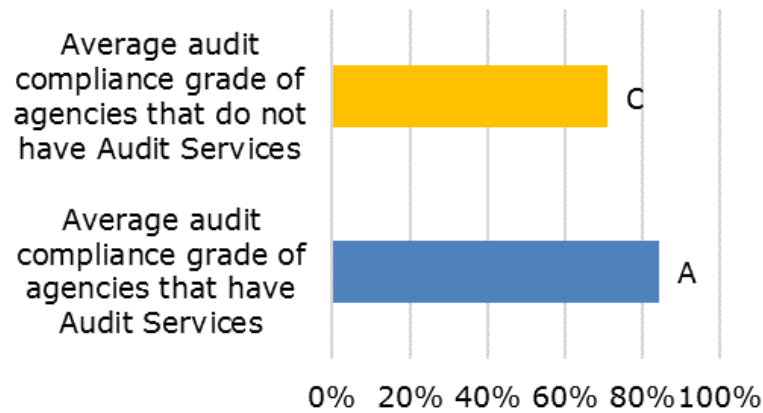
- 1) Sensitive System Audits conducted at least once every three-years +
- 2) Audit Plan Updated and Submitted +
- 3) Quarterly Finding Updates Submitted =

A



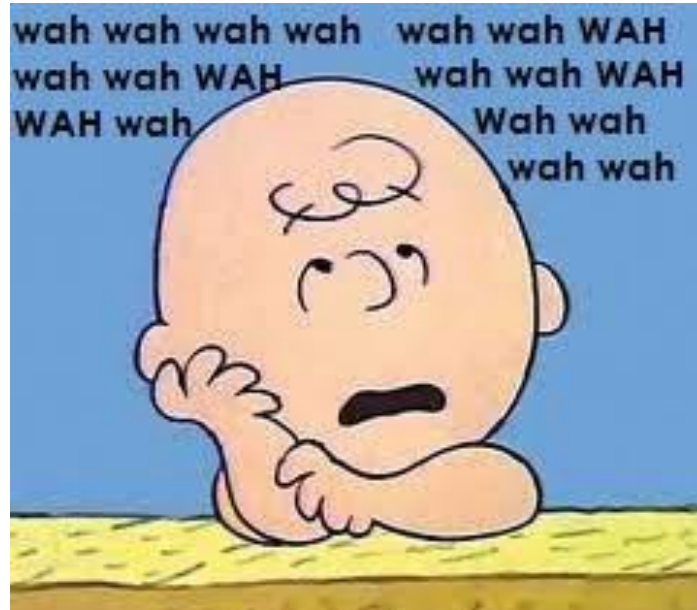


Average Audit Compliance Grades Audit Services Agencies vs. Non- Audit Services Agencies



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ Risk-Based Audits
- ❖ Benefits from Using the Service
- ❖ **Common Issues Found During Audits**
- ❖ Memorandum of Understanding





- No Formally Documented and Approved IT Security Policies and Procedures.
- ISO does not report to the Agency Head.
- Agency Head not formally designating System Owners, System Owners not designating Data Owners and/or System Admins.
- Not documenting how the impacts resulting from a compromise of data confidentiality, integrity, or availability were determined.



- Account Management
 - Inappropriate privileges, separation of duties
 - Not Disabling Inactive Application Accounts
 - Not using a 42-day password change frequency for sensitive system authenticators or for Admin accounts

- Not using Two-Factor Authentication
 - When accessing sensitive systems over the Internet
 - When using a network connection to access development environments or perform administrative functions on servers or multi-user systems



- Establishing remote connections with vendors that circumvent the network's perimeter protections (LogMeIn, GotoAssist).
- Hosting agreements do not contain current information security terms and conditions or are inappropriate for type of service.
- Limited review and analysis of audit logs.
- Few approved Security Exceptions on file for known control failures.





- Identifies the in-scope sensitive IT systems
- Audit cycle is three-years
- Deliverable = One Audit Report per cycle covering the in-scope systems
- Total charge is split into three installment payments



- Every two-years, Planning and Budget uses the sensitive systems in Archer to determine agency funding for IT Security Audit Services and associated charges.
- Funding and charges may be adjusted by DPB during the term of the three-year MOU.



- ❖ IT Security Audit Standard
- ❖ Centralized IT Security Audit Service
- ❖ Risk-Based Audits
- ❖ Benefits from Using the Service
- ❖ Common Issues Found During Audits
- ❖ Memorandum of Understanding



Contact me at (804) 416-5174

or

Mark.McCreary@VITA.VIRGINIA.GOV





CYBERSECURITY AWARENESS MONTH 2021

CYBERSECURITY AWARENESS MONTH

Cybersecurity Month is fast approaching so let's start planning our activities now. Below are the weekly themes for the month.

Week 1: Be Cyber Smart

Take simple actions to keep our digital lives secure.

Week 2: Fight the Phish!

Highlight the dangers of phishing attempts—which can lead to ransomware or other malware attacks—and how to report suspicious emails.

Week 3: Explore. Experience. Share.

Celebrate National Initiative for Cybersecurity Education's (NICE) [Cybersecurity Career Awareness Week](#) and the global cybersecurity workforce, as well as host our own CISA hiring fair and highlight the varying educational tools CISA has.

Week 4: Cybersecurity First

Explore how cybersecurity and staying safe online is increasingly important as our world continues to operate virtually for so much of work and play.

ENGAGEMENT IDEAS

- Contribute your voice and resources to social media conversations by using the hashtags *#BeCyberSmart* and *#CybersecurityAwarenessMonth* or have *Fireside Chat with your agency CISO or security personnel*.
- Include a message about the importance of cybersecurity in newsletters, mailings on your agency website during October. Work with your Comms Department to get the word out.
- Host an event or meeting to discuss local, relevant cybersecurity issues.
- Organize, provide, or promote cybersecurity training and exercise opportunities for your internal and external stakeholders.
- Participate in a local or virtual training or exercise to improve cybersecurity and resilience within your organization.
- Use the tip sheets available at cisa.gov/cybersecurity-awareness-month to read up on various cybersecurity topics.

SCHEDULE OF EVENTS

- Oct. 1: Work with your leadership to issue an official company proclamation in support of #CyberMonth and their commitment to Do Your Part.
#BeCyberSmart
- Oct. 1: Send a Buzz highlighting your agency's involvement in Cybersecurity Awareness Month and provide helpful cybersecurity tips for them to #BeCyberSmart
- Oct. 1: Send/schedule first series of daily or weekly tips to social media/employees on how to stay safe online
- Oct. 11: Send/schedule second series of daily or weekly tips to social media/employees on how to stay safe online
- Oct. 18: Send/schedule third series of daily or weekly tips to social media/employees on how to stay safe online and how to join the cyber workforce
- Oct. 25: Send/schedule fourth series of daily or weekly tips to social media/employees on how to stay safe online
- Oct. 26: Host a Cybersecurity Awareness Month Partner event for employees

GET THE WORD OUT!

Governor's Proclamation:

<https://www.governor.virginia.gov/newsroom/proclamations/proclamation/cybersecurity-awareness-month.html>

Twitter

Facebook

Instagram

LinkedIn

Blogs

RESOURCES AND EVENTS

<https://www.cisa.gov/cybersecurity-awareness-month>

https://staysafeonline.org/cybersecurity-awareness-month/?utm_source=CISA&utm_medium=website&utm_campaign=NCSAM_Site&utm_term=NCSAM

<https://staysafeonline.org/resource/ransomware-and-responsibility-government-responsibility-and-individual-responsibility-explained/> - Video

<https://staysafeonline.org/resource/oh-behave-2021/> The annual Cybersecurity Attitudes and Behaviors Report

RESOURCES AND EVENTS

<https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-awareness-week> - Week Three

<https://www.cdse.edu/Training/Security-Awareness-Games/>

<https://www.vita.virginia.gov/information-security/awareness/kids-safe-online-poster-contest/> KIDS SAFE ONLINE 2022 poster contest

<https://www.sans.org/security-awareness-training/mlp/secure-the-family-2021/>
Practical Ways to Stay Safe Online at home

VDH CYBERSECURITY MONTH EVENT

Cyber Talk Series: Please join us for a conversation with Ms. Beth Burgin Waller. She is currently serving as the Chair, Cybersecurity and Data Privacy Practice at Woods Rogers PLC. Ms. Waller will speak on Ransomware from a Legal Perspective (A Guide To Incident Response From A Lawyer In The Trenches). MS. Waller also presented the topic (Ransomware from a Legal Perspective) to VITA back in August. It is very educational and informative!

Date: Friday, October 15, 2021 | 12:00PM | Virtual Meeting

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

Link:

<https://covaconf.webex.com/covaconf/j.php?RGID=r22726077449d32704519144c5d965ab6>

Please contact infosec@vdh.virginia.gov if you have any questions.

VITA EVENTS

VITA will be hosting a weekly CSAM Kahoots trivia contest based on the theme of the week. More details coming soon!

SAVE THE DATE:

FBI Special Agent Jesse Schibilia

Thursday, Oct 21 11 am to noon

The topic and registration link will be forthcoming.



CYBERSECURITY TRAINING REQUIREMENTS

CYBERSECURITY CURRICULUM

Agencies are required to procure, obtain or develop a cybersecurity curriculum that meets all of the requirements identified here:

- (A) Core Requirements;
- (B) Policy Review and Acceptance;
- (C) Role Based Training;
- (D) Other Regulatory Requirements;
- (E) Phishing Exercise
- (F) Additional training where required

CORE REQUIREMENT COURSES

Separation of Duties

Security Incidents

Proper disposal of Data Storage Media

Proper Use of Encryption.

Access Controls, Secure Passwords

Working Remotely

Intellectual Property Rights

Security of Data

Phishing and Email

Social Engineering

Mobile Devices

Ethics

Least Privilege Identifying and Reporting

Privileged Access

Insider Threat

Cloud Services

Browsing Safely

Physical Security

Hacking

Personal Identifiable Information (PII)

Privacy

Social Network

Malware

POLICY REVIEW AND ACCEPTANCE COURSES

Require documentation of IT System users' acceptance of the agency's security policies. Cybersecurity awareness training must include policy review and acceptance.

Acceptable Use - All users of IT systems must agree to the agency's acceptable use policy.

Remote Access Policy - All users of IT systems must agree to the agency's remote access usage and/or Telework Policy.

Other Applicable Policies - Users of IT systems must review and agree to comply with any applicable agency security policies.

ROLE BASE TRAINING

Agencies must provide appropriate cybersecurity training based on the assigned roles and responsibilities of individuals with specific security requirements.

Data Owner Training

System Admin Training

Data Custodian Training

Agency Head Training

REGULATORY REQUIREMENT COURSES

Agencies must provide training for all regulatory or contractual requirements that affect IT users. Agencies need to decide the appropriate level of regulatory training that is required for its users

Federal Tax Information (FTI)

Health Insurance Portability and Accountability Act (HIPAA)

Criminal Justice Information Services (CJIS)

Family Educational Rights and Privacy Act (FERPA)

Social Security Administration Training (SSA)

Payment Card Information (PCI)

Federal PII

Personal Health Information (PHI)

ADDITIONAL TRAINING WHERE REQUIRED

Agencies should offer training that goes beyond the required curriculum items when necessary in the agency's environment. The items below are a few suggested additional training that agencies should consider for their employees where appropriate

Senior Leadership Training

New Employee Orientation Training

Creating a Cyber Secure Home

PHISHING EXERCISE

Agencies are required to conduct a phishing exercise or phishing training with their employee / contractor users. A phishing campaign will help identify if users can successfully recognize, avoid and report phishing attempts that may occur.

VITA will be developing a phishing campaign.



IT SECURITY GOVERNANCE

Ed Miller
Director

October 6, 2021



AGENDA

- ❖ **Updates to Existing Standards**
- ❖ **New Security Standards**
- ❖ **Archer Updates**

UPDATES EXISTING SECURITY STANDARDS

Updates to Existing Standards

- ❖ SEC501 – Information Security Standard
- ❖ SEC525 - Hosted Environment Security Standard

UPDATES EXISTING SECURITY STANDARDS

- ❖ SEC501 and SEC525 are each in the area of 280+ different controls
- ❖ Most of the controls are exactly same in both standards
- ❖ However, there are 62 controls that are different

UPDATES EXISTING SECURITY STANDARDS

For example:

- ❖ 501 AC-7: (a) Enforces a limit of 10 consecutive invalid logon attempts by a user during a 15 minute period
- ❖ 525 A-7:(a) Enforces a limit of three consecutive invalid logon attempts by a user during a 15 minute period

UPDATES EXISTING SECURITY STANDARDS

- ❖ In addition, there is a new NIST 800-53 rev 5
- ❖ We want to review this in detail and determine what adjustments we want to make to 501/525. Many of the new revisions 5 adjustments are based on the latest threat intelligence and latest state-of-the art recommended practices.

NEW SECURITY STANDARDS

- ❖ We are looking to expand and add a few NEW standards:
 - ❖ Identity Access Management Standard: This will set baselines for using IAM tools to manage user access, permissions, and onboarding/off boarding of users.
 - ❖ Operational Technology (OT) Standard: This would cover industrial control systems, SCADA, and IOT, and Internet-of-Things.

ARCHER UPDATES

- ❖ Expect expansion of “application instances”.
- ❖ If your agency uses a software or service that a Service Provider provides, another agency provides or a company provides, we will be adding those items to your “Application” inventory in Archer

ARCHER UPDATES

- ❖ Expect expansion of “application instances”.
- ❖ These application instances, are essentially SAAS, and should be treated the same way as an SAAS, almost like an ECOS application.

ARCHER UPDATES

- ❖ Expect expansion of “application instances”.
- ❖ We recognize:
 - ❖ Your agency doesn’t technically “own” it, but you do need a “system owner” to manage your piece of it
 - ❖ Your agency only has a limited role in managing controls for applications like this: if its sensitive, i.e. limited RA, limited audit, etc.



QUESTIONS?

Upcoming events



NOVEMBER ISOAG

Nov. 3, 1 to 4 p.m.

Presenters:

Roy Logan/ Nasa

Krishna Marella & Joe Chambers/ Xerox

Meredith Ward/ Nascio

IS ORIENTATION

FINAL IS ORIENTATION 2021

DEC. 8, 2021

1 – 3 PM

PRESENTER: MARLON COLE

REGISTRATION LINK :

<https://covaconf.webex.com/covaconf/onstage/g.php?MTID=e6299241bfefde9a4e45b6e1b8a81e7cb>

VASCAN 2021

Securing New Ways to Work

WHEN: OCTOBER 7 AND OCTOBER 8

WHERE: VIRGINIA COMMONWEALTH UNIVERSITY (IN PERSON)

COST: CONFERENCE ONLY \$150

CONFERENCE AND TRAINING \$400

(CONFERENCE \$150 + TRAINING \$250)

TRAINING: LINUX FORENSICS

REGISTRATION LINK:

[HTTPS://VASCAN.VCU.EDU/CONFERENCE-REGISTRATION/](https://vascan.vcu.edu/conference-registration/)



**THANK YOU FOR
ATTENDING!**

