WELCOME TO THE Nov. 1, 2023 ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

November 1, 2023

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Tina Gaines/ VITA
Testing System Security Controls	Eduardo Takamura/NIST
Performing Incident Handling and COOP Exercises	David Cole/SysAudits
Web Modernization/Security	Joshua Jones/VITA
Virginia Identity Program External Communications Plan	Ron Sticinski/VITA
KnowBe4 Update	Tina Gaines/VITA
Upcoming Events	Tina Gaines/VITA
Adjourn	

Testing System Security Controls

A brief discussion based on NIST SP 800-53A control assessment guide

NIST SPECIAL PUBLICATION

SP 800-53A

53A

REVISION 5

ASSESSING
SECURITY AND PRIVACY CONTROLS
IN INFORMATION SYSTEMS
AND ORGANIZATIONS

RISK MANAGEMENT FRAMEWORK

Briefing for:
Virginia Information Technologies Agency (VITA)
Information Security Officer Advisory Group (ISOAG)
November 1, 2023

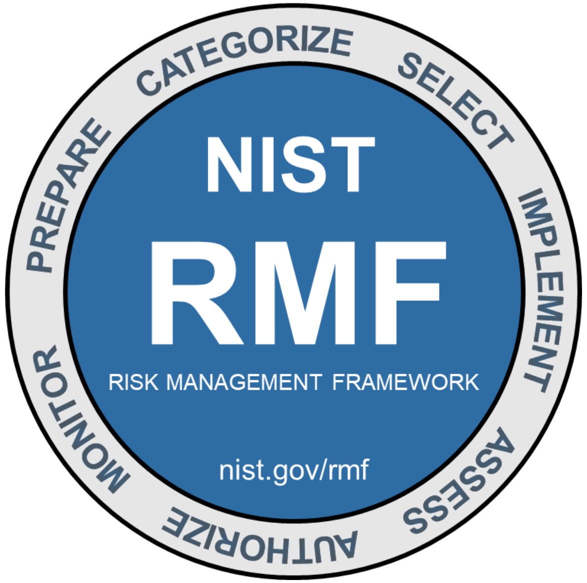
Presented by:
Eduardo Takamura (NIST)
NIST Risk Management Framework (RMF) Team
Computer Security Division (CSD)

DISCLAIMER: any mention of entities, equipment, materials, or services throughout this talk is for information only; it does not imply recommendation or endorsement by NIST, nor is it intended to imply best available solution for any given purpose.

NIST INFORMATION TECHNOLOGY LABORATORY

Outline

- **Risk Management** *(controls in risk management, risk management hierarchy)*
- **Controls** *(what are controls?)*
- **Assessments** *("why test controls?", assessment methods)*
- **Examples** *(testable controls and control testing)*
- **Automation** *(support for control assessments)*
- **Q&A**



https://nist.gov/rmf

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

https://csrc.nist.gov

Risk Management: *security and privacy RM*

GOAL: to increase or maintain security and privacy by reducing risks to an acceptable level.

ENABLER: use of protective measures and safeguards (security and privacy controls) to reduce the likelihood of a successful attack.

NECESSITY: to ensure controls* are implemented correctly, operating as expected, and meeting security and privacy requirements.

(*) selected given their protection level commensurate with identified risks.

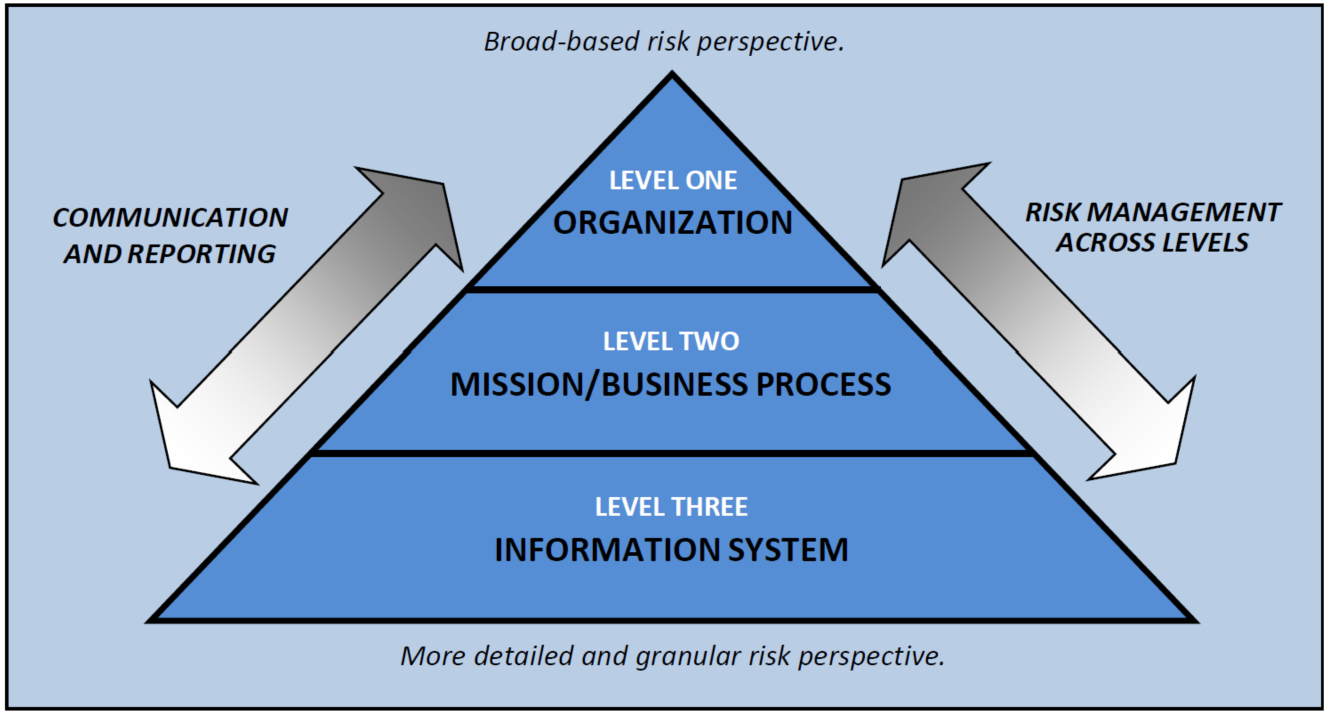
RISK REDUCTION

NIST SPECIAL PUBLICATION
SP 800-37
37
REVISION 2
RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS: A SYSTEM LIFE CYCLE APPROACH FOR SECURITY AND PRIVACY
RISK MANAGEMENT FRAMEWORK

NIST SPECIAL PUBLICATION
SP 800-39
39
MANAGING INFORMATION SECURITY RISK: ORGANIZATION, MISSION, AND INFORMATION SYSTEM VIEW
RISK MANAGEMENT FRAMEWORK

Risk Management: *hierarchy*

NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations,* identifies three levels in a risk management hierarchy:



Broad-based risk perspective.

COMMUNICATION AND REPORTING

LEVEL ONE
ORGANIZATION

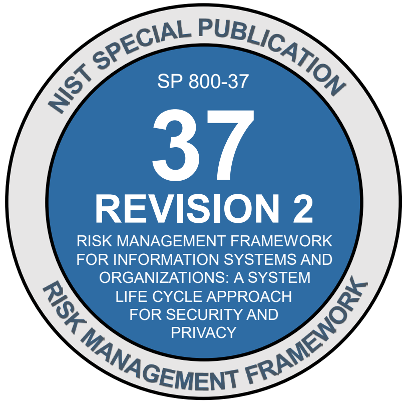
LEVEL TWO
MISSION/BUSINESS PROCESS

LEVEL THREE
INFORMATION SYSTEM

RISK MANAGEMENT ACROSS LEVELS

More detailed and granular risk perspective.

Figure 1: Organization-wide risk management approach


NIST SPECIAL PUBLICATION
SP 800-37
37
REVISION 2
RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS: A SYSTEM LIFE CYCLE APPROACH FOR SECURITY AND PRIVACY
RISK MANAGEMENT FRAMEWORK

SCOPE, BOUNDARIES & ACCOUNTABILITY

Controls: *what are controls?*

Controls: protective measures and safeguards for meeting security and privacy objectives, *commensurate with risk*.

Security control: the safeguards or countermeasures prescribed for an information system or an organization to protect the *confidentiality*, *integrity*, and *availability* of the system and its information. [OMB A-130]

Privacy control: the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable *privacy requirements* and *manage privacy risks*. [OMB A-130]

PROTECTIVE MEASURES AND SAFEGUARDS

Controls: *objectives*

- To make the information systems we depend on more penetration-**resistant**;
- To **limit** the damage from attacks when they occur;
- To make the systems **cyber-resilient** and **survivable**; and
- To **protect** individual's privacy.

CYBER-RESILIENCE AND SURVIVABILITY

Controls: *system, common and hybrid controls*

- ***System Controls***: controls specific to a system (e.g., password complexity enforcement on a local device)

- ***Common Controls***: controls that can be applied to (i.e., inherited by) multiple organizational systems (e.g., awareness and literacy training, policy and procedures, some physical and environmental controls)

- ***Hybrid Controls***: common controls that are implemented by both the common control provider (e.g., organization) and the organizational systems

NIST SPECIAL PUBLICATION
SP 800-53
53
REVISION 5
SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS
RISK MANAGEMENT FRAMEWORK

ACCOUNTABILITY AND COST EFFECTIVENESS

Controls: *assessment*

After controls are implemented, they must be verified to ensure:

- Controls are implemented correctly
- Controls are operating as intended (i.e., control objectives are being met)
- Controls are producing the desired outcome (i.e., security and privacy requirements are being met)

Note: other-than-satisfied controls (i.e., controls that are not fully implemented) may pose risk to the system and organization.

CONTROL EFFECTIVENESS & RESIDUAL RISKS

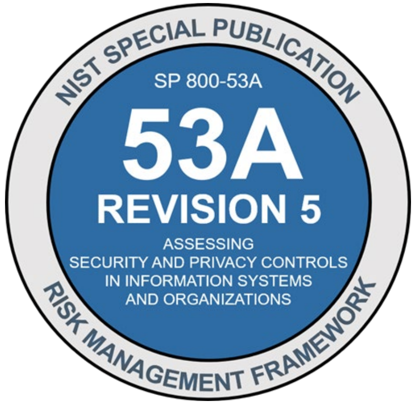
Assessments: *methods*

NIST Special Publication 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations,* identifies the potential methods for assessing controls:

EXAMINE

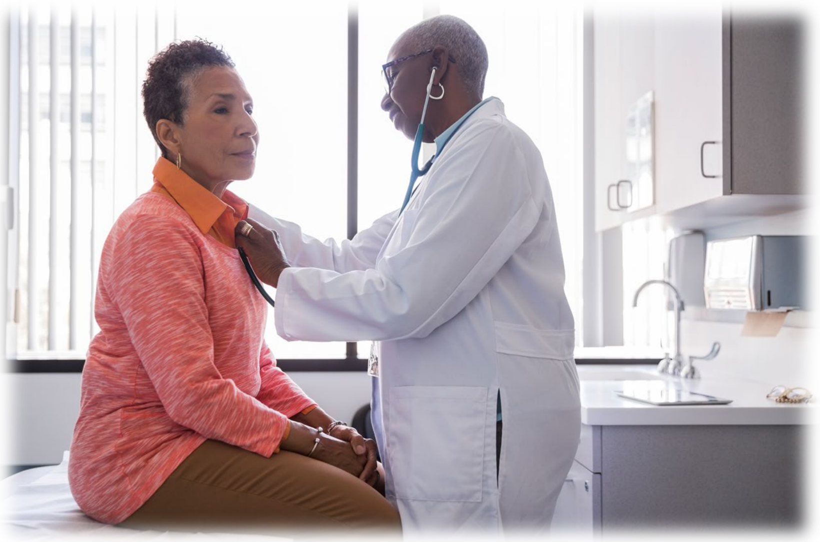
INTERVIEW

TEST



Assessments: *methods (cont’d)*

All assessment methods are used to collect data, and more than one method can be utilized. Analogy: *medical check-up*.



DATA COLLECTION

EXAMINE

INTERVIEW

TEST

Testing controls

- Collected data (i.e., *actual state*) is compared/measured against a requirement or specification (i.e., *desired state*).
- Used when expected results (i.e., *desired state*) are very specific (i.e., a value or a range of values).
- Tends to be reliable and helps promotes non-repudiation (provided that the implementation is correct).
- Support for remote assessments.
- Not just for compliance checking; test results can be compared to or support interview and/or examine results.

ASSURANCE, ACCOUNTABILITY & NON-REPUDIATION

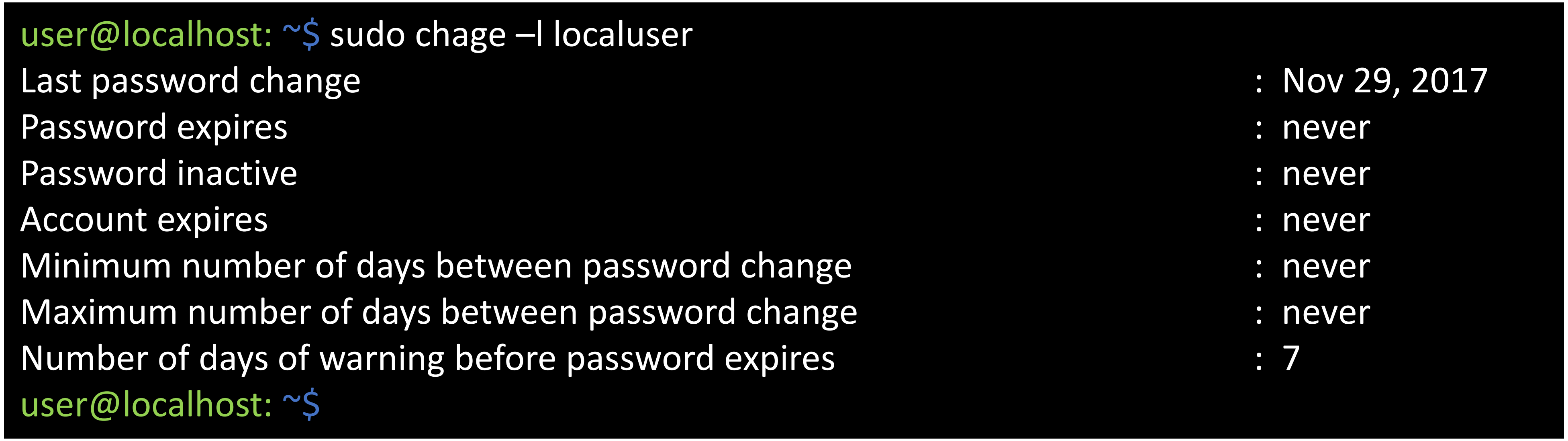
AUTOMATION & REMOTE ASSESSMENT

CATEGORIZE SELECT IMPLEMENT ASSESS AUTHORIZE MONITOR PREPARE
NIST
RMF
RISK MANAGEMENT FRAMEWORK
nist.gov/rmf

NIST SPECIAL PUBLICATION
SP 800-37
37
REVISION 2
RISK MANAGEMENT FRAMEWORK FOR INFORMATION SYSTEMS AND ORGANIZATIONS: A SYSTEM LIFE CYCLE APPROACH FOR SECURITY AND PRIVACY
RISK MANAGEMENT FRAMEWORK

Example: IA-5(1) Authenticator Management | Password-Based Authentication (L/M/H)

Linux shell command: `sudo chage -l <user>`



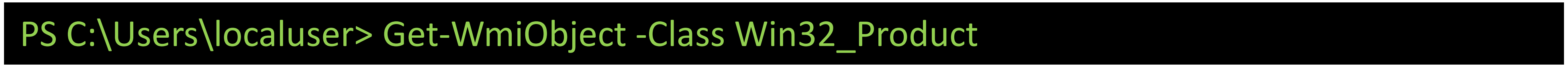
```
user@localhost: ~$ sudo chage –l localuser
Last password change                                    :  Nov 29, 2017
Password expires                                        :  never
Password inactive                                       :  never
Account expires                                         :  never
Minimum number of days between password change          :  never
Maximum number of days between password change          :  never
Number of days of warning before password expires       :  7
user@localhost: ~$
```

Reference: https://www.geeksforgeeks.org/chage-command-in-linux-with-examples/

INTERVIEW AND EXAMINATION STILL NEEDED

Example: CM-8 System Component Inventory (L/M/H)

Powershell command to enumerate installed applications: `Get-WmiObject -Class Win32_Product`



```
PS C:\Users\localuser> Get-WmiObject -Class Win32_Product
```

INTERVIEW AND EXAMINATION STILL NEEDED

Example: CM-8 System Component Inventory (L/M/H)

Linux shell command to enumerate installed software packages (Red Hat/CentOS): `rpm –qa --last`

INTERVIEW AND EXAMINATION STILL NEEDED

Automation

Tests may be automatable (if both desired state and actual state are *machine readable*). If automatable, potentially faster to conduct (and re-test).

- **Fully-automated** (but not 100% “lights-out” testing/assessments). Includes automated data collection and analysis (i.e., comparison, measurement). Human verification needed.*
- **Semi-automated** (manual/visual inspection, verification, examination needed)

Automated testing can support *ongoing assessments* that are essential to continuous monitoring.

Ongoing assessments and continuous monitoring can support *ongoing authorization*.

(*) an assessment that is fully automated does not mean a control is fully assessed; in most cases, only the test method is automated.

NIST INTERAGENCY REPORT
IR 8011
8011
SERIES
AUTOMATION SUPPORT FOR
CONTROL ASSESSMENTS
RISK MANAGEMENT FRAMEWORK

EFFICIENCY, ACCURACY, NON-REPUDIATION, FALSE/TRUE POSITIVES

Coming soon

- **NIST SP 800-53A assessment procedures online** (NIST Cybersecurity and Privacy Reference Tool [CPRT]): https://csrc.nist.gov/projects/cprt/catalog#/cprt/home

- **SP 800-53/53B/53A Public Comment Site:** https://nist.gov/rmf/sp800-53-controls

- **NIST Interagency Report (IR) 8011, *Automation Support for Security Control Assessments*** (guidance update + new technical guidance)

- **NIST Cybersecurity Whitepaper: *IR 8011, Automation Support for Control Assessments: Project Updates & Vision*** (forthcoming)

800-53 PUBLIC COMMENT SITE
SP 800-53
53
SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS
nist.gov/rmf/sp800-53-controls

CYBER SECURITY AND PRIVACY REFERENCE TOOL
CPRT
53
SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS
https://csrc.nist.gov/projects/cprt

NIST INTERAGENCY REPORT
IR 8011
8011
SERIES
AUTOMATION SUPPORT FOR CONTROL ASSESSMENTS
RISK MANAGEMENT FRAMEWORK

NIST UPDATES

Thank You

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST RMF
RISK MANAGEMENT FRAMEWORK
nist.gov/rmf
CATEGORIZE SELECT IMPLEMENT ASSESS AUTHORIZE MONITOR PREPARE

nist.gov/rmf   sec-cert@nist.gov   nist.gov/cyber

SysAudits | Systems Security Audit Professionals

WWW.SysAudits.com

David Cole: 11dc@audshield.com

Date December 6, 2022

Purpose: To document the Annual 2022 ABC Co. Table-Top Exercise for Incident Handling and Continuity of Operations.

Scope: ABC Co. IHP and COOP/DR plans and simulation of attack/compromise and restoration of services.

Source: David Cole, CISO table-Top lead

<table>
<tr><th colspan="3">ABC Co. IHP</th><th colspan="3">ABC CO. COOP</th></tr>
<tr><td colspan="3">Agency Policy</td><td colspan="3">Agency Policy</td></tr>
<tr><th colspan="6">Guidance</th></tr>
<tr><td colspan="2">Six-tabletop-exercises-FINAL.pdf</td><td colspan="2">CIS_Controls_Version_8.xlsx</td><td colspan="2">CIS_Controls_v8_Online.22.02.pdf</td></tr>
</table>

Table-Top Exercise Scenarios:

1. ABC Co. Malware Infection

SCENARIO: An employee within ABC Co. organization used the company’s digital camera for business purposes. In the course of doing so, they took a scenic photograph that they then loaded onto their personal computer by inserting the SD card. The SD card was infected with malware while connected to the employee’s personal computer. When re-inserted into an ABC Co. machine, it infected the ABC Co. system with the same malware.

What is ABC Co. response?

Questions

1. **Who within the organization would you need to notify?**

Upon identification from ABC Co. laptop antivirus notification, an email and call are placed to the ABC Co. CISO. A screenshot of the antivirus notification is emailed to help demonstrate the malware alert.

2. **How would your organization identify and respond to malware infecting your system through this vector?**

CISO will request that the laptop be taken off Internet. The staff involved in the compromise will complete an incident report and share with the ABC Co. CISO. ABC Co. laptops have audit and logging capabilities and antivirus to identify malware. The initial response includes screenshot of the notification, followed by an email and call to the ABC Co. CISO. The laptop is removed from production until further investigation and provide to the ABC Co. CISO through physical drop off.

3. **What is the process for identifying the infection vector?**

Laptop will be provided to CISO for review. ABC Co. CISO will review the incident notification, audit logs, and antivirus dashboard to identify the specific attack vector. Based on this information, security alerts will be researched further as needed through industry standard source such as Microsoft or the Center for Internet Security.

4. What other devices could present similar threats?

ABC Co. only has laptops in its environment and no IT infrastructure. Therefore, workstations are the only devices that could be impacted. Upon further investigation, determine if Box.com was connected and if other connections were live during discovery.

5. What should management do?

Management should evaluate the impact of the malware threat to mission operations and determine if data has been compromised. Based on this analysis, management and CISO should determine if clients and other entities should be notified. Further, the laptop will be reviewed for sanitization and reimaging based on the results of the investigation.

6. How can you prevent this from occurring again?

Training for staff if the malware originated from phishing or user actions. The source of the malware may need to be targeted as a specific subject area that is enhanced in the upcoming security awareness training

7. Does your organization have training and policies in place to prevent this?

ABC Co. trains all staff annually on security awareness. The CISO completes specific training and exercises on incident handling.

8. Do policies apply to all storage devices?

ABC Co. only has laptops in its environment and no IT infrastructure. Therefore, workstations are the only devices

9. Processes tested:

Detection ability/User awareness

10. Threat actor:

Accidental insider

11. Asset impacted:

Laptop and possible Cloud Box.com

Lessons Learned- After Action Report: ABC Co. must ensure that all staff maintain awareness of the actions needed to notify the CISO of malware incidents. Further, the delivery of affected laptops in person may need to be reviewed to determine if staff should send the laptop through certified delivery for an expedited return if the staff is working remotely.

ABC Co. laptops antivirus and audit and logging capabilities provide the CISO with needed information to identify the threat and attack vector. Due to the small size of the organization, notification of the incident to the CISO and ISSO moved efficiently and quickly.

Applicable CIS Controls: CIS Control 8: Malware Defenses, CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services, CIS Control 12: Boundary Defense

ABC Co. Malware: Triggering of ABC Co. COOP Plan

During the incident notification and investigation process, management will determine if the COOP should be activated. Based on the severity of the malware and its impact to operations, the COOP may be triggered if a credible threat is active or if critical information has been compromised and further investigation is needed before resuming operations. If the COOP is activated, the following steps will be taken:

- Determine if information needed for operations shall be restored, , such as operating system files and application software from ABC Co. managed laptops, workstations, servers, and user level information, such as user level files stored on a shared network drive, at a frequency that is consistent with ABC Co. defined recovery time objectives (RTO), and Recovery Point (RPO) objectives
- Evaluate telecommunication needs to determine if an alternate network operations are needed.
- Prepare communications to affected clients advising of operations continuity and plans/timeline to resume operations.

COOP After Action Report: No actions to currently report.

VIRGINIA IT AGENCY

WEBSITE MODERNIZATION PROGRAM

ISOAG MEETING

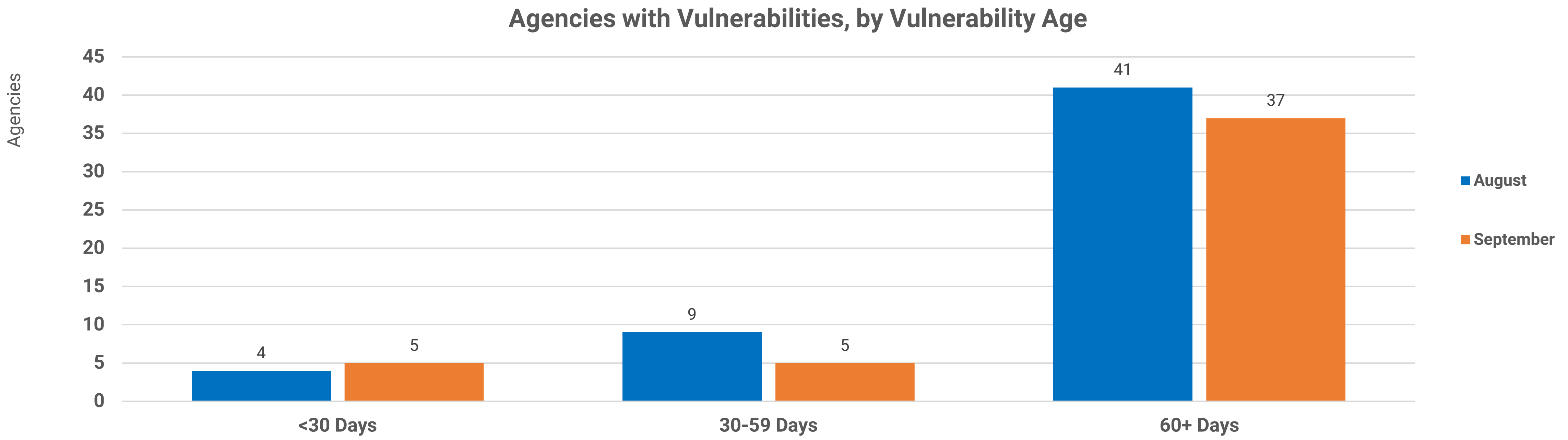
JOSHUA JONES

Program Lead

NOVEMBER 1, 2023

COMMONWEALTH CITIZEN WEBSITE MODERNIZATION PROGRAM UPDATES

- Reporting
- Prioritization and Resources
- Office Hours



- Reporting shared with the Secretary of Administration.
- Numbers are moving in right direction, but more must be done.
- Expectation is for there to be **0** past-due vulnerabilities by year end.
- Log in to Acunetix 360 to view, manage, and rescan issues.

Topic	Solution
Prioritization	Remediate Critical and High vulnerabilities within 30 days. All agencies must operationalize vulnerability remediation. Security scanning is not one-and-done. Identify responsible parties and ensure remediation efforts are part of their work routine.
Resources	Be proactive. Attend office hours. Ask for assistance. Work with CSRM on any suspected False Positives. Know your CAM and Enterprise Architect. Work with your architect to document issues that can't be remediated on time. Contact webmod@vita.virginia.gov with any questions.
eGov vendors	All eGov vendors have access to Acunetix 360 (if approved by agency). For questions, concerns, or to report issues about an eGov vendor, contact Manny Liban.
Other vendors	Create a COV account for vendor resources. Submit the COV account information to commonwealthsecurity@vita.virginia.gov to grant them access to Acunetix 360.
Nucleus access	Rollout on-going. Nucleus FAQs (KB0019481). More details to be shared at next ISOAG.

Office Hours

- Purpose: Provide guidance on Acunetix 360 usage, vulnerability management, security policy, and answer any questions you may have.
- Every Tuesday from 10 to 11 a.m.
- Open door, come any time in that hour
- Microsoft Teams (MEETING LINK)
- Or call in here: 434-230-0065, Conference ID: 542 653 741#

Questions

???

Virginian Identity Program (VIP) Update

Program Purpose

The Commonwealth of Virginia (COV) has launched an initiative to investigate the feasibility of an enterprise-wide single sign-on (SSO) solution for COV website and application users who are Virginians. Virginians in this context excludes statewide employees and COV partners. For example, a user potentially could use the same credentials to log in to the websites and applications on multiple agencies' websites.

Virginian Identity Program (VIP) Update

Program Goal and Objectives

The goal of SSO for COV applications is to:

- Create ease of doing business with state and local government agencies by providing a single username and password for constituents.
- Providing a central Virginian identity management solution at VITA.
- Provide protection of identities and systems with items such as multifactor authentication and additional identity proofing tools.
- Allow agencies to reprioritize personnel resources and reduce infrastructure.
- Ensure compliance with COV standards.

Virginian Identity Program (VIP) Update

Recent Accomplishments

- Completed 3 POCs and selected the Okta Customer Identity and Access Management (CIAM) solution as the key identity provider technology for VIP
- Received conditional eCOS approval for the Okta CIAM
- Received Project Initiation Approval (PIA)
- Established Impact Makers as the Project Management Office (PMO) team
  - Key goal is to gather agency requirements and create a request for proposal (RFP) to acquire the services of an identity proofing provider for the Commonwealth

Virginian Identity Program (VIP) Update

Goals of Detailed Planning Phase

- Create a robust service including security and architecture reviews.
- Evaluate RFP responses for identity proofing provider and select an awardee
- Establish the VIP solution in an Okta FedRAMP-certified tenant
- Conduct a pilot with the Governor's Office during March 2024

Virginian Identity Program (VIP) Update

Next Steps – Understanding Agency Needs

VITA plans to gather insights from different sources outlined below to ensure that the SSO solution aligns with the current and future needs of our customers. The strategy involves:

- Presenting at upcoming meetings to garner feedback and answer any initial questions:
  - AITR meetings
  - Information security officer advisory group (ISOAG) sessions
  - Relationship management committees (RMC)
  - Chief Information Officer (CIO) advisory council (CAC) sessions
- Conducting a listening tour with an initial group of executive branch agencies
- Providing customer account managers (CAM) as a resource

VIRGINIA
IT AGENCY

KnowBe4 Update

Name – Tina Gaines
Job title – Security Analyst/KB4 Training Team Leader

KnowBe4 Quarterly Product Update Video

Here at KnowBe4, we're always adding new features and improving our products. Watch the latest Quarterly Product Update to catch up on all the fresh content and new features that we've added to your KnowBe4 platform over the last quarter.

Here's the direct link to the KnowBe4 platform support article and video:
https://support.knowbe4.com/hc/en-us/articles/360015575313

The Security Awareness Company – Top 5 Phishing Fundamentals

Phishing continues to be one of the most common and effective cyber attacks that target organizations and individuals alike. This short Mobile-First module reviews the five fundamentals of phishing attacks to reinforce what phishing is, why it's dangerous and how to avoid falling for common scams.

Eighteen new pieces of training content added this month. Training content from the Security Awareness Company, including Top 5 Phishing Fundamentals, is available at the Diamond subscription level.

Popcorn Training – World Wild Web: Acceptable Use of Devices

Countless threats are trying to find new ways of compromising your devices. That is why your organization has such strict policies in place about what work devices can and cannot be used for. In this training module, you will learn how to browse the internet safely and protect yourself against cybercrime.

Twenty-four new pieces of training content added this month. Training content from Popcorn Training, including World Wild Web: Acceptable Use of Devices, is available at the Diamond subscription level.

How To Behave: Protecting Sensitive Information

This Mobile-First module is key for improving security practices in your organization. Your users will learn about the various types of sensitive data and how to keep them secure. At the end, your users will be better equipped to protect sensitive information, reduce risk and prevent cybersecurity breaches.

One new piece of training content added this month. Training content from El Pescador, including How To Behave: Protecting Sensitive Information, is available at the Diamond subscription level.

KnowBe4 – 2024 Common Threats

•In this training module, you will learn some of the latest ways that cybercriminals are targeting you and your organization using social engineering. Kevin Mitnick demonstrates a new spin on a common email trick to show how cybercriminals get information from you and then access your computer and the organization's network.

•Fifteen new pieces of training content added this month. 2024 Common Threats is available across Gold, Platinum and Diamond subscription levels.

KnowBe4 – 2024 Kevin Mitnick Security Awareness Training

Cybercriminals are indiscriminate in their pursuit of targets, and with this 15-minute training, you'll gain insights into the tools and tactics they use. You will learn to recognize the warning signs of cyberattacks and understand the best actions to take when faced with such situations. You will learn how to strengthen your defense against potential threats and ensure a safer digital environment for you and your organization. You'll also get to see the inner workings of a cyberattack with a demonstration from legendary security consultant Kevin Mitnick.

Five new pieces of training content added this month. 2024 Kevin Mitnick Security Awareness Training - 15 minutes is available across all subscription levels.

The Security Awareness Company – Dark Patterns and Deceptive Design

Dark patterns are a common occurrence in user interfaces that are designed to manipulate your user's actions. This short, Mobile-First module explores how dark patterns work, why they can be dangerous and what people can do to protect themselves.

Three new pieces of training content added this month. Training content from the Security Awareness Company, including Dark Patterns and Deceptive Design, is available at the Diamond subscription level.

El Pescador – How To Behave: Detecting Suspicious Activity

This Mobile-First module introduces a method for recognizing and dealing with suspicious activity related to information security and data protection. You will learn how to recognize suspicious behavior across email, social media, networks and systems, mobile devices, and cloud environments. Hone the skills needed for addressing suspicious activity effectively and protecting your organization's sensitive information and systems.

One new piece of training content added this month. Training content from El Pescador, including How To Behave: Detecting Suspicious Activity, is available at the Diamond subscription level.

El Pescador – How To Behave: Detecting Suspicious Activity

This Mobile-First module introduces a method for recognizing and dealing with suspicious activity related to information security and data protection. You will learn how to recognize suspicious behavior across email, social media, networks and systems, mobile devices, and cloud environments. Hone the skills needed for addressing suspicious activity effectively and protecting your organization's sensitive information and systems.

One new piece of training content added this month. Training content from El Pescador, including How To Behave: Detecting Suspicious Activity, is available at the Diamond subscription level.

MediaPRO – Security Awareness for Executives

Executives will learn the importance of data security at a higher level within the organization. This training module discusses how to safely use work devices remotely, the risks of using personal devices, how to create a strong password, what social engineering is and data security best practices.

Three new pieces of training content added this month. Training content from MediaPRO, including Security Awareness for Executives, is available at the Diamond subscription level.

Log into your KMSAT console and search for these course titles in your ModStore. You can preview this content and select what works best for your organization.

KnowBe4 Conference

Exciting news – registration for KB4-CON is now open! Join us **March 4-6, 2024** at the beautiful Gaylord Palms Resort and Convention Center in sunny **Orlando, Florida.**

KB4-CON is KnowBe4’s premier annual conference, bringing together KnowBe4 customers, channel partners, security advocates, keynote speakers, and industry professionals for three days of learning, sharing, and growing your cybersecurity knowledge.

What can you expect at KB4-CON 2024?
Get ready for an amplified experience with more breakout sessions, providing you an opportunity to delve deeper into the world of cybersecurity. Plus, we've extended KB4 Lab hours, fostering connections with KnowBe4 product experts and exhibitors. It's more than just sessions and keynotes; we're crafting an exciting journey into the cutting-edge world where cybersecurity and AI converge.

The best part? **Take advantage of the early bird pricing, available through December 15, 2023. Be part of the journey for just $129!**

What are you waiting for? Register today!

Don’t like clicking on redirected links? Copy and paste this URL into your browser:
https://knowbe4.cventevents.com/owbn8D?RefId=emregocust

Training Deadlines:

- All training 2023 training must be completed by December 31st.

- Annual Cybersecurity Awareness Training Verification Compliance Form must be submitted to CSRM on or before January 31. 2024. This form can be found in SEC527 and may be sent via email or completed online in Archer.

UPCOMING EVENTS

The next scheduled IS Orientation:

November 16, 2023

1p – 3p (virtual)

Presenters: Erica Bland
Renea Dickerson
Tina Gaines

https://covaconf.webex.com/weblink/register/r7838d02d183f27b2d9d5a3d3a2a07c51

ISOAG Meeting:

December 3, 2023

1p – 3p (virtual)

Presenters: TBD

https://covaconf.webex.com/weblink/register/re26598060b580da703f31a9587dff931

MEETING ADJOURNED

VIRGINIA IT AGENCY