Job Aid: Security Configuration Assessment of Information Systems (IS)

Using this job aid

This job aid provides an overview of the process for assessing the technical security controls and system configuration of contractor information systems (IS) using the Defense Information System Agency (DISA) vulnerability scanning protocols in accordance with the National Industrial Security Program (NISP).

The steps the Information System Security Professional (ISSP), Information System Security Officer (ISSO), or Information System Security Manager (ISSM), if applicable, must follow are:

1. Gather Documentation
2. Install tools and scan system
    - Security Content Automation Protocol (SCAP)
    - Security Technical Implementation Guide (STIG) Viewer
3. Conduct assessment of vulnerabilities
    - IF:
        - ISSO or ISSM: Fix vulnerabilities
        - ISSP: Annotate findings

Gather system documentation

1

This section provides a list of the types of documentation the ISSM/ISSO/ISSP must review to facilitate the assessment. This list is not exhaustive, and not all documents listed may apply to the assessment.

Refer to the Office of the Authorizing Official for more information; see the Technical Assessment Guide specific to the operating system in use.

- Master System Security Plan (MSSP) or System Security Plan (SSP)
- Authorization Letter, if performing a Security Vulnerability Assessment (SVA)
- Information System Profile (IS Profile)
- Hardware and Software Baselines
- Authorized Users List and Signed User Briefings
- Trusted Download Procedures, Briefings, Logs
- System Diagram and/or Network Topology, if applicable
- DD Form 254, Department of Defense Contract Security Classification Specification
- DSS Form 147, Record of Controlled Area
- Memorandum of Understanding (MOU) / Industrial Security Agreement (ISA), if applicable
- Manual Audit Log
- Removable Media Creation Log
- Maintenance Logs
- Sanitization Procedures, if applicable
- Audit Variance / Hibernation Procedures, if applicable
- Threat Data (to determine current threat picture)

Install tools and scan system

2

This section provides a brief description of the tools that must be downloaded to scan information systems for vulnerabilities.

Open example screens showing how to use SCAP tool to scan.

Security Content Automation Protocol (SCAP) Compliance Checker	An automated vulnerability scanning tool that leverages the DISA STIGs and OS specific baselines to analyze and report on the security configuration of an information system Can be obtained in two ways, depending upon the possession of a DoD PKI token: • PKI Enabled: http://iase.disa.mil/stigs/scap/Pages/index.asp • Non-PKI Enabled: http://MAX.gov PDF file containing installation instructions is included within the ZIP file for each Operating System version of the SCAP Compliance Checker
DISA Security Technical Implementation Guidelines (STIG) Viewer	A Java-based application used in conjunction with the SCAP Compliance Checker scans results in order to view the compliance status of the system's security settings. • Unclassified and non-PKI controlled • Access and download at: http://iase.disa.mil/stigs/Pages/stig-viewing-guidance.aspx Requires no installation and runs as a JAVA applet
Operating System (OS) Baselines	The STIG Viewer leverages operating system baselines to generate checklists used for vulnerability assessments. • Version specific; non-PKI controlled • Access and download at: http://iase.disa.mil/stigs/os/Pages/index.aspx
Scan System	*See the Technical Assessment Guide specific to the operating system in use.*

Conduct assessment on vulnerabilities

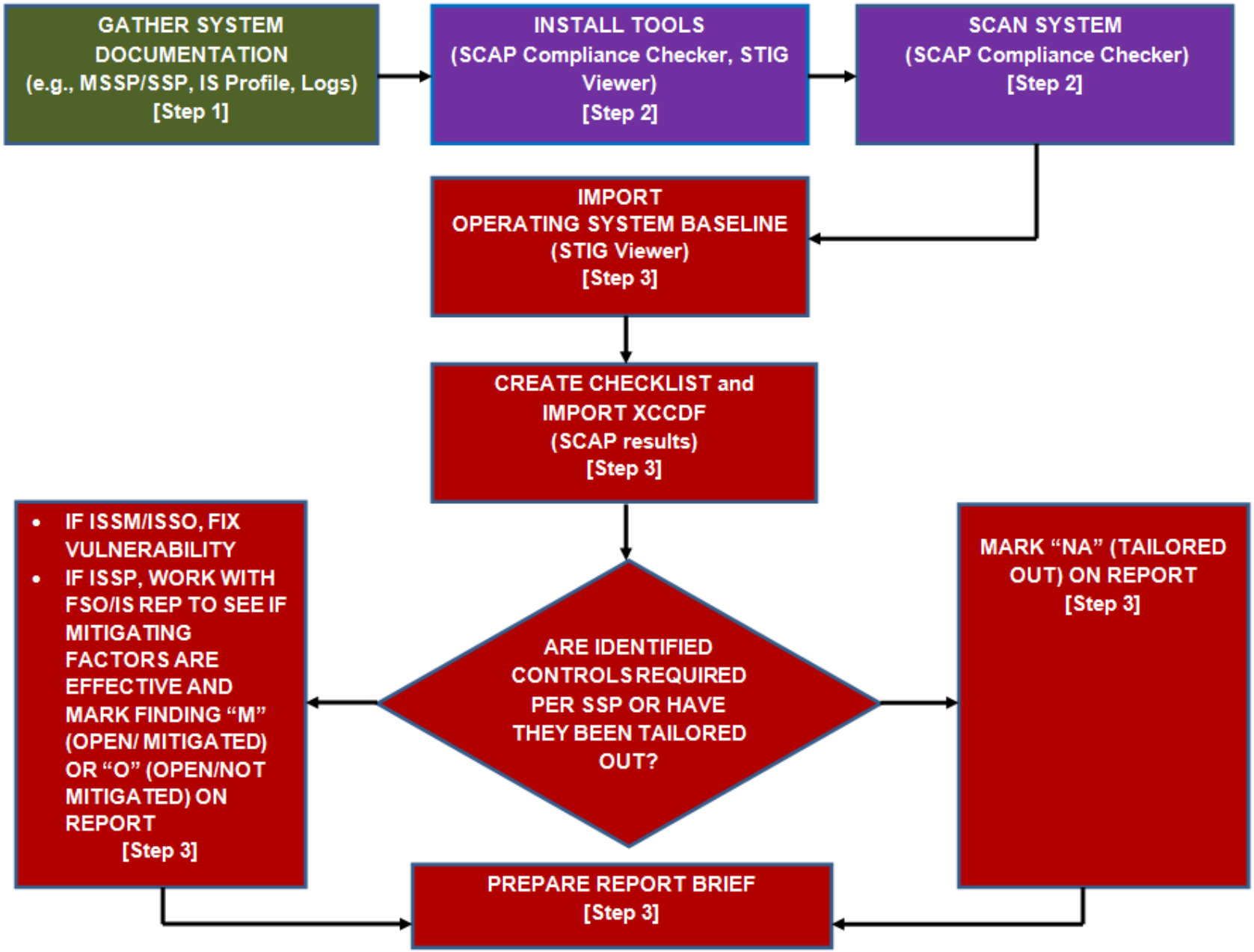
3

This section provides the high level steps the ISSM/ISSO/ISSP must follow upon completion of the vulnerability scan to assess the vulnerabilities in the security configuration of a system.

Open example screens showing how to use STIG Viewer.

1. Open STIG Viewer and import the appropriate STIG baseline
2. Create a checklist from the drop down menu "Checklist" in your STIG Viewer using relevant STIG benchmarks
3. Import XCCDF file and sort by Vulnerability IDs
4. Compare the control ID's on the report to the SSP and other documentation listed above to determine which control ID's are 'required' and which are 'tailored out'
   - Mark the 'tailored out' controls as 'NA' in the report
5. Examine the 'required' control ID's in the report to see if any vulnerabilities exist. For each vulnerability you find:
   - If you are the ISSM or ISSO, fix the vulnerability
   - If you are the ISSP, work with the Facility Security Officer (FSO) and Industrial Security Representative (IS Rep) to determine if mitigating factors are effective based on risk and the specific threat to that network and mark the vulnerability as a 'finding' in the report
     - If acceptable mitigating factors are in place, mark the vulnerability with an 'M' (for Open Vulnerability, Mitigated/Compliant) in the report
     - If acceptable mitigating factors are NOT in place, mark the vulnerability with an 'O' (for Open Vulnerability, Not Mitigated; Non-Compliant) in the report

   Note: CAT levels are not tracked under the Risk Management Framework (RMF) but can be helpful in determining which are more critical for resource allocation and therefore mitigation priority (i.e., CAT I before CAT III).
6. Prepare report brief in accordance with agency or organizational processes


GATHER SYSTEM DOCUMENTATION (e.g., MSSP/SSP, IS Profile, Logs) [Step 1]
INSTALL TOOLS (SCAP Compliance Checker, STIG Viewer) [Step 2]
SCAN SYSTEM (SCAP Compliance Checker) [Step 2]
IMPORT OPERATING SYSTEM BASELINE (STIG Viewer) [Step 3]
CREATE CHECKLIST and IMPORT XCCDF (SCAP results) [Step 3]
ARE IDENTIFIED CONTROLS REQUIRED PER SSP OR HAVE THEY BEEN TAILORED OUT?
IF ISSM/ISSO, FIX VULNERABILITY
IF ISSP, WORK WITH FSO/IS REP TO SEE IF MITIGATING FACTORS ARE EFFECTIVE AND MARK FINDING "M" (OPEN/ MITIGATED) OR "O" (OPEN/NOT MITIGATED) ON REPORT [Step 3]
MARK "NA" (TAILORED OUT) ON REPORT [Step 3]
PREPARE REPORT BRIEF [Step 3]