Technical Implementation of Assessment & Authorization in the NISP

Student Guide

May 2024

Center for Development of Security Excellence

Lesson 1: Course Overview

Introduction

Welcome

Welcome to the Technical Implementation of Assessment and Authorization, or A&A, in the NISP Course. The purpose of this course is to provide you with the knowledge needed to assess information systems for authorization under the National Industrial Security Program, or NISP.

Information

Use the buttons to review the hardware and software requirements, download the student guide, and review a tutorial for navigating this course.

Course Scenario

Meet Monique, an Information Systems Security Manager, or ISSM, at Lockhardt, Inc. Lockhardt is a new company that has recently won a new government contract. The company is geographically dispersed with several different environments. Monique has been working on preparing Lockhardt's information system for authorization under the NISP.

She has guided Lockhardt through steps 0-3 of the Assessment and Authorization process, which are (0) Prepare (1) Categorize, (2) Select, and (3) Implement.

Now she will be using the Security Content Automation Protocol, or SCAP, Compliance Checker and Security Technical Implementation Guide, or STIG Viewer, to self-assess Lockhardt's system security controls so that Lockhardt will be prepared for authorization.

Course Objectives

Here are the course objectives. Review them and select "Next" when you're finished.

- Distinguish the steps to install and properly configure the SCAP Compliance Checker and STIG Viewer
- Perform the steps used to conduct a SCAP scan to assess risks to information systems
- Identify mitigation strategies of a known vulnerability
- Identify unmitigated vulnerabilities required to be included in a Plan of Actions & Milestones (POA&M)

Lesson 2: Obtaining the SCAP Compliance Checker and STIG Viewer

Lesson Introduction

To begin a self-assessment for Lockhardt, Inc., Monique must obtain two tools: a SCAP Compliance Checker and a STIG viewer. This lesson will explain the purpose of these tools and how to obtain them.

Lesson Objectives

Here are the lesson objectives. Review them and select "Next" to continue.

- Identify the purpose of the SCAP Compliance Checker and how to obtain it
- Identify the purpose of the STIG Viewer and how to obtain it

Introduction to the SCAP Compliance Checker

Monique begins the self-assessment process by obtaining the SCAP Compliance Checker. The SCAP Compliance Checker is an automated vulnerability scanning tool. It leverages the Defense Information Systems Agency, or DISA, Security Technical Implementation Guides, or STIGs, and Operating System-specific baselines to analyze and report on the security configuration of an information system.

The SCAP Compliance Checker is not the only method of scanning for vulnerabilities. Other DOD-approved tools authorized by your command may be available.

It is important to note that administrative privileges on the machine to be scanned are required to install the SCAP Compliance Checker application and to run scans.

Installing the SCAP Compliance Checker

The SCAP Compliance Checker may be obtained from the DOD CYBER EXCHANGE PUBLIC. You will need to know the operating system of the machine you are scanning. In this demonstration, we are using Windows 11. Select the appropriate SCAP Compliance Checker for your operating system from the list to start the download of the ZIP file.

- Open an internet browser.
- Click in the address bar.
- Navigate to https://public.cyber.mil/stigs/scap/.
- Select the appropriate SCAP Compliance Checker for your operating system.

You will need to know the operating system of the machine you are scanning. In this demonstration, we are using Windows 11.

- Select the appropriate SCAP Compliance Checker for your operating system from the list to start the download of the ZIP file.

Knowledge Check 2.1

Answer this question.

Which of the following do you need to know before installing the SCAP Compliance Checker?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ The date your system was last scanned

○ The Operating System's baseline results

○ The operating system of the machine you're scanning

Downloading the Baseline

Next, Monique will need to download the appropriate baseline, also known as a benchmark. The baseline is used to generate checklists used for vulnerability assessments. They are version-specific, unclassified, and non-PKI controlled.

Monique returns to the DOD CYBER EXCHANGE page where she found the SCAP Compliance Checker. She navigates to the Microsoft Windows 11 STIG Benchmark and downloads the baseline.

- Open an internet browser.
- Click in the browser address bar.
- Go to DISA's Information Assurance Support Environment (IASE) the DOD CYBER EXCHANGE PUBLIC at https://public.cyber.mil/stigs/scap/.
- Select the appropriate operating system.
- Select the most recent STIG Benchmark.
- Save the ZIP file to your desktop.

Introduction to the STIG Viewer

Monique has successfully obtained the SCAP Compliance Checker and baseline, which she will use to analyze and report on the security configuration of her information system. To view the compliance of the system's security settings, she needs another tool: the STIG Viewer.

The STIG Viewer is an unclassified, non-PKI controlled tool. It can be downloaded from the DOD CYBER EXCHANGE PUBLIC website. It is a java-based application, requires no installation, and runs as a Java applet. Administrators should be aware that Java tends to flag vulnerability/antivirus suites. If Java isn't installed, an error will appear.

The STIG Viewer is used in conjunction with the SCAP Compliance Checker scan results in order to view the compliance status of the system's security settings.

Other DOD-approved tools are available.

Downloading the STIG Viewer

To download the STIG Viewer, go to the DOD CYBER EXCHANGE PUBLIC. Look for the "STIG Viewer" page. Scroll to the STIG Viewer section and select the most recent version. Save the file to your desktop.

To download the STIG Viewer, go to DISA's IASE webpage.

- Open an internet browser.
- Click in the browser address bar.
- Enter the URL as shown: https://public.cyber.mil/stigs/downloads/?_dl_facet_stigs=stig-viewing.
- Scroll to the section titled STIG Viewer.
- Select the most current version.
- Save to your Desktop.

Downloading the STIGs

Next, Monique will need to download the appropriate STIGs.

STIGs are Security Technical Implementation Guides – Configuration Standards. The STIGs are based on DOD policy and security controls and contain technical guidance to "lock down" information systems and software that might otherwise be vulnerable to a malicious computer attack.

- Open an internet browser.
- Click in the browser address bar.
- Enter the address for the DOD CYBER EXCHANGE portal: https://public.cyber.mil/stigs/downloads/.

- The STIGs are organized by operating system on the DOD CYBER EXCHANGE portal. Select the appropriate operating system.
- Select Windows 11.

Your desktop is now equipped with the SCAP Compliance Checker, STIG Viewer, and STIGs.

Knowledge Check 2.2

True or False?

STIG Viewers are non-PKI controlled.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ True

○ False

Knowledge Check 2.3

Which of the following phrases applies to the SCAP Compliance Checker?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

□ Administrative privileges required

□ Java-based

□ Shows compliance status of an IS

□ Analyzes and reports the security configuration of an IS

Knowledge Check 2.4

Which of the following phrases applies to the STIG Viewer?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

□ Java-based

□ Administrative privileges required

□ Shows compliance status of an IS

□ Installation not required

Knowledge Check 2.5

Which of the following phrases applies to the SCAP Compliance Checker and the STIG Viewer?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ Installation not required

○ Java-based

○ Available at DISA’s IASE the DOD CYBER EXCHANGE website

Lesson Summary

In this lesson, you learned about two tools essential to the self-assessment process: The SCAP Compliance Checker and the STIG Viewer. You are now ready to follow Monique as she conducts a system scan.

Lesson 3: Running a SCAP Scan

Lesson Introduction

Monique will now initiate a SCAP scan. Time will vary based on network speed, but it may take about 3 minutes to run the scan. Before doing the scan, let's see how to select and save appropriate configuration settings.

Lesson Objectives

Here are the lesson objectives. Review them and select "Next" to continue.

- Select and save appropriate configuration settings for the SCAP Compliance Checker
- Describe the process used to run a SCAP scan and save results

Initiate a Scan

To initiate a scan, Monique opens the SCAP Compliance Checker Application.

During this lesson, you will be performing the same actions as Monique. Follow the audio cues and use your mouse to find the messages in blue boxes that will help you complete the process.

She'll need to select the appropriate baseline. In her case, it is the Microsoft Windows 11 STIG Benchmark - Ver 1, Rel 1. She will check the box to select the file, and then left click on the entry to select the Mission Assurance Category, or MAC level. Generally, an ISSM should select MAC-3 Classified.

To initiate the scan, Monique selects the SCAP Compliance Checker icon.

- Double-click the "SCAP Compliance Checker (SCC) 4.2" shortcut icon.
- In the window that appears, navigate to the benchmark that you previously downloaded.
- You'll need to select the appropriate baseline. For this demonstration, it is the Microsoft Windows 11 STIG Benchmark - Ver 1, Rel 1.
- Select the Open button.
- Select the Profile dropdown menu to select the Mission Assurance Category, or MAC level.
- Generally, an ISSM should select MAC-3 Classified. MAC-3_Classified is the default configuration setting for systems under the NISP.
- Select MAC-3_Classified.
- To initiate the scan, choose a scan type from the Scan Type dropdown menu.

- Select Local Scan from the Scan Type dropdown menu.
- Select “Start Scan” to initiate the scan.

Knowledge Check 3.1

Answer this question.

Which of the following is a suggested configuration setting?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ MAC-1

○ MAC-2

○ MAC-3

View All Settings Report and Non-Compliance Report

After Monique completes the SCAP scan, she can access two different generated reports. One report is the largest html file, the All Settings Report. The other is the smaller html file, which is the Non-Compliance Report.

- Once the scan has completed, she selects View Results.
- Next, she selects the largest HTML file, which is titled All Settings Report.
- Monique reads through the report to gain familiarity of it, but the results shown in this report do not impact the scan.
- To exit, close the report.

When Monique selects the smaller HTML file, she has access to a Non-Compliance Report. This report lists open vulnerabilities.

- Double-click the smaller size HTML file, which will be titled “Non-Compliance Report.”
- This is a report that shows only open vulnerabilities.

View Results in STIG Viewer

Next, Monique is ready to review the SCAP scan results in the STIG Viewer.

She opens the STIG Viewer and selects the imported STIG profile. She selects the gear icon and Create checklist from STIG.

- To view the results, first open the STIG Viewer.
- Select the STIG Viewer.

- Select Open STIG.

Monique opens the STIG Viewer and selects the imported STIG profile. She selects the gear icon and selects ‘Create checklist from STIG.’

- Double-click the imported STIG profile to load the STIG.
- Select the gear icon.
- Select Create checklist from STIG.

Next, she selects Import, and then Import XCCDF Results. She returns to her desktop one more time and selects the Results file and selects Open.

- Select Import.
- Select Import XCCDF Results.
- Double-click the desktop.
- Double-click the XCCDF file.
- Select Complete Import.

Knowledge Check 3.2

Answer this question.

Where are the SCAP scan results stored in human-readable form?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ ZIP folder

○ HTML file

○ XCCDF file

Knowledge Check 3.3

Answer this question.

What is the purpose of initiating a SCAP scan?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ Assess risks to information systems

○ Identify vulnerabilities needing remediation

○ Preparation for assessment by an ISSP/SCA

○ All of the above

Lesson Summary

In this lesson, you learned how to conduct a SCAP scan and import the results into the STIG Viewer.

You are now ready to take a closer look at the results in the STIG Viewer.

Lesson 4: Assessing and Remediating Vulnerabilities

Lesson Introduction

Narrator: Franklin, the Facility Security Officer (FSO) at Lockhardt, Inc., has stopped by to discuss the SCAP scan with Monique.

Franklin: How are you doing, Monique? Are you having success with the SCAP Compliance Checker?

Monique: Yes, I've gotten it to run two reports, and now I'm ready to have a look at the results in the STIG Viewer.

Franklin: The STIG Viewer?

Monique: Yes, as part of the automated approach we now have in the Risk Management Framework, or RMF, I imported the STIGs, or Security Technical Implementation Guides, specific to our system into this STIG Viewer in the form of a checklist. The STIG Viewer will now compare our settings with the checklist and identify any vulnerabilities we may need to address.

Franklin: I'd like to see the results. Could I have a look?

Monique: Sure, please join me. I'll walk you through the results in the STIG Viewer.

Narrator: The STIG Viewer will provide Lockhardt, Inc. not only with a list of vulnerabilities, but also suggestions for fixing them.

Lesson Objectives

Here are the lesson objectives. Review them and select "Next" to continue.

- Identify categories of vulnerabilities
- Compare scan results to the System Security Plan (SSP) to identify vulnerabilities

Results Overview

Monique: Here are the results in the STIG Viewer. We can see from looking at the caption that there are 121 open findings, 87 findings that were closed, or not vulnerabilities, and 1 that was not reviewed.

Franklin: That looks like a lot of open findings!

Monique: Yes, but some of them may actually not be vulnerabilities. The STIG Viewer assists us in sorting through them and identifying any that need remediation. You'll also see that 1 finding was not reviewed. This is likely a manual check. These findings can't be assessed automatically and must be reviewed manually. The STIGs also cover managerial and administrative checks as well.

Franklin: What are the CAT tabs?

Monique: These are different levels of severity. Level 1 is the most severe and Level 3 is the least severe. The NISP does not require corrective actions for each of these levels, but best industry practices recommend we mitigate CAT 1 findings first. I'll select CAT 1 and have a look at the results.

Interpreting the Results

Monique: Besides seeing the results in the Results section, we can also see them color coded in the left column. A red exclamation point indicates Open, a green checkmark is Not a Finding, and a black square is Not Reviewed. I'll select one of the open findings. It is V-253388, Autoplay, which means that a workstation has Autoplay enabled. If a CD were inserted and autorun was enabled, then someone from outside the network may be able to access information they shouldn't.

The middle column provides valuable details related to the findings. There is a Discussion section that helps us understand the potential vulnerability exploit. In this case, it is telling us that having Autoplay enabled on a system may introduce malicious code to a system.

Next there is a Check Text section to show us if the system is properly configured. The description here will tell us if we may need to change the registry, add a registry key, or modify the registry hive. In this case, we'll need to review the installed services or registry settings.

And here is likely the most valuable section, the Fix Text section. It provides guidance in how to resolve the issue. As you can see, we'll need to turn off autoplay.

In addition, the CCI section identifies Control Correlation Identifiers in the NIST SP 800-53.

Knowledge Check 4.1

Answer this question.

Which findings are most severe?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ CAT 1

○ CAT 2

○ CAT 3

Judging Open Findings

Franklin: It's great to see there are fixes for our open findings. Looks like you will be working on mitigating these for the next few days.

Monique: Yes, I have some work to do, but some of the findings that are categorized as open may be false positives. For example, this finding, V-253445, requiring a warning banner when logging in, is categorized as open because the specialized system doesn't have user interface, as cited in our System Security Plan, or SSP and associated security controls.

Franklin: I see. The SCAP Compliance Checker is a powerful tool, but your knowledge as an ISSM is needed to truly determine the criticality of these findings.

Knowledge Check 4.2

True or False?

The SCAP Compliance Checker is the best judge of the criticality of an open finding.

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ True

○ False

Knowledge Check 4.3

Answer this question.

Do all open results from the SCAP scan require controls?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ Yes, and these are listed in the "Fix Text" tab of the STIG Viewer

○ No, and the ISSM can reference the SSP for guidance on findings requiring controls

Lesson Summary

In this lesson, you learned how to interpret the results provided in the STIG Viewer by identifying categories of vulnerabilities and comparing the results to the System Security

Plan. In the next lesson, we will discuss how to document vulnerabilities that need corrective actions before they can be resolved.

Lesson 5: Documenting Vulnerabilities

Lesson Introduction

During Monique's evaluation of the SCAP Compliance Checker results, she identified some vulnerabilities needing corrective actions. As part of the self-inspection process, she is required to document these vulnerabilities in a Plan of Action and Milestones, or POA&M. This lesson will further explain the purpose of the POA&M and how to use it.

Here are the lesson objectives. Review them and select "Next" to continue.

Lesson Objectives

- Identify the purpose of a POA&M
- Describe details expected to be included in a POA&M
- Explain the procedure for using a POA&M, including who creates the plan, who compiles results in a SSP, and who monitors the plan

Pretest your Knowledge

How much do you already know about POA&Ms? Answer this question to test your knowledge.

Which of the following describe the purpose of the POA&M?

Select all that apply.

☐ The POA&M is a report prioritizing corrective actions

☐ POA&Ms are submitted early in the RMF process to inform the Authorizing Official (AO) of vulnerabilities

☐ The POA&M is used to monitor progress on mitigating vulnerabilities

☐ The POA&M is maintained as part of the Security Authorization Package

☐ POA&Ms are updated approximately once per year

Pretest Answer

Which of the following describe the purpose of the POA&M?

- ☑ The POA&M is a report prioritizing corrective actions
- □ POA&Ms are submitted early in the RMF process to inform the Authorizing Official (AO) of vulnerabilities
- ☑ The POA&M is used to monitor progress on mitigating vulnerabilities
- ☑ The POA&M is maintained as part of the Security Authorization Package
- □ POA&Ms are updated approximately once per year

Feedback: *POA&Ms are not submitted early in the RMF process to inform the Authorizing Official (AO) of vulnerabilities. Instead they are used by the AO to monitor progress in correcting weaknesses. POA&Ms are living documents that are maintained throughout the system lifecycle.*

Purpose of the POA&M

How did you do? As you may have already known or just learned, one of the most important purposes of a POA&M is to monitor the progress of correcting security vulnerabilities. To achieve this purpose, the POA&M is a living document that is maintained throughout the system life cycle. It is used by the Information System Security Manager, or ISSM, to monitor progress in correcting weaknesses and is maintained as part of the Security Authorization Package. POA&Ms are required for a new system, a system undergoing recertification, 3rd party inspection, or self-inspection.

Unmitigated Vulnerabilities to be included in the POA&M

Listings in the POA&M should be unmitigated vulnerabilities. Examples include an outdated patch, an incorrect version of Java, a misconfigured security setting, or a deviation from DCSA M-L-L Baseline due to data owner (customer) requirements.

Until these listings are mitigated, their status is recorded in the open findings section of the POA&M and continuously monitored.

How to Use a POA&M Template in NISP eMASS

Monique will be using a template to assist her in creating a POA&M. This template resides in the NISP Enterprise Mission Assurance Support Service, or eMASS.

The eMASS requires a POA&M for Non-Compliant, or NC, controls. A POA&M Template is available in the “Help” section of eMASS.

The eMASS allows users to create and edit POA&M items, add additional milestone and completion dates, review and modify the POA&M, provide the Authorizing Official, or AO with risk assessments, and ensure transparency to corrective actions and mitigation efforts.

A POA&M item is required any time a vulnerability is identified. POA&M items that are corrected quickly should still be documented in order to capture all relevant information and track the progress of corrective actions. When documenting a POA&M item, users must address all required fields in eMASS.

Let's look at what's required when creating and editing POA&M items in eMASS. The overall intent is to accurately document the critical aspects of the corrective action plan, identify the resources required for remediation, assess and analyze associated risk, and provide a scheduled completion date.

It is important to understand that the POA&M is a living document. If anything changes—such as the schedule, timeline, or milestones—make sure you come back and update it.

Document POA&M milestones and completion dates. Enter specific high-level steps to be executed in mitigating the weaknesses and the estimated completion date for each step.

Describe the vulnerability identified during the assessment process. If annotating a system vulnerability is determined to be classified as per the Security Classification Guidance, or SCG, indicate in eMASS that details will be maintained on site.

While a package is being processed past the SCA Role to the Team Lead Role in the "Package Approval Chain", or PAC, a snapshot is created, and all POA&M items (both control-level and system-level) will be locked. Users can view details of locked POA&M items but can only edit the risk analysis fields.

Completion status. Users are responsible for updating a POA&M "Completion Status" based on actions taken against a control (e.g., control status change). The eMASS users can choose to view the POA&M items in a "Table View" or "Card View" format. Reference the eMASS User Guide in the Plan of Action and Milestones Section.

FAQs: Using and Monitoring the POA&M

Franklin: Monique, could you tell me more about the POA&M you're creating?

Monique: Sure, Franklin. As an ISSM, my role is to create the POA&M as part of the SSP. I use the POA&M to communicate issues we cannot resolve to the ISSP or SCA. The ISSP or SCA will evaluate the POA&M and determine next steps. I'll monitor it as we take steps to mitigate our vulnerabilities.

Franklin: Do you create the POA&M on your own, or do you need input from others?

Monique: I work with the ISO, PM, or SM to enter some information into the POA&M such as noncompliant security controls, controls that are not applicable, remediation tasks, required resources, milestones and completion dates, and inherited vulnerabilities. The ISO, PM, or SM will initiate corrective actions.

Franklin: Will the ISSP/SCA approve the POA&M?

Monique: No, as part of the RMF process, ultimately, the AO approves or rejects elements of the POA&M.

Franklin: Thank you, Monique. This is much clearer to me now.

Knowledge Check 5.1

Answer this question.

Which of the following is a responsibility of an ISSM?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ Monitors progress

○ Evaluates vulnerabilities

○ Approves or rejects

○ Initiates corrective actions

Knowledge Check 5.2

Which of the following is a responsibility of an ISSP/SCA?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ Monitors progress

○ Evaluates vulnerabilities

○ Approves or rejects

○ Initiates corrective actions

Knowledge Check 5.3

Which of the following is a responsibility of an AO?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ Monitors progress

○ Evaluates vulnerabilities

○ Approves or rejects

○ Initiates corrective actions

Knowledge Check 5.4

Which of the following is a responsibility of an ISO or PM/SM?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ Monitors progress

○ Evaluates vulnerabilities

○ Approves or rejects

○ Initiates corrective actions

Knowledge Check 5.5

Answer this question.

What is the purpose of a POA&M?

Select the best response. Then check your answers in the Answer Key at the end of this Student Guide.

○ Document the RMF process

○ Monitor progress in mitigating vulnerabilities

○ Communicate vulnerabilities to the FSO

Lesson Summary

In this lesson, you learned the ISSM's responsibilities for creating and monitoring a POA&M, the end product of the SCAP scan and STIG comparison. This living document will aid you in mitigating your vulnerabilities and documenting them for the AO.

Lesson 6: Course Conclusion

Course Review

Congratulations. You have completed the Technical Implementation of Assessment & Authorization in the NISP course.

You should now be able to perform all of the listed activities.

This course provided you with instruction needed to use the SCAP Compliance Checker and STIG Viewer to identify vulnerabilities and document unmitigated vulnerabilities on a POA&M. If you are an ISSM like Monique, you now have more tools to prepare for authorization.

To review the course, access the Student Guide.

To receive credit for this course, you must take the course examination. Follow the instructions on screen to access the online exam.

Course Objectives

- Distinguish the steps to install and properly configure the SCAP Compliance Checker and STIG Viewer
- Perform the steps used to conduct a SCAP scan to assess risks to information systems
- Identify mitigation strategies of a known vulnerability
- Identify unmitigated vulnerabilities required to be included in a Plan of Actions & Milestones (POA&M)

Appendix A: Answer Key

Lesson 2 Knowledge Checks

Knowledge Check 2.1

Which of the following do you need to know before installing the SCAP Compliance Checker?

○ The date your system was last scanned

○ The Operating System's baseline results

⦿ The operating system of the machine you're scanning

Feedback*: You need to know the operating system of the machine you're scanning before installing the SCAP Compliance Checker.*

Knowledge Check 2.2

True or False: STIG Viewers are non-PKI controlled.

⦿ True

○ False

Feedback*: STIG Viewers are non-PKI controlled.*

Knowledge Check 2.3

Which of the following phrases applies to the SCAP Compliance Checker?

☑ Administrative privileges required

□ Java-based

□ Shows compliance status of an IS

☑ Analyzes and reports the security configuration of an IS

Knowledge Check 2.4

Which of the following phrases applies to the STIG Viewer?

☑ Java-based

□ Administrative privileges required

☑ Shows compliance status of an IS

☑ Installation not required

Knowledge Check 2.5

Which of the following phrases applies to the SCAP Compliance Checker and the STIG Viewer?

○ Installation not required

○ Java-based

⦿ Available at DISA’s IASE the DOD CYBER EXCHANGE website

Lesson 3 Knowledge Checks

Knowledge Check 3.1

Which of the following is a suggested configuration setting?

○ MAC-1

○ MAC-2

⦿ MAC-3

***Feedback**: MAC-3 is the default configuration setting for systems under the NISP.*

Knowledge Check 3.2

Where are the SCAP scan results stored in human-readable form?

○ ZIP folder

○ HTML file

⦿ XCCDF file

***Feedback**: SCAP scan results in human-readable form are stored in an XCCDF file.*

Knowledge Check 3.3

What is the purpose of initiating a SCAP scan?

○ Assess risks to information systems

○ Identify vulnerabilities needing remediation

○ Preparation for assessment by an ISSP/SCA

⦿ All of the above

***Feedback**: The SCAP scan is used to prepare for assessment by an ISSP/SCA, assess risks to information systems, and identify vulnerabilities needing remediation.*

Lesson 4 Knowledge Checks

Knowledge Check 4.1

Which findings are most severe?

◉ CAT 1

○ CAT 2

○ CAT 3

***Feedback**: CAT 1 findings are **most** severe.*

Knowledge Check 4.2

The SCAP Compliance Checker is the best judge of the criticality of an open finding.

○ True

◉ False

***Feedback**: The ISSM is the best judge of the criticality of an open finding.*

Knowledge Check 4.3

Do all open results from the SCAP scan require controls?

○ Yes, and these are listed in the “Fix Text” tab of the STIG Viewer

◉ No, and the ISSM can reference the SSP for guidance on findings requiring controls

***Feedback**: Not all open results require controls. Some open results may be false positives or require manual checks.*

Lesson 5 Knowledge Checks

Knowledge Check 5.1

Which of the following is a responsibility of an ISSM?

◉ Monitors progress

○ Evaluates vulnerabilities

○ Approves or rejects

○ Initiates corrective actions

***Feedback**: The responsibility of an ISSM is to monitor progress.*

Knowledge Check 5.2

Which of the following is a responsibility of an ISSP/SCA?

○ Monitors progress

◉ Evaluates vulnerabilities

○ Approves or rejects

○ Initiates corrective actions

***Feedback**: The responsibility of an ISSP/SCA is to evaluate vulnerabilities.*

Knowledge Check 5.3

Which of the following is a responsibility of an AO?

○ Monitors progress

○ Evaluates vulnerabilities

◉ Approves or rejects

○ Initiates corrective actions

***Feedback**: The responsibility of an AO is to approve or reject.*

Knowledge Check 5.4

Which of the following is a responsibility of an ISO or PM/SM?

○ Monitors progress

○ Evaluates vulnerabilities

○ Approves or rejects

◉ Initiates corrective actions

***Feedback**: The responsibility of an ISO or PM/SM is to initiate corrective actions.*

Knowledge Check 5.5

What is the purpose of a POA&M?

○ Document the RMF process

◉ Monitor progress in mitigating vulnerabilities

○ Communicate vulnerabilities to the FSO

***Feedback**: The purpose of a POA&M is to monitor progress in mitigating vulnerabilities.*