DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR COMBAT COMMAND
JOINT BASE LANGLEY-EUSTIS VA

17 May 2019

MEMORANDUM FOR ACC SAPF CYBERSECURITY PERSONNEL (ISSMs & ISSOs)

SUBJECT: RMF Plan

Reference: Memorandum for ACC CCs, SAP IT Status and Update, dtd 16 May 2019

1. With respect to the referenced memorandum HQ ACC/A5/8ZXC has developed the RMF plan for workflow of the documentation required to obtain an ATO. This adapt to the SAP AO, SAF/AAZ, requirements for documentation as they change. When changes are received by the MAJCOM from the SAP AO's office the MAJCOM ISSMs will distribute for implementation. This plan outlines the Bodies of Evidence (BoE) required, workflow (i.e. CASTS utilization), and expectations during the review process.

2. BoE Requirements. All documentation shall be completed on the appropriate system for submission.

a. Categorization Memorandum – This document provides a brief description of the mission area being supported by the information system.

b. System Security Plan (SSP) – This document provides a detailed description of the system, mission area, summary of categorization, media handling, users (i.e. general user, privileged users, and DTAs) and location of any reference documents (i.e. MOA/U, IA SOP, and pertainent memorandums). When referencing other documentation the unit must ensure the SCA has access to the documentation.

c. Network Topology – A diagram depicting the overall connectity of the system.

d. Hardware List – The list shall include nomenclature (i.e. desktop, laptop, switch, etc.), make, model, serial number, and room number where the equipment is utilized. If the equipment is 'Deployable' make note in the room number column.

e. Software List – The list shall include Operating System (OS), applications (i.e. Microsoft Office, Adobe, CD/DVD creation, and etc.), special tools (i.e. ACAS, WireShark, and audit reduction software). Any software that has reached End of Life (EoL) must have a justification for continued use included (i.e. due to mission requirements).

f. Security Control Traceability Matrix (SCTM) – This spreadsheet details the units the controls tha are planned/implement/tailored out system security controls.

g. Vulnerability Scans – The unit will complete the scans and report IAW the CONOPs available via the CASTS library. Consult the the MAJCOM ISSM if there are any questions.

h. Plan of Action & Milestones (POA&M) – This document shall address any deficiencies in the implementation of security controls (i.e. plan to implement DAR, update OS, replace EoL software) and detail an update status. This is a living document that shall be updated throughout the life of the

system. This document is based on the results of the vulnerability scans and the security controls in the SCTM.

i. Risk Assessment Report – This document provides a description of the overall environment where the systems must operates and identifies risks/vulnerabilities to the system associated with the operational environment and mission area.

j. Continuous Monitoring Strategy (CONMON) – The baseline template will be provided by the MAJCOM SCA; then based upon the assessment of the system, updates will be due at regular intervals.

k. The Security Assessment Report (SAR) – This document is produced by the SCA and copy will be provided to the unit.

l. Templates for all documentation is located in CASTS.

3. WorkFlow.

a. All documentation must be submitted to the MAJCOM ISSMs for review prior to assessment by the SCA.

b. All documentation shall be submitted via CASTS unless the unit does not have access to CASTS. If the unit cannot access CASTS the alternative is CORE File Share. The unit will work with the MAJCOM ISSM to track submissions for SCA review.

c. Complete Package submission – All documentation (items identified in paragraph 2.a through 2.i) shall be zipped in a single file and routed via CASTS to the MAJCOM ISSM for review. The ISSM will download from CASTS, review, document feedback for the unit, and/or present to the SCA for assessment. In the event the zip file cannot be uploaded the unit will work with the MAJCOM ISSM for submission.

d. The naming convention for documents shall follow the format:

"CAF ID #-Document-Date"
Example: CAF_0000-SSP-20190517

e. The Zip file shall follow the naming format:

"CAF ID#-RMF Package-Date"
Example: CAF_0000-RMF Package-20190517

4. RMF packages will be processed however the SAP AO will not distribute ATOs if the unit has not completed a DoD Census and the Win10/DAR spreadsheet with a POAM to meet OS upgrade and encryption for data-at-rest. Questions regarding the processes outlined in this document will be addressed to the MAJCOM ISSMs in writing for a formal response.

DELEON.ADRIAN.F.1080319297 Digitally signed by DELEON.ADRIAN.F.1080319297 Date: 2019.05.17 13:18:34 -04'00'

Adrian F. DeLeon, GS-14, DAF
HQ ACC/A5/8ZXC CAF SAPMO Cyber Security

ACC Package Processing Steps

v1.1
18 December 2019

Contents

Overview

The purpose of this document is to provide steps to conduct a Risk Management Framework (RMF) assessment using the System Assessment Report (SAR) Generator and Risk Assessment Report (RAR) Generator. Risk assessment is employed to guide and inform decision makers on information security risks. The goal is to address the potential adverse impacts to organizational operations and assets, individuals, and other organizations and to identify the risks that are common to the organization's core missions/functions/processes, common infrastructure, support services, and/or information systems.

This document provides step-by-step instructions to utilize the tools to conduct the risk assessment. Prior to assessment, the assessor should ensure the unit provides all required body of evidences (BoEs). This includes, but is not limited to: System Categorization, System Security Plan (SSP), Security Control Traceability Matrix (SCTM), network diagram, hardware/software list, vulnerability scans, and Security Technical Implementation Guide (STIG) applicability list. To complete these steps, assessors will need the Security Control TRExport file, SAR Generator, and RAR Generator.

After completion in the RAR, ACC risk assessors will document the system overview, findings, and recommended ATO length in the Cybersecurity Risk Assessment (CRA) document to inform leadership and decision makers the risk associated with the system. Risk assessors will also complete the SAF AAZ SAR template for the system. At this point, the risk assessors should also generate the POA&M from the RAR, and send it to the unit ISSOs to complete.

HQ ACC A5/8Z plans to update the Latest STIGs file quarterly. Units may either download the file or create their own. The Latest STIGs file is a file that includes all vulnerability IDs in every STIG. If applicable, start with creating the latest STIG listing. DISA releases updated STIGs on a quarterly basis. For the schedule, refer to: https://cyber.mil/stigs/release-schedule/.

Creating Latest STIG Spreadsheet (if applicable)

HQ ACC A5/8Z plans to update the Latest STIGs file quarterly. Units may either download the file or create their own.

Requirement: Vulnerator. Download from https://github.com/Vulnerator/Vulnerator/releases.

Download latest STIG Compilation

1. Browse to: https://cyber.mil/stigs/downloads/?_dl_facet_stigs=stig-compilations
2. Download the FOUO STIG compilation.

Open ALL STIGs in DISA STIG Viewer

1. Open STIG Viewer.
2. File→ Import→ Browse to FOUO_SRG_STIG_Library_x_x.zip, click Open. Do the same with non-FOUO library.
3. Select all STIGs under CK/Name.
4. Checklist→ Create Checklist – Check Marked STIG(s).
5. Save Checklist created.

Open Vulnerator

1. Open Vulnerator.
2. Import CKL→ Import the saved CKL file.
3. Execute.
4. Once file is processed, save the file.

Latest STIG List Creation

1. Open the spreadsheet and go to STIG Details.
2. Delete Columns (column letters may change upon deletion of a column):

   A – IA Control
   I – Risk Factor
   K – Description DO NOT DELETE DESCRIPTION (SEE BELOW)
   L – Check Content
   M – Solution
   N – Host Name
   O – IP Address
   P – Status
   Q – Comments
   R – Finding Details
   S – File Name
   T – Group Name
   U – Review Status
   V - Notes

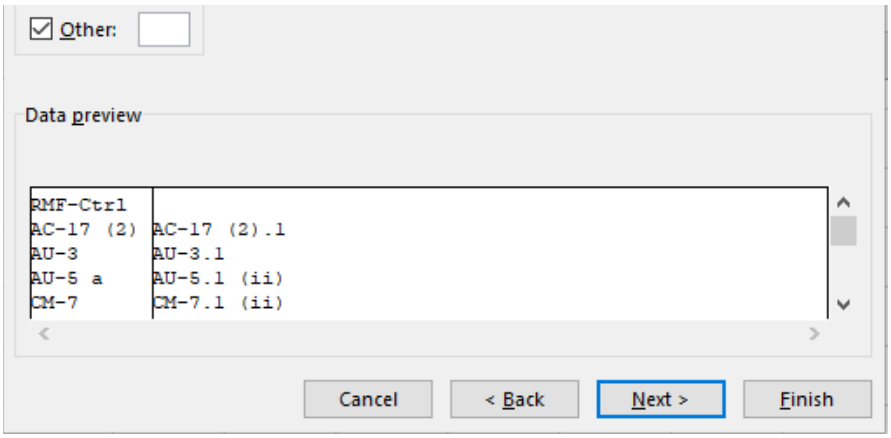
3. Rename and move the fields to the respective columns below (note SV Rule and Rule_ID content):

A	B	C	D	E	F	G	H	I
V-ID	Rule_ID	STIG CAT	RMF-Ctrl	CCI	STIG Title	STIG Description	SV_Rule	STIG File Title
V-67957	AADC-AG-000018	II	AC-17 (2) AC-17 (2).1	CCI-000068	The A10 Networks ADC, when used for TLS encryption and decryption, must be configured to comply with the required TLS settings in NIST SP 800-52.	SP 800-52 provides guidance on using the most secure version and configuration of the TLS/SSL protocol. Using older unauthorized versions or incorrectly configuring protocol negotiation makes the gateway vulnerable to known and unknown attacks which exploit vulnerabilities in this protocol. This requirement applies to TLS gateways (also known as SSL gateways) and is not applicable to VPN devices. Application protocols such as HTTPS and DNSSEC use TLS as the underlying security protocol thus are in scope for this requirement. NIS SP 800-52 provides guidance. SP 800-52 sets TLS version 1.1 as a minimum version, thus all versions of SSL are not allowed (including for client negotiation) either on DoD-only or on public facing servers.	SV-82447r1_rule	A10 Networks ADC ALG Security Technical Implementation Guide STIG

4. Turn on data filter on row 1, and perform the following:
   a. Change all blank CCI's to 'NULL'. (Do not use ')
   b. Change all blank RMF-Ctrl's to 'Orphan'. (Do not use ')(Complete step 5a-c first).
   c. NOTE: Easiest/fastest way to do this, select the range, then type 'Orphan' in one cell, and all other cells are still selected, press Ctrl + Enter.

Not sure why

5. Copy Column D RMF-Ctrl, create a new tab, and paste the column in column A.
   a. Data → Text to Columns → Delimited → Next → Other → Hit Ctrl + J in the box (as seen below) → Next → Finish



   b. Copy column A in the new tab and paste in Column D.
   c. Use the Find and Replace function to change:
      i. Remove the space between the parent control and sub control
         1. Find: ' ('
         2. Replace with: '('
      ii. Remove all roman numbers (i.e., i, ii, iii, iv, v…).
         1. Find: '(i)'
         2. Replace with: ''

Parent control only....

On the New D or back to the new tab????

Column A doesn't have any roman numbers so neither will the New column D. Do we do this on the new tab that has the delimited columns above??

3. Note: there might be a few '(i and ii)', '(iv and v)', '(iii and v)'

iii. Use the filtering option to verify all are removed.

Transfer from NIPR to Assessment System

1. Securely/appropriately transfer spreadsheet to assessment system.
2. Open the Latest_STIGs_Template. Delete the STIG File column.
3. Copy and paste new spreadsheet over the old.

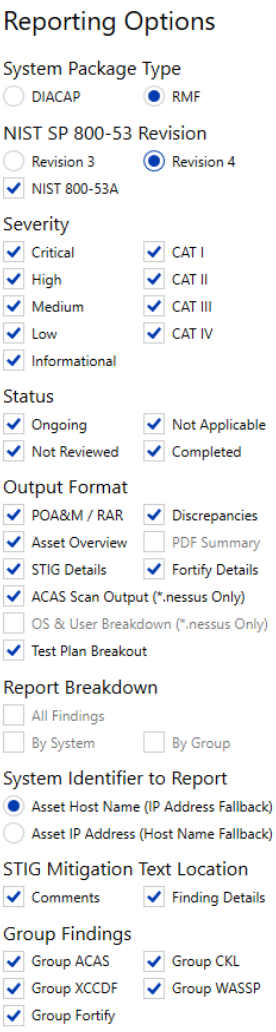
Vulnerator

Purpose: Consolidate raw scan files. Accepted file formats are:

Application Execution	File Type
ACAS	.csv; .nessus
CKL	.ckl
XCCDF	.xml
WASSP	.html
Fortify	.fpr

All scans should be completed within 30 days of submission. Scans are accepted up to 90 days.

1. Open the latest version of the Vulnerator.
    a. If Vulnerator is not on your Victory machine, contact the 53rd CSS.
2. Under NIST SP 800-53 Revision, ensure Revision 4 and NIST 800-53A is selected. No other options should be modified. See below for a screenshot of options selected.
3. In the Application Execution section, import the scan files.
4. Once all files are imported, selected Execute. When completed, status will change to Processed and generate an Excel file.



Populating the "TRExport" Template

1. Open the unit SCTM and a TRExport Template.
    a. Ensure the TRExport Template contains the correct security controls for system categorization (i.e., MLL, MML, etc.).
2. Populate Column M, Date Tested, with the appropriate date format DD-MMM-YY.
3. Populate Column N, Tested By, with the ISSO name.
4. Populate Colum O, Comments, with "Refer to the SCTM."
5. Populate Column L, Compliance Status, with "Compliant", "Non-Compliant", or "Not Applicable".
    a. The compliance status must be copied and pasted into cell. To accomplish this, type "Compliant", "Non-Compliant", or "Not Applicable" in one cell in Column P, copy the cell, and paste in Column O. After completion of one status, filter Column O to show only blanks.
    b. SCTM "Implemented" controls are labeled "Compliant" in TRExport file.
    c. SCTM "Tailored Out" controls are labeled "Not Applicable" in TRExport file.

   d. SCTM “Planned” or “Partial” controls are labeled “Non-Compliant” in TREport file.
   e. Any remaining controls in the SCTM or TREport, mark them “Non-Compliant” in TREport file.
6. Save the file: (Classification) CAF_00XXX_TREport_YYYYMMDD.

SAR Generator

1. Open the SAR Generator file and click on “Clear SAR Data” to ensure document is cleared.
2. Click on “Press Here to Start”.
3. Select the appropriate system categorization level and click OK.
4. Select “Neither” and click OK.
5. Click on “Browse” and navigate to the system TREport file and click Execute.
   a. A popup window, “Please be patient, creating baseline and adding test results to SAR. This will take a couple of minutes!” Click OK.
6. Click on “Browse” and navigate to the blank POA&M file provided and click Execute.
   a. A popup window will provide the POA&M version. Click OK.
   b. A second popup window, “You selected a blank POA&M – only the Test Results will be added to the SAR!” Click OK.
7. Save the file: (Classification) CAF_00XXX_SAR_Generator_YYYYMMDD.

RAR Generator

1. Open the RAR Generator and click on “Clear All Data”.
   a. If a prompt shows, click OK.
2. Click on “Import SAR” and select the saved system SAR.
3. Enter your initials and click OK.
4. Click on “Import Vulnerator Report” in C&C Tab.
5. Browse to the saved Vulnerator Report and click OK. Browse to the Latest STIGs file and click OK.
   a. A popup window, “Scan results have been added and a new Vulnerator tab was added to the RAR. Security controls in red font were determined using BlackBox logic.” Click OK.
6. Save the file: (Classification) CAF_00XXX_RAR_Generator_YYYYMMDD.

Evaluating System RAR

1. In security control family tabs, review:
   a. All Non-Compliant and Not Applicable controls.
   b. All Authorizing Official (AO) or Organizational Risk Tolerance Baseline (ORTB) controls.
      i. Displayed in Column J, Control Type.
   c. All controls with STIG findings.
2. For each control identified, read the CCI Definition and Validation Procedures.

3. Comments will be entered in the control overview box and SME Comments, column O. Refer to the RAR Assessment Comments/Rationale section below.
    a. SME Comments must be before “Raw Risk * “statement. Do NOT delete Raw Risk statement.
4. In Columns T, U, V, the Likelihood, Impact, and overall Risk is assigned. Units may enter numbers 1, 2, 3, 4, 5 to evaluate the likelihood and impact. Do not change the impact without mitigations. Refer to Determining Risk Likelihood and Impact section for information related to evaluating risk.
5. At the end of the assessment, in tab C&C, click on “Create POAM”. This POA&M should be sent to the unit for completion.
    a. ACC risk assessors must complete the CRA and SAR steps below.

Note: To refresh NSA, NSA Mapping, and Risk Matrix Charts, click on Base Control Review and Baseline Control Review Tabs.

Note: All unmapped STIG findings will default to CM-6.1 and/or CM-6.5.

Determining Risk Likelihood and Impact

Determining risk is largely dependent on an understanding by the Security Controls Assessor Representative (SCAR)/SME of the system they are assessing, the requirements of a security control and mitigations provided by the program/system office. Additionally, understanding the ***threat x weakness x likelihood x impact*** will aid the SCAR/SME in accurately determining final system risk.

While the SCAR/SME’s risk determination is largely subjective, using NIST SP 800-30 Risk Management Guide, provides a repeatable process for making risk determinations which aids in reducing some of the subjectivity.

Likelihood of Threat Event Initiation and Occurrence

The “Likelihood of Threat Event Initiation & Occurrence (Adversarial and Non-Adversarial)” table is used to determine the likelihood of external, internal and non-malicious threats occurring.

Qualitative Value	Likelihood of Threat Event Initiation & Occurrence (Adversarial and Non-Adversarial)
Very High	***Confirmed***-Adversary is **almost certain** to initiate the threat event (i.e., adversary capability, intent, and/or targeting are very high); -or- -Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	***Expected***-Adversary is **highly likely** to initiate the threat event (i.e., adversary capability, intent, and/or targeting are high); -or- -Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
Moderate	***Anticipated***-Adversary is **somewhat likely** to initiate the threat event (i.e., adversary capability, intent, and targeting are moderate); -or- -Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
Low	***Predicted***-Adversary is **unlikely** to initiate the threat event (i.e., adversary capability, intent, and/or targeting are low); -or- -Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	***Possible***-Adversary is **highly unlikely** to initiate the threat event (i.e., adversary capability, intent, and/or targeting are very low); -or- -Error, accident, or act of nature **is highly unlikely to occur; or occurs less than once every 10 years.**

Likelihood of Threat Event Resulting in Adverse Impacts

The “Likelihood of Threat Event Resulting in Adverse Impacts” table is used to determine the likelihood of an event resulting in an adverse impact. In conjunction with this table, mitigations can help determine the likelihood of an event having an adverse impact. Some examples of the mitigations used are:

- System connection type
- Ports, protocol and Service (PPS) compliance
- Physical Security
- Strong Boundary Defense
- How well a program implements compensating controls and mitigations

Qualitative Value	Likelihood of Event Resulting in Adverse Impact
Very High	**No security measure** can be identified to remediate the vulnerability; if the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	Compensating controls are in place and at least **minimally effective**; if the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	Relevant security control or other remediation is **partially implemented and somewhat effective**; if the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	Relevant security control or other **remediation is fully implemented and somewhat effective**; if the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	Relevant security control or other **remediation is fully implemented, assessed, and effective**; if the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

Overall Likelihood

The “Likelihood of Threat Event Initiation & Occurrence” determination results and “Likelihood of Event Resulting in Adverse Impact” determination results are cross referenced into the “Overall Likelihood” 5x5 to determine the final likelihood risk determination:

OVERALL LIKELIHOOD					
Likelihood of Threat Event Initiation & Occurrence	**Likelihood of Event Resulting in Adverse Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Overall Impact

The "Impact of Threat Events" table describes the harm that may occur given the potential for threats to exploit vulnerabilities – in other words, overall impact (See below table). The Overall Impact is determined as follows:

- It is the "expected" outcome regardless of likelihood
- In most cases, the RAW Vulnerability Severity value will have the same value as this impact value
- Impact is unchanging. That is, regardless of compliance or mitigations if an event occurred, the overall impact remains the same:

OVERALL IMPACT	
Qualitative Values	**Impact of Threat Events**
Very High	The threat event could be expected to have **multiple severe or catastrophic** adverse effects.
High	The threat event could be expected to have a **severe or catastrophic** adverse effect. For example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	The threat event could be expected to have a **serious** adverse effect. For example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	The threat event could be expected to have a **limited** adverse effect. For example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	The threat event could be expected to have a **negligible** adverse effect.

Overall Risk

"**Overall Likelihood**" determination results plus the "**Overall Impact**" determination results are combined to create the "**Overall Risk**" table (See Below). This table is used to determine final risk for a system/enclave. The Risk Description table describes what constitutes the various risk levels from "Very Low" to "Very High" risk.

OVERALL RISK					
Overall Likelihood	**Overall Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Risk Definition Table

Qualitative Values	RISK Description
Very High	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Note: The RAR "Impact" column is pre-populated with the default raw risk value. Raw risk is associated with the impact because it represents the effect of a vulnerability before considering likelihood factors such as mitigations. Basically, each Raw Risk value equates to an applicable Impact & Likelihood numeric value:

Raw Risk	**Impact levels**	**Likelihood** (Lower # for Mitigation)
Raw Risk I	High (4)	High (4) or (3)
Raw Risk II	Mod (3)	Mod (3)
Raw Risk III	Low (2)	Low (2)

RAR Assessment Comments/Rationale

Inherited controls (I-C or I-NC) do not need to be assessed unless there is a STIG/Scans showing a vulnerability

Control Overview Section (Parent Control Overview SME Comments)

Non-ORTB: This control has been assessed as compliant for administration purposes only.

Non-Compliant STIG: Non-Compliant as per STIG finding. Mitigated to *[Very Low, Low, Moderate, High] [provide mitigations]*.

Non-Compliant CCI: Non-Compliant due to CCI criteria not being met. Mitigated to *[Very Low, Low, Moderate, High] [provide mitigations]*.

Inherited Compliant: Inherited compliant from [*enter name of inheritance]*.

Inherited Non-Compliant: Inherited non-compliant from *[enter name of inheritance]*.

ORTB: Concur ORTB *[Compliant/Non-Compliant/Not Applicable]*. *[Provide short justification]*.

Not Applicable: Concur with not applicable.

SME Comment Section (Column O)

Non-ORTB Comments: Concur *[Compliant/Non-Compliant/Not Applicable]* per *[SCTM, STIG, reference]*. *[Justifications/Mitigations]*.

Changing Control Status: Changed from *[compliance, non-compliance, not applicable]* to *[compliance, non-compliance, not applicable]* per *[provide justification]*.

Inheritance Controls: Concur inherited *[compliant or non-compliant]* with *[STIG, reference]*.

ORTB: Concur inherited *[compliant or non-compliant]*. Inheriting from *[reference]*.

Non-Compliant: Non-compliant as per *[provide justification and/or mitigation]*.

Compliant: Compliant as per *[provide justification]*.

Not Applicable: Not applicable per *[provide justification]*.

SC-15: Collaborative Computing Devices

01Dec19, ZZZ
SME COMMENTS: Concur with not applicable.

Parent Control Overview SME Comments

Phase	Overall Compliance	Overall %	Scans	Raw Severity Value
IP	0 of 0			II

Column O

#	RMF Ctrl ID	RMF Name	Assessment Procedure Number	CCI #	CCI Definition	Validation Procedures	SAR Validation Statu	Control Type	Recommended Implementation Guidance	Mitigations	SAR Comments	SME Status	SME Comments
1	SC-15	Collaborative Computing Devices	SC-15.1	CCI-001150	The information system prohibits remote	The organization conducting the inspection/as	NA		The organization being inspected/assessed configures the information		TR: -- TR Validation Status copied to SAR was *** Not	NA	Concur with N/A per *justification*. Raw Risk: II (Technical - STIG/SRG)
2	SC-15	Collabor	SC-15.2	CCI-001151	The	The	I-C		DoD has defined		Inherited	NA	Concur with N/A.
3	SC-15	Collabor	SC-15.3	CCI-001152	The	The	NA		The organization		TR: -- TR	NA	Concur with N/A.

Artifact Quality Rubric

1. Open the Artifact Quality Rubric. Click on Clear Form to ensure form has no previously entered data.
2. Evaluate each row to determine the score assigned to the category.
3. Once all rows are evaluated, the bottom of the document will calculate the final score. Refer to the chart to determine the recommended ATO length based on the quality and risk of the system.
    a. High water mark is used to determine the risk of the system.

Completing the CRA and SAR

CRA

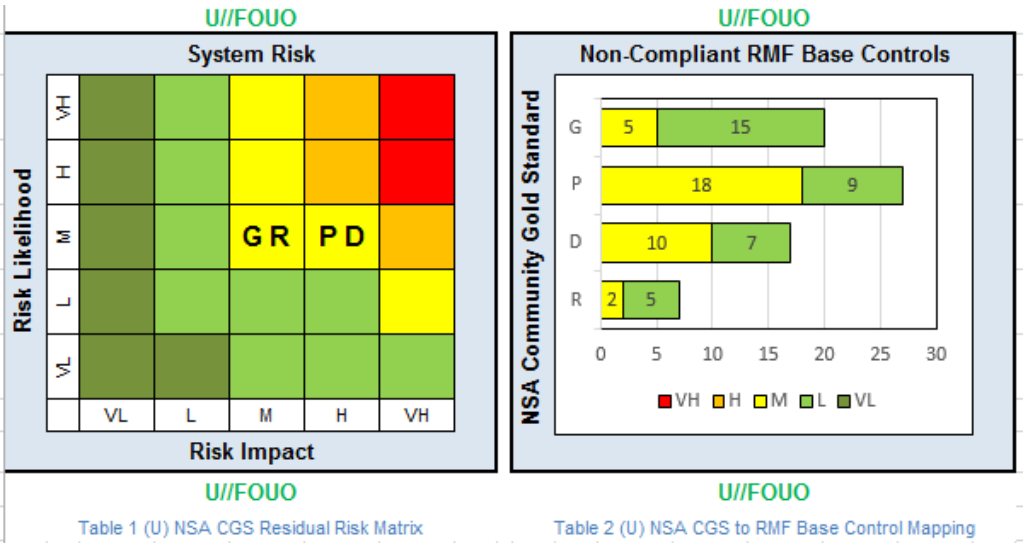
1. Open the CRA Template.
2. Fill in all template information.
3. Ensure all mark-up comments are deleted and all text is black.

Section 1 – Risk Summary:

- Date (ATD)
- Only list non-compliant controls; (e.g. The enclave has (20) Moderate and (5) Low non-compliant RMF base controls).
- Provide recommended ATO Time Frame (enter # of months) and With or Without Conditions.

Section 2 – Residual Risk Determination:

- From the Risk Matrix tab in the RAR, copy both NSA CGS graphics simultaneously from Excel; position the cursor in the center>>then Paste Special>Pictures:



- From the NSA tab in the RAR, copy the NSA Community Gold Standard graphic from Excel; position the cursor in the center>>then Paste Special>Pictures:

Section 3 – System Description and Characteristics:

- Add mission, encryption, access/authorization, CSSP description (if applicable).
- State if the system does/does not connect to any external network.
- Modify the wording as needed.

Section 4 – Additional Comments:

- Start by deleting items that are not applicable to your assessment and add others as needed.
- Use bullet statements to keep your comments brief and to the point.
- The Artifact Quality Rubric Score determination for ATO duration is entered here.

SAF AAZ SAR

1. Open the SAR Template.
2. Fill in all template information.
3. Ensure all mark-up comments are deleted, all text is black, and all background/highlighted colors are set to no fill.

Acronyms

Air Combat Command (ACC)
Authorizing Official (AO)
Body of Evidence (BoE)
Cybersecurity Risk Assessment (CRA)
Defense Information Systems Agency (DISA)
For Official Use Only (FOUO)
Headquarters (HQ)
Organizational Risk Tolerance Baseline (ORTB)
Plan of Action and Milestone (POA&M)
Risk Management Framework (RMF)
Secretary of the Air Force (SAF)
Security Control Traceability Matrix (SCTM)
Security Technical Implementation Guide (STIG)
Subject Matter Expert (SME)
System Assessment Report (SAR)
Risk Assessment Report (RAR)
System Security Plan (SSP)

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is almost certain to initiate the threat event.
High	80-95	8	Adversary is highly likely to initiate the threat event.
Moderate	21-79	5	Adversary is somewhat likely to initiate the treat event.
Low	5-20	2	Adversary is unlikely to initiate the threat event.
Very Low	0-4	0	Adversary is highly unlikely to initiate the threat event.

TABLE G-3: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT OCCURRENCE (NON-ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	80-95	8	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
Moderate	21-79	5	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
Low	5-20	2	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	0-4	0	Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

APPENDIX H

IMPACT

EFFECTS OF THREAT EVENTS ON ORGANIZATIONS, INDIVIDUALS, AND THE NATION

This appendix provides: (i) a description of useful inputs to the impact determination task; (ii) representative examples of adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation; (iii) exemplary assessment scales for assessing the impact of threat events and the range of effect of threat events; and (iv) a template for summarizing and documenting the results of the impact determination Task 2-5. The assessment scales in this appendix can be used as a starting point with appropriate tailoring to adjust for any organization-specific conditions. Table H-4, an output from Task 2-5, provides relevant inputs to the risk tables in Appendix I.

TABLE H-1: INPUTS – DETERMINATION OF IMPACT

Description	Provided To		
	Tier 1	**Tier 2**	**Tier 3**
From Tier 1 (Organization level) - Impact information and guidance specific to Tier 1 (e.g., impact information related to organizational governance, core missions/business functions, management and operational policies, procedures, and structures, external mission/business relationships). - Guidance on organization-wide levels of impact needing no further consideration. - Identification of critical missions/business functions. - Exemplary set of impacts, annotated by the organization, if necessary. (Table H-2) - Assessment scale for assessing the impact of threat events, annotated by the organization, if necessary. (Table H-3)	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Impact information and guidance specific to Tier 2 (e.g., impact information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Identification of high-value assets.	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Impact information and guidance specific to Tier 3 (e.g., likelihood information affecting information systems, information technologies, information system components, applications, networks, environments of operation). - Historical data on successful and unsuccessful cyber attacks; attack detection rates. - Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). - Results of continuous monitoring activities (e.g., automated and nonautomated data feeds). - Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. - Contingency Plans, Disaster Recovery Plans, Incident Reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

TABLE H-2: EXAMPLES OF ADVERSE IMPACTS

Type of Impact	Impact

HARM TO OPERATIONS	- Inability to perform current missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Inability, or limited ability, to perform missions/business functions in the future.
	  - Inability to restore missions/business functions.
	  - In a sufficiently timely manner.
	  - With sufficient confidence and/or correctness.
	  - Within planned resource constraints.
	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements (e.g., liability).
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to image or reputation (and hence future or potential trust relationships).

HARM TO ASSETS	- Damage to or loss of physical facilities. - Damage to or loss of information systems or networks. - Damage to or loss of information technology or equipment. - Damage to or loss of component parts or supplies. - Damage to or of loss of information assets. - Loss of intellectual property.
HARM TO INDIVIDUALS	- Injury or loss of life. - Physical or psychological mistreatment. - Identity theft. - Loss of Personally Identifiable Information. - Damage to image or reputation.

HARM TO OTHER ORGANIZATIONS	- Harms (e.g., financial costs, sanctions) due to noncompliance.
	  - With applicable laws or regulations.
	  - With contractual requirements or other requirements in other binding agreements.
	- Direct financial costs.
	- Relational harms.
	  - Damage to trust relationships.
	  - Damage to reputation (and hence future or potential trust relationships).

HARM TO THE NATION	- Damage to or incapacitation of a critical infrastructure sector.
	- Loss of government continuity of operations.
	- Relational harms.
	  - Damage to trust relationships with other governments or with nongovernmental entities.
	  - Damage to national reputation (and hence future or potential trust relationships).
	- Damage to current or future ability to achieve national objectives.
	  - Harm to national security.

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact Affected Asset	Maximum Impact
Table H-2 or Organization-defined	Table H-2 or Organization-defined	Table H-3 or Organization-defined

APPENDIX I

RISK DETERMINATION

ASSESSING RISK TO ORGANIZATIONS, INDIVIDUALS, AND THE NATION

This appendix provides: (i) a description of potentially useful inputs to the risk determination task including considerations for uncertainty of determinations; (ii) exemplary assessment scales for assessing the levels of risk; (iii) tables for describing content (i.e., data inputs) for adversarial and non-adversarial risk determinations; and (iv) templates for summarizing and documenting the results of the risk determination Task 2-6. The assessment scales in this appendix can be used as a starting point with appropriate tailoring to adjust for any organization-specific conditions. Table I-5 (adversarial risk) and Table I-7 (non-adversarial risk) are outputs from Task 2-6.

TABLE I-1: INPUTS – RISK

Description	Provided To		
	Tier 1	**Tier 2**	**Tier 3**
From Tier 1 (Organization level) - Sources of risk and uncertainty information identified for organization-wide use (e.g., specific information that may be useful in determining likelihoods such as adversary capabilities, intent, and targeting objectives). - Guidance on organization-wide levels of risk (including uncertainty) needing no further consideration. - Criteria for uncertainty determinations. - List of high-risk events from previous risk assessments. - Assessment scale for assessing the level of risk as a combination of likelihood and impact, annotated by the organization, if necessary. (Table I-2) - Assessment scale for assessing level of risk, annotated by the organization, if necessary. (Table I-3)	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Risk-related information and guidance specific to Tier 2 (e.g., risk and uncertainty information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies).	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Risk-related information and guidance specific to Tier 3 (e.g., likelihood information affecting information systems, information technologies, information system components, applications, networks, environments of operation).	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Very high risk means that a threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	High risk means that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	Moderate risk means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	Low risk means that a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	Very low risk means that a threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

TABLE I-4: COLUMN DESCRIPTIONS FOR ADVERSARIAL RISK TABLE

Column	Heading	Content
1	Threat Event	Identify threat event. (Task 2-2; Table E-1; Table E-2; Table E-5; Table I-5.)
2	Threat Sources	Identify threat sources that could initiate the threat event. (Task 2-1; Table D-1; Table D-2; Table D-7; Table I-5.)
3	Capability	Assess threat source capability. (Task 2-1; Table D-3; Table D-7; Table I-5.)
4	Intent	Assess threat source intent. (Task 2-1; Table D-4; Table D-7; Table I-5.)
5	Targeting	Assess threat source targeting. (Task 2-1; Table D-5; Table D-7; Table I-5.)
6	Relevance	Determine relevance of threat event. (Task 2-2; Table E-1; Table E-4; Table E-5; Table I-5.) If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.
7	Likelihood of Attack Initiation	Determine likelihood that one or more of the threat sources initiates the threat event, taking into consideration capability, intent, and targeting. (Task 2-4; Table G-1; Table G-2; Table I-5.)
8	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event and the predisposing conditions which could increase the likelihood of adverse impacts. (Task 2-5; Table F-1; Table F-3; Table F-4; Table F-6; Table I-5.)
9	Severity Pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions. (Task 2-5; Table F-1; Table F-2; Table F-5; Table F-6; Table I-5.)
10	Likelihood Initiated Attack Succeeds	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration threat source capability, vulnerabilities, and predisposing conditions. (Task 2-4; Table G-1; Table G-4; Table I-5.)
11	Overall Likelihood	Determine the likelihood that the threat event will be initiated and result in adverse impact (i.e., combination of likelihood of attack initiation and likelihood that initiated attack succeeds). (Task 2-4; Table G-1; Table G-5; Table I-5.)
12	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. (Task 2-5; Table H-1, Table H-2; Table H-3; Table H-4; Table I-5.)
13	Risk	Determine the level of risk as a combination of likelihood and impact. (Task 2-6; Table I-1; Table I-2; Table I-3; Table I-5.)

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

TABLE I-6: COLUMN DESCRIPTIONS FOR NON-ADVERSARIAL RISK TABLE

Column	Heading	Content
1	Threat Event	Identify threat event. (Task 2-2; Table E-1; Table E-3; Table E-5; Table I-7.)
2	Threat Sources	Identify threat sources that could initiate the threat event. (Task 2-1; Table D-1; Table D-2; Table D-8; Table I-7.)
3	Range of Effects	Identify the range of effects from the threat source. (Task 2-1; Table D-1; Table D-6; Table I-7.)
4	Relevance	Determine relevance of threat event. (Task 2-2; Table E-1; Table E-4; Table E-5; Table I-7.) If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.
5	Likelihood of Threat Event Occurring	Determine the likelihood that the threat event will occur. (Task 2-4; Table G-1; Table G-3; Table I-7.)
6	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event and the predisposing conditions which could increase the likelihood of adverse impacts. (Task 2-5; Table F-1; Table F-3; Table F-4; Table F-6; Table I-7.)
7	Severity Pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions. (Task 2-5; Table F-1; Table F-2; Table F-5; Table F-6; Table I-5.)
8	Likelihood Threat Event Results in Adverse Impact	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration vulnerabilities and predisposing conditions. (Task 2-4; Table G-1; Table G-4; Table I-7.)
9	Overall Likelihood	Determine the likelihood that the threat event will occur and result in adverse impacts (i.e., combination of likelihood of threat occurring and likelihood that the threat event results in adverse impact). (Task 2-4; Table G-1; Table G-5; Table I-7.)
10	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. (Task 2-5; Table H-1, Table H-2; Table H-3; Table H-4; Table I-7.)
11	Risk	Determine the level of risk as a combination of likelihood and impact. (Task 2-6; Table I-1; Table I-2; Table I-3; Table I-7.)

TABLE I-7: TEMPLATE – NON-ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11
Threat Event	Threat Sources	Range of Effects	Relevance	Likelihood of Event Occurring	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Event Results in Adverse Impact	Overall Likelihood	Level of Impact	Risk

Clear Form

ACC SAP Security Control Assessor (SCA) for Organizational Risk Tolerance Baseline (ORTB) Artifact Quality Rubric

Artifact Name	Poor - 1	Average - 2	Good - 3	Excellent - 4	Total
Network Topology	• Contains only basic information regarding system components. • Authorization boundary is not clearly defined. • Equipment interconnectivity is not identified. • Devices are not clearly identifiable.	• Contains >=80% HW components w/equipment type (encryptor, server, workstation, etc.). • Equipment interconnectivity >=80% accurate. • Authorization boundary is clearly defined. • Devices are somewhat identifiable.	• Contains >=90% HW components w/equipment type (encryptor, server, workstation, etc.) • Equipment interconnectivity >90% accurate. • Authorization boundary is clearly defined. • Devices are mostly identifiable.	• Contains all HW components w/equipment type (encryptor, server, workstation, etc.) and quantities. • Clearly depicts all equipment interconnectivity. • Authorization boundary is clearly identified and in proper format. • All devices are clearly identifiable.	
Hardware List	• Does not contain data elements IAW ACC HW/SW guide. • Is significantly different (>10%) than hardware depicted on Topology.	• Contains most (> 4) data elements IAW ACC HW/SW guide. • Is not significantly different (<10%) than hardware depicted on Topology.	• Contains all data elements IAW ACC HW/SW guide. • Matches the Topology (very few (1-2) discrepancies).	• Contains all data elements IAW ACC HW/SW guide. • Matches the Topology exactly.	
Software List	• Does not contain data elements IAW ACC HW/SW guide. • Has significant discrepancies with other system documentation.	• Contains most (>4) data elements ACC HW/SW guide. • Does not have significant discrepancies (<10%) with other system documentation.	• Contains all data elements IAW ACC HW/SW guide. • Very few discrepancies (1-2) with other system documentation.	• Contains all data elements IAW ACC HW/SW guide. • Matches other system documentation.	
PPSM and registration # (Enterprise Systems Only)	• Contains many (>3) discrepancies • Does not have a registration #.	• Provided using current / recent (<3 months) template version. • Contains few (<3) discrepancies • Does not have a registration #.	• Provided using current / recent (<3 months) template version. • Contains no discrepancies • Does not have a registration #.	• Provided using current template version. • Contains no discrepancies • Has a registration #.	
Vulnerability Scans	• Not provided in correct format (e.g., Nessus, Vulnerator, Asset Manager). • Not within 90 days of submission. • Coverage < 80% of required, representative / unique components.	• Submitted in correct format (e.g., Nessus, Vulnerator, or Asset Manager) • Within 90 days of submission. • Coverage >=80% of required, representative / unique components.	• Submitted in correct format (e.g., Nessus, Vulnerator, or Asset Manager). • Within 60 days of submission. • Coverage > 90% of required, representative / unique components.	• Submitted in correct format (e.g., Nessus, Vulnerator, or Asset Manager). • Within 30 days of submission. • Coverage of all required, representative / unique components.	
System Categorization Memo	• System Categorization memo is not submitted	• NOT APPLICABLE	• NOT APPLICABLE	• Accurately completed • System Categorization Memo submitted and signed.	
STIG Applicability List	• STIG applicability list is missing many (<50%) STIGS based on the technology defined in other system documents (e.g., HW/SW list, Topology, System Description).	• STIG applicability list is missing several (50%-80%)STIGS based on the technology defined in other system documents., (e.g. HW/SW list, Topology, System Description).	• STIG applicability list is missing few (>=80%) STIGS based on the technology defined in other system documents. (e.g., HW/SW list, Topology, System Description).	• STIG applicability list is complete STIGS based on the technology defined in other system documents. (e.g., HW/SW list, Topology, System Description).	
STIG compliance checks	• Not provided in correct format (.ckl). • Not within 90 days of submission. • Coverage <80% of STIGs on	• Provided in correct format (.ckl). • Within 90 days of submission. • Coverage >=80% of STIGs on STIG Applicability list.	• Provided in correct format (.ckl). • Within 60 days of submission. • Coverage >=90% of STIGs on STIG Applicability List.	• Provided in correct format (.ckl). • Within 30 days of submission. • Coverage >100% of STIGs on STIG Applicability List.	

Artifact Name	Poor - 1	Average - 2	Good - 3	Excellent - 4	Total
Non-Tailorable Controls Must address: AC-6.1, SA-22, SC-28	• Address 1 of 3 Controls	• Address 2 of 3 Controls	• Address 3 of 3 Controls	• 3 of 3 controls Addressed and Compliant See Note 2	
Configuration Management Should address: CM-1, 2, 3, 6, 7, 7(3), 8, 9	• Addresses <80% of the required baseline controls.	• Addresses >=80% of the required baseline controls.	• Addresses 100% of the required baseline controls.	• Addresses 100% of the required baseline controls. • Program provides evidence of implementation for at least 80% of required CCIs. See Note 3.	
Contingency Planning and Procedure Should address: CP-9, 9(3))	• Addresses <80% of the required baseline controls.	• Addresses >=80% of the required baseline controls.	• Addresses 100% of the required baseline controls.	• Addresses 100% of the required baseline controls. • Program provides evidence of implementation for at least 80% of required CCIs. See Note 4.	
Access Control Should address: AC-2, 2(7), 5, 6, 6(2), 17, 17(2), 17(3)	• Addresses <80% of the required baseline controls.	• Addresses >=80% of the required baseline controls.	• Addresses 100% of the required baseline controls.	• Addresses 100% of the required baseline controls. • Program provides evidence of implementation for at least 80% of required CCIs. See Note 5.	
Identification and Authentication Should address: IA-2, 2(2), 4, 5, 5(1), 5(2), 5(7)	• Addresses <80% of the required baseline controls.	• Addresses >=80% of the required baseline controls.	• Addresses 100% of the required baseline controls.	• Addresses 100% of the required baseline controls. • Program provides evidence of implementation for at least 80% of required CCIs. See Note 6.	
Assessment Procedures and POA&M	• All items on POA&M returned from SCAR review have been addressed. • All required fields are complete. • <80% of resources have been identified. • <80% of items have scheduled completion dates within 180 days of submission. • All items have current "Status" completed. • <80% items have comments, updated from SCAR comments, that explain completion or justification of status of "Ongoing" or "Not-Applicable" controls.	• All items on POA&M returned from SCAR review have been addressed. • All required fields are complete. • >=80% of resources have been identified. • >=80% of items have scheduled completion dates within 180 days of submission. • All items have current "Status" completed. • >=80% items have comments, updated from SCAR comments, that explain completion or justification of status of "Ongoing" or "Not-Applicable" controls.	• All items on POA&M returned from SCAR review have been addressed. • All required fields are complete. • >=90% of resources have been identified. • >=90% of items have scheduled completion dates within 180 days of submission. • All items have current "Status" completed. • >=90% items have comments, updated from SCAR comments, that explain completion or justification of status of "Ongoing" or "Not-Applicable" controls.	• All items on POA&M returned from SCAR review have been addressed. • All required fields are complete. • All resources required are identified. • All items have scheduled completion dates within 180 days of submission. • All items have current "Status" completed and accurate. • All items have comments, updated from SCAR comments, that explain completion or justification of status of "Ongoing" or "Not-Applicable" controls.	
				Total	**0**

Instructions on Use:

1. Evaluate each artifact / document for quality based on the defined criteria.
2. Total scores from each line item.
3. Classify quality of the package, using the total points, based on the following criteria:
    - *If comments listed in any of the red filled cells apply, the system will not receive an ATO. This should be identified during the initial assessment and corrected prior to scoring for quality.*

	Without PPSM	With PPSM
Poor Quality (<40%)	0-20	0-22
Average Quality (40%)	21-30	23-33
Good Quality (60%)	31-41	34-44
Excellent Quality (>=80%)	42 and above	45 and above

    - **Poor Quality:** Send instructions to the field describing how to bring artifacts, test results and/or POA&M entries up to minimum standards. This should be accomplished during the initial assessment phase of the A&A assessment and may require sending the package to the start.
    - **Average or Good Quality:** The CRA of Average or Good quality packages must specify conditions within the CRA which detail specific requirements to make the package excellent quality.
4. Using the table below, combine the quality score with the system risk to determine the recommended length of the ATO.

Notes:

1. Non-Tailorable Controls
- AC-6.1 – Screen shots from a sample of system configurations. (* Also in Note 3)
- SA-22 – Justification and documents for approval for the continued use of unsupported system components
- SC-28 – Implementation and reporting of Data at Rest (DaR) for all supported systems

2. The following can be provided as evidence of implementation:
- CM-1.4, 1.6 – Organization web portal, intranet or email screen capture showing dissemination of CMP
- CM-1.8, 1.9 – Change record or version history of CMP or other record showing review and update of CMP
- CM-2.2 – Configuration files or screen shots from a sample of hardware configurations

- CM-3.2, 3.3, 3.4, 3.5, 6.11, 6.12 – Sample of CCB Minutes or Change Control Request Form
- CM-6.5 – Applicable STIG or SRG checks
- CM-6.6, 6.7, 6.8 – POA&M and Test Results
- CM-7.1, 7.3 – PPSM and configuration files or configuration screenshots
- CM-7(3).2 – PPSM
- CM-8.1, 8.2, 8.3 – Hardware List
- CM-8.7 – Change log or version history of Hardware List
- CM-9.2, 9.4, 9.6, 9.10 – CCB Minutes, Change Control Request Form, Security Impact Analysis

3. The following can be provided as evidence of implementation:
- CP-9.2, 9.4, 9.6 – Audit logs / screen shot from a sample of systems to ensure they are configured to perform backups as defined in the contingency plan
- CP-9(3).2 – Required if Availability is High: Record of where backup copies of critical software are stored

4. The following can be provided as evidence of implementation:
- AC-2.3 – Appointment letter or sample of 2875s with signature
- AC-2.6 – Role based Access Control List, Memorandum for Record, or other document specifying authorized users
- AC-2.8, 2.9, 2.10, 2.11, 2.19, 2.20, 2.21 – Sample of 2875s
- AC-2.13, 2.15, 2.16, 2.17, 2.18, 2.22 – Audit trail of account maintenance / monitoring activities
- AC-2(7).2 – Acceptable Use Policy
- AC-5.1, 5.2, 5.3, 5.4, 5.5 – Sample of job descriptions
- AC-6.1 – Screen shots from a sample of system configurations
- AC-17.5 – Audit trail of authorizations for remote access
- AC-17(2).1, .2 – Sample of screen shots showing configuration for encryption and/or applicable STIG results
- AC-17(3).1 – Sample of screen shots showing configuration for routing of remote access and/or applicable STIG results

5. The following can be provided as evidence of implementation:
- IA-2.1, (2).1 – Screen shot of configuration or of identification/authentication procedure from user perspective; applicable STIG checks
- IA-5(1).12 – Screen shot of configuration settings to show only encrypted representations of passwords are stored or applicable STIG checks.
- IA-5(1).18 – Screen shot of configuration settings to show the system prohibits the reuse of passwords for a minimum of 5 generation
- IA-5(2).1, .2, .3, .4 – Screen shot of configuration settings to show compliance with PKI requirements
- IA-5(7).1, .2, .3 – Screen shot of configuration settings to show compliance with requirements for unencrypted static authenticators

		Maximum Length of ATO in Months				
QUALITY	Excellent	6*	12*	24	36	36
	Good	6*	12*	18	30	36
	Average	3*	9*	12	24	30
		Very High	High	Moderate	Low	Very Low
		RISK				

Quality Score: 0

Risk Level: Choose