



CENTERS for MEDICARE & MEDICAID SERVICES

Enterprise Information Security Group

7500 Security Boulevard

Baltimore, Maryland 21244-1850



**Enterprise Information
Security Group**

*Risk Management, Oversight,
And Monitoring*

Risk Management Handbook

Volume II

Procedure 5.6

**Documenting Security Control
Effectiveness in CFACTS**

FINAL

Version 1.1

September 18, 2013

Document Number: CMS-CISO-2013-vII-pr5.6

(This Page Intentionally Blank)

**SUMMARY OF CHANGES IN *DOCUMENTING SECURITY CONTROL
EFFECTIVENESS IN CFACTS*, VERSION 1.1**

1. All references and hyperlinks to the Information Security Library were updated.
2. All references (by name, acronym, graphic, etc.) to OCISO changed to EISG

**SUMMARY OF CHANGES IN *DOCUMENTING SECURITY CONTROL
EFFECTIVENESS IN CFACTS*, VERSION 1.00**

Baseline Version

(This Page Intentionally Blank)

TABLE OF CONTENTS

1 OVERVIEW.....1

1.1 Purpose..... 1

1.2 Other Relevant Procedures..... 1

2 SECURITY CONTROL DOCUMENTATION PROCEDURE2

2.1 Documenting Security Control Assessments in CFACTS..... 2

 2.1.1 Procedure Users 2

 2.1.2 Initial Conditions 2

 2.1.3 Security Control Assessment Documentation Procedure 3

2.2 Remediating a Failed Control Assessment 17

 2.2.1 Procedure Users 17

 2.2.2 Initial Conditions 17

 2.2.3 Remediating a Failed Control Assessment Procedure 17

2.3 Creating a Finding from a Failed Assessment 24

2.4 Uploading Findings Directly 24

 2.4.1 Procedure Users 24

 2.4.2 Initial Conditions 24

 2.4.3 Uploading Findings Directly Procedure 25

2.5 Creating a Weakness from an Existing Finding 25

 2.5.1 Procedure Users 25

 2.5.2 Initial Conditions 26

 2.5.3 Creating a Weakness From an Existing Finding Procedure 26

2.6 Figures..... 28

3 APPROVED29

LIST OF TABLES

NO TABLE OF FIGURES ENTRIES FOUND.LIST OF FIGURES

Figure 1 “Test Result” Logic Diagram..... 28

(This Page Intentionally Blank)

1 OVERVIEW

1.1 PURPOSE

The purpose of this procedure is to provide the security personnel with CFACTS data entry responsibilities the necessary procedures for entering the following information into CFACTS:

- Documenting security control testing in CFACTS.
- Documenting and associating a corrective action plan for a failed control assessment.
- Uploading *Findings* from a security assessment spreadsheet.
- Creating a weakness from an existing *Finding* in CFACTS.

1.2 OTHER RELEVANT PROCEDURES

Other relevant procedures include:

- RMH Volume II, Procedure 1.1, *Accessing the CFACTS*. This procedure is required to gain access to, and log into the CFACTS.
- RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS*. This procedure requires that security controls be properly documented in CFACTS as a prerequisite for documenting testing of the applicable security control(s).
- RMH Volume II, Procedure 6.2, *POA&M Management*. This procedure is required to ensure that *Weaknesses* are properly documented and managed in CFACTS.
- RMH Volume II, Procedure 7.3, *CMS Annual Attestation Procedure* relies on this procedure to ensure that POA&M information is current as a prerequisite for submitting an annual attestation.

All applicable RMH procedures are available on the CMS information Security website, in the *Information Security Library* at: <http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>.

2 SECURITY CONTROL DOCUMENTATION PROCEDURE

PROCEDURE	PRINCIPLE
2.1 DOCUMENTING SECURITY CONTROL ASSESSMENTS IN CFACTS	
2.1.1 PROCEDURE USERS	
1. CMS ISSO. 2. Business Partner SSO. 3. Designated CFACTS data entry person. 4. EISG Staff.	
2.1.2 INITIAL CONDITIONS	
1. User has authorized access to the applicable CMS system in CFACTS. a. Refer to RMH Vol II, Procedure 1.1, <i>Accessing the CFACTS</i> , for further guidance on gaining authorized access to CFACTS.	<i>Some user roles may not have the necessary access rights to enter vulnerabilities into CFACTS. Contact the EISG at mailto:ciso@cms.gov with questions regarding user roles and their access limits.</i>

PROCEDURE	PRINCIPLE
2.1.3 SECURITY CONTROL ASSESSMENT DOCUMENTATION PROCEDURE	<i>This procedure should be used when a security Test Procedure is conducted.</i>
1. Log into CFACTS using RMH Volume II, Procedure 1.1, <i>Accessing the CFACTS</i> .	<i>Opens the applicable system to the Identification tab.</i>
2. Click on the link for the applicable system from either the <i>Home</i> screen or the <i>Browse</i> Screen.	<i>Enables the Security Controls tab.</i>
3. Select the <i>Security Controls</i> tab.	<i>Enables the Security Control Assessment view on the Security Controls tab.</i>
4. Select the <i>Security Control Assessment</i> radio button.	<i>Tree View in the On setting will display a listing of the Security Control requirements on the left side of the screen.</i>
5. If not already in <i>Tree View</i> mode, select <i>Tree View</i> to <i>On</i> .	<i>Users will be directed to return to this step for additional Controls and/or Test Procedures, as applicable.</i>
NOTE:	<i>Users may also navigate by using the First, Previous, Next, and Last links at the bottom of the page.</i>
The following steps will be performed for EACH Control and each associated Test Procedure assessed.	
6. Navigate to the applicable <i>Security Control</i> by selecting the applicable control from the listing on the left side of the screen.	
7. Click on the link for the applicable <i>Test Procedure</i> .	

PROCEDURE

PRINCIPLE

8. If the *Compliance Description* is not filled in:

a. **Exit this procedure** and proceed to RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS* to complete the *Compliance Description* before proceeding with this procedure.

PROCEDURE

PRINCIPLE

WARNING:

Steps up through Step 21.d. must be completed within 15 minutes. If the system is allowed to “Time-Out”, any new data not Saved will be lost.

9. If a control requirement has been **verified** as *Optional* (as specified in the requirement’s *Applicability* field in the ARS appendix), perform the following:

NOTE:

An Assessor may verify that the *Not Applicable* designation has been made appropriately.

a. In the *Test Result* field, check the *Not Applicable* checkbox.

*If the application is allowed to time-out before completion of Step 21.d. without saving newly-entered data, that data **will be lost**.*

To extend beyond the fifteen minute window, when the time-out Warning screen presents itself, perform either of the following:

*If **new data has been entered**, click the **Save** button at the bottom of the form.*

*If **NO new data has been entered**, Save the form **or** Refresh the browser window.*

*The Applicability field for certain ARS CMSR requirements (Baseline or Enhancements) may designate certain requirements as Optional for **specified** contractor types. If, based on the ARS designation of the contractor Type, it has been **verified** that these controls are not necessary for a specified contractor, then the applicable requirement’s Assessment Procedure may be marked as Not Applicable. **No other reasons for a Test Result of Not Applicable are authorized.** Contact the EISG at <mailto:CISO@cms.gov> if you have any question regarding this determination.*

*Marking a control as Not Applicable does **NOT** exclude that requirement from the scope of any assessments. Assessors must review to determine if that designation has been made correctly.*

PROCEDURE

PRINCIPLE

b. In the *Actual Results* field, explain why this *Assessment Procedure* (and associated *Control Requirement*) has been marked as *Not Applicable*, including which contract type has been cited (as stated in the ARS) for this exclusion.

Example: "PL-5 is designated as Optional for ABMAC contracts. The [name current system] is designated as an ABMAC. We have verified that this requirement is not necessary in the local implementation for ABMAC or any other supporting contractor function. Therefore this Assessment Procedure is designated as 'Not Applicable'."

c. Return to Step 6 and commence assessing another control, or exit this procedure, as applicable.

NOTE:

Assessment results of *Failed with Compensating Control* is NOT authorized responses at CMS.

NOTE:

FULLY-inheritable controls do not require additional testing at the *System-Specific* level. However, if an inherited control requires testing at the *system-specific* level to verify that it has been properly implemented, then it is NOT considered to be FULLY-inheritable.

Fully-inheritable control effectiveness cannot be influenced by individual systems. If an individual system is capable of influencing the effectiveness of an inheritable control, then that control cannot be considered to be FULLY-inheritable—which mandates that additional testing be required at the system-specific level to ensure that the control is implemented at its full effectiveness.

10. Refer to Figure 1 - "*Test Result*" Logic Diagram, to determine the appropriate *Test Result* for the applicable *Test Procedure*.

Refer to Figure 1, "Test Result" Logic Diagram, to execute the decision tree process for determining what the Test Result status should be for the applicable Test procedure.

11. For the applicable *Test Result* for a control that is **NOT** fully or partially *inherited*:

Perform these steps/sub-steps ONLY if the control is not inherited at all.

a. If the *Test Procedure* is determined to be **Not Started**:

If the applicable assessments have not been fully competed, then it should be documented as Not Started.

(1) Check (or verify as checked) the **Not Started** checkbox.

PROCEDURE

PRINCIPLE

(2) Return to Step 6 and commence assessing another control, or exit this procedure, as applicable.

b. If the *Test Procedure* is determined to have **Failed**:

(1) Check (or verify as checked) the **Failed** checkbox.

(2) If the *Failure* applies to ALL *Assessment Procedures* for the applicable control requirement, check (or verify as checked) the *Test Results Options* field to indicate *Apply test results to all test cases for this control*.

(3) Proceed to Step 13 to document the *Actual Results* of the assessment.

c. If the *Test Procedure* is determined to have *Passed*:

(1) Check (or verify as checked) the **Passed** checkbox.

(2) Proceed to Step 13 to document the *Actual Results* of the assessment.

12. For the applicable *Test Result* for a **FULLY** or **PARTIALLY** inherited control:

a. Verify that the *Inherited* checkbox is checked. If the *Inherited* checkbox is not checked, return to Step 11 and perform the procedure for a control that is **NOT** fully or partially inheritable.

Checking this checkbox will duplicate the Test results, and other applicable test result fields from this Assessment Procedure, to ALL other all Assessment Procedures for the applicable control requirement.

*Inherited Test Results are indicated with the Inherited checkbox “checked” and greyed-out (not enabled for use). If the Test Result checkbox for inherited is **NOT** checked, then the control **cannot be considered as inherited**.*

PROCEDURE

PRINCIPLE

b. For **FULLY** inherited **Common Controls**:

(1) Maintain the *Test Result* as indicated by the *Common Control Provider*.

(2) Return to Step 6 and commence assessing another control, or exit this procedure, as applicable.

c. For **PARTIALLY** inherited **Hybrid Controls**:

(1) If the inherited *Test Procedure* is indicated as **Not Started**:

(a) **DO NOT** modify *Test Results* field for *inherited* controls that are *Not Started*.

(b) Proceed to Step 13 to document the *Actual Results* of the assessment at the *system-specific (inheritor) system* level.

(2) If the inherited *Test Procedure* is indicated as **Passed**:

(a) If the *system-specific (inheritor) system Test Procedure* is determined to be **Not Started**:

i. Check (or verify as checked) the *Override* checkbox.

Fully inheritable controls do not require additional testing at the inheritor level. However, if a Common Control requires testing at the inheritor level to ensure that it has been properly implemented, or if additional controls are required to fully address a failed Common Control, then that control is considered a Hybrid Control, and is NOT fully-inheritable.

Do NOT change the Test Result from the result achieved by the control provider.

Inherited Test Procedure (Control Provider assessment) has not been performed.

“Incomplete” control assessment (not fully completed at BOTH the inherited Control Provider AND the Inheritor level) is to be marked as Not Started.

Inherited Test Procedure (inherited Control Provider level control assessment) has been performed, and has Passed all testing requirements.

Inherited Test Procedure (inherited Control Provider level control assessment) has not been performed.

PROCEDURE

PRINCIPLE

ii. Check (or verify as checked) the *Not Started* checkbox.

“Incomplete” control assessment (not fully completed at BOTH the inherited Control Provider AND the Inheritor level) is to be marked as Not Started.

iii. Return to Step 6 and commence assessing another control, or exit this procedure, as applicable.

(b) If the *system-specific (inheritor) system Test Procedure* is determined to have **Failed**:

This is verified through assessment of the system-specific implementation of the inherited control.

i. Check (or verify as checked) the *Override* checkbox.

Checking the Override checkbox will enable users to modify the indicated status that was inherited from the common control provider.

ii. Check (or verify as checked) the **Failed** checkbox.

iii. If the *Failure* applies to ALL *Assessment Procedures* for the applicable control requirement, check (or verify as checked) the *Test Results Options* field to indicate *Apply test results to all test cases for this control*.

Checking this checkbox will duplicate the assessment results, and other applicable assessment result fields from this Assessment Procedure, to ALL other all Assessment Procedures for the applicable control requirement.

iv. Proceed to Step 13 to document the *Actual Results* of the assessment at the *system-specific (inheritor) system* level.

(c) If the *system-specific (inheritor) system Test Procedure* is determined to have **Passed**:

This is verified through assessment of the system-specific implementation of the inherited control.

i. Verify unchecked (or uncheck) the *Override* checkbox.

ii. Check (or verify as checked) the **Passed** checkbox.

PROCEDURE

PRINCIPLE

iii. Proceed to Step 13 to document the *Actual Results* of the assessment at the *system-specific (inheritor) system* level.

(3) If the inherited *Test Procedure* is indicated as **Failed**:

(a) If the *system-specific (inheritor) system* has **NOT** applied an *Alternate/Compensating Control* to compensate for the failed *inherited* control:

i. **DO NOT** modify *Test Results* field for **Failed** *inherited* control.

ii. If the *Failure* applies to ALL *Assessment Procedures* for the applicable control requirement, check (or verify as checked) the *Test Results Options* field to indicate *Apply test results to all test cases for this control*.

iii. Proceed to Step 13 to document the *Actual Results* of the assessment at the *system-specific (inheritor) system* level.

(b) If the *system-specific (inheritor) system* has applied an *Alternate/Compensating Control* to compensate for the **Failed** *inherited* control **and** the *system-specific (inheritor) system Test Procedure* is determined to have **Failed**:

i. **DO NOT** modify *Test Results* field for **failed** *inherited* control.

ii. If the *Failure* applies to ALL *Assessment Procedures* for the applicable control requirement, check (or verify as checked) the *Test Results Options* field to indicate *Apply test results to all test cases for this control*.

Alternate/Compensating controls are additional controls (beyond those other NIST-required controls) that are specifically designed to address a failure or ineffectiveness of another required control.

Checking this checkbox will duplicate the assessment results, and other applicable assessment result fields from this Assessment Procedure, to ALL other all Assessment Procedures for the applicable control requirement.

Alternate/Compensating controls are additional controls (beyond those other NIST-required controls) that are specifically designed to address a failure or ineffectiveness of another required control.

Checking this checkbox will duplicate the assessment results, and other applicable assessment result fields from this Assessment Procedure, to ALL other all Assessment Procedures for the applicable control requirement.

PROCEDURE

PRINCIPLE

iii. Proceed to Step 13 to document the *Actual Results* of the assessment at the *system-specific (inheritor) system* level.

(c) If the *system-specific (inheritor) system* has applied an *Alternate/Compensating Control* to compensate for the **Failed** inherited control and the subsequent *system-specific (inheritor) system Test Procedure* is determined to have **Passed**:

i. Check (or verify as checked) the *Override* checkbox.

ii. Check (or verify as checked) the **Passed with Compensating Control** checkbox.

iii. In the *Actual Results* field, describe how the compensating control addressed the failure at the common control provider level.

iv. Proceed to Step 13 to document the remainder of the *Actual Results* of the assessment at the *system-specific (inheritor) system* level.

*Alternate/Compensating controls are **additional** controls (beyond those **other** NIST-required controls) that are specifically designed to address a failure or ineffectiveness of another required control.*

Example: “AC-2.1 Compensating Control: Local system applied additional local policy to address Roles and Responsibilities (missing at the enterprise level) and complete the necessary requirements for AC-2.”

PROCEDURE

PRINCIPLE

13. For the *Actual Results*, enter the full text description of the results of the assessment. Ensure that the following elements are included in the *Actual Results* field:

This field should describe:

- 1) *How the control was assessed,*
- 2) *What the actual results were for **each** of the required Test Procedures (Interview, Examine, and/or Test.)*
- 3) *If an Alternate/Compensating Control has been implemented and assessed, then those results should be **added** to any existing or inherited assessment results that may already documented.*

Do NOT simply restate the security requirement and say (or imply) that the control implementation simply “failed to meet” or “met” the control requirement.

*For failed assessment results, CMS **also** requires the four minimum elements defined in the GAO Yellow Book, Government Auditing Standards¹, to be included in any deficiencies noted.*

a. The *criteria* for the control requirement.

Discuss all portions of the applicable control Assessment Procedure was assessed.

Example: “AC-2.1 Assessment Criteria: Tester examined access control policies to determine if the organization requires appropriate approvals for requests to establish accounts, as required in AC-2 baseline requirement in CMS ARS.”

b. The observed *condition* at the time of the assessment.

Discuss the observed situation, as it existed at the time of the assessment.

Example: “AC-2.1 Condition: Users are currently granted Admin-level access to the application with only Network-Admin review and authority. No management personnel approve access requests.”

¹ The U.S. Government Accountability Office (GAO) *Government Auditing Standards* (Yellow Book) can be found at <http://www.gao.gov/yellowbook>.

PROCEDURE

PRINCIPLE

c. If the control did not meet all of the requirements, document the likely cause for the discrepancy.

Discuss the probable reason for this condition existing.

Example: “AC-2.1 Cause: The application Business Owner has not developed a documented process for requesting and approving access to various defined user Groups.”

d. The effect (or potential effect) for the observed condition.

Discuss the potential (or real) impact for the observed condition.

Example: “AC-2.1 Effect: Not having an approval process allows a single individual (network Admin) the default authority to grant access to a user, without separate management review of the ‘appropriateness’ of the requested access. This ‘authority’ allows the network-Admin, who is likely not qualified to assess the ‘business need’ of a request, to grant inappropriate access with little or no oversight or review.”

14. For the Interviewee(s), enter the full names of the individuals that were interviewed, tested, and/or examined during execution of the applicable Test Procedures.

This information is used for follow-up actions during the development and mitigation of the POA&M. Knowing the individuals associated with the assessment of the applicable control and the identification process for this issue can greatly assist in the development and execution of the subsequent corrective actions.

*While the field name say’s “Interviewee(s)”, the intent is to identify **anyone** within the system’s administrative processes whom is familiar with the assessment actions that identified this result.*

PROCEDURE

PRINCIPLE

15. For the *Collected Evidence*, list all of the evidence that collected during the execution of the applicable *Test Procedure*.
16. To store *Collected Evidence files* within the CFACTS tool, perform the following steps:
- a. In the *Compliance Details* field, select *New* to open the *Add Description* screen.
 - b. In the *Add Description* screen *Title* field, enter a **unique** title of the file being uploaded.
 - c. In the *Description* field, briefly describe the contents and purpose of the uploaded file.
 - d. Click the *Save* button to close the *Add Description* screen.
 - e. For the newly created *Compliance Detail*, click on the *Upload* link.
 - f. On the *Upload Support Documentation* screen, click on *Browse* and select the applicable file to be uploaded.

This information is used for follow-up actions during the development and mitigation of the POA&M. Access to the specific evidence associated with the assessment of the applicable control and the identification process for this weakness can greatly assist in the development and execution of the subsequent corrective actions. If the evidence is stored in an accessible store, list the location of the evidence.

Perform this step only if supporting evidence FILES need to be stored.

Example: "AC-19.1 Nov-2011 Assessment Evidence File 1"

Ensure that the description describes that the file is supporting information to support assessment results. Other files may already exist that are related to the implementation of the control. It is important to differentiate in the description so that other users can identify the purpose of the uploaded file.

Example: "AC-19.1: Nessus scan data for server ABCD1 indicating failed patch implementation for CVE-2011-1234".

PROCEDURE

PRINCIPLE

g. Select the *Image* radio button for image files—for ALL others, select *Text*.

Files loaded as Image files will place an image thumbnail in the Supporting Artifact field in place of the Title text. As such, be sure to place enough information in the Description field to identify the purpose (i.e., “AC-19.1:...” and description) of the file.

h. Click the *Upload* button.

i. After the file has been uploaded, click on the *Close* button.

17. For the *Sample Size*, list the specific size of the sample taken during the execution of the applicable *Test Procedure*.

*Examples include:
“Interviewed 3 of 5 System Administrators”
“Examined all XYZ Policies”
“Tested 10 out of 25 Linux servers.”*

18. For the *Comments*, enter any additional information that can be used to assist in the creation or mitigation of the applicable POA&M action.

In many cases, auditors will provide suggested remediation steps and/or the underlying cause of the failure. This information should be included in the Comments—exactly as provided by the applicable reviewer.

19. For the *Tester*, enter name of the applicable assessor.

*This information is useful for follow-up questions on the nature of the assessment, particularly for failed assessment results.
Example:
“Jane Doe of XYZ-Auditing Corp.”*

20. For the *Date of Test*, enter actual date of the assessment.

*Note that the default for this field is the **current** date. It is highly likely that this field must be adjusted to indicate the **actual** date of the applicable assessment.*

21. If automated tools were used to identify this failure:

a. Select the wizard button for *Additional Information*.

b. Enter the *Automated Tool Name*.

c. Enter the applicable *Automated Tool Check ID Number*.

PROCEDURE

PRINCIPLE

- d. Click the *Save* button.
22. If additional *Controls* or *Test Procedures* need to be documented:
- a. Return to Step 6 and commence assessing another control.
23. Upload documentation of the Security Control Assessment into CFACTS as follows:
- a. Click on the *SA&A Tracking* tab.
 - b. Scroll down to the *Security Control Assessment* section.
 - c. In the section for loading supporting documents, click on the *New* link.
 - d. In the *Title* field, type in the *Year* and *Type* of assessment document.
 - e. Click on the *Browse* button and select the applicable file to upload.
 - f. Click on the *Upload* button.
 - g. Click on the *Close* button.
24. For each **Failed Test Procedure**, proceed to Section 2.2, *Remediating a Failed Control Assessment*.

Upload any supporting documentation into CFACTS as documentary evidence of the assessment specific. Include any assessment plans, preliminary reports, final reports, working papers, and other supporting documentation (such as SSP review reports, IS RA review reports, CP review reports, or other supporting reports for the overall assessment.)

Redirects the user to the SA&A tracking screen.

Opens the Upload Support Document screen.

Example: "2012: Annual Assessment Report (Preliminary)"

Uploads the selected file into CFACTS.

Closes the Upload Support Document screen and returns the user to the SA&A Tracking screen.

Failed assessment results are converted directly to weaknesses.

PROCEDURE

PRINCIPLE

**2.2 REMEDIATING A
FAILED CONTROL
ASSESSMENT**

2.2.1 PROCEDURE USERS

1. CMS ISSO.
2. Business Partner SSO.
3. Designated CFACTS data entry person.
4. EISG Staff.

2.2.2 INITIAL CONDITIONS

1. User has authorized access to the applicable CMS system in CFACTS.
 - a. Refer to RMH Vol II, Procedure 1.1, *Accessing the CFACTS*, for further guidance on gaining authorized access to CFACTS.
2. User has been directed by another procedure to perform actions in this procedure.

Some user roles may not have the necessary access rights to enter vulnerabilities into CFACTS. Contact the EISG at <mailto:ciso@cms.gov> with questions regarding user roles and their access limits.

**2.2.3 REMEDIATING A FAILED
CONTROL ASSESSMENT
PROCEDURE**

1. In CFACTS, navigate to the *Security Controls* tab for the applicable system.

PROCEDURE

PRINCIPLE

2. Select the *Security Control Assessment* radio button.
3. If not already in Tree View mode, select *Tree View to On*.
4. Navigate to the applicable *Security Control* by selecting the applicable control from the listing on the left of the screen.
5. Click on the link for the applicable *Test Procedure* that the system has failed.

Enables the Security Control Assessment view on the Security Controls tab.

Tree View in the On setting will display a listing of the Security Control requirements on the left side of the screen.

Alternatively, users may also navigate by using the First, Previous, Next, and Last links at the bottom of the page.

If the Test Procedure has already been identified by CFACTS as Failed, then the applicable Test Procedure link will appear in Red.

WARNING:

Steps up through Step 12.g. must be completed within 15 minutes. If the system is allowed to “Time-Out”, any new data not Saved will be lost.

*If the application is allowed to time-out before saving newly-entered data (after the Warning screen is displayed), that data **will be lost**.*

To extend beyond the fifteen minute window, when the time-out Warning screen presents itself:

If new data has been entered, click Save.

If NO new data has been entered, Refresh the browser window.

6. If the failed *Test Procedure* has not been fully documented:
 - a. Exit this procedure and document the *Failed* assessment procedure in accordance with, Section 2.1, *Documenting Security Control Assessments in CFACTS*.
7. Navigate down the screen to the *Failed Test Options* field.
8. If no links are shown in this field, perform **one** of the following steps:
 - a. Return to Step 4 and navigate to an *Assessment Procedure* that has failed, **or**

There will be several links available for selection in the field

No links present means that the applicable Assessment Procedure has not Failed. No new Weakness needs to be created.

PROCEDURE

PRINCIPLE

b. Exit this procedure, and modify the *Test Results* for this *Test Procedure* in accordance with Section 2.1, *Documenting Security Control Assessments in CFACTS*, to indicate that this *Test Procedure* has failed.

This procedure is for documenting Failed Test Procedures. No links visible indicates that this control requirement has not been recorded as Failed.

9. If a *Weakness* exists for the *failed control*, proceed as follows:

a. Click on the *View weakness for a failed control* link.

Opens the Weakness Details Report screen.

*If the link does not exist, then an applicable weakness does **not** exist.*

b. If **all** of the listed weakness(es) have a *Status of Completed* or *Pending Verification*, perform the following:

Newly identified failed assessment procedures must be remediated. Since closed POA&M actions did not prevent an additional failure, a new Weakness and POA&M action items (with milestones) must be developed to address the additional issue(s).

(1) Close the *Weakness Details Report* screen.

Returns to the Self-Assessment screen.

(2) Proceed to Step 10.

Proceed to creating a new weakness.

c. For **each open** *Weakness* listed, perform the following:

Open means it has a status of one of the following: Draft, Not-Started, Ongoing, or Delayed.

(1) If the *Weaknesses* description and the *Milestones with Completion Dates* are **not** appropriate for this failed assessment procedures:

“Appropriate” means that the weakness milestones (corrective actions) can be relied upon to correct the issues identified in the failed assessment procedure.

(a) Click on the *Weaknesses* link.

Opens the Edit Weakness screen.

(b) Click on the button in the *Link to Control Title* field.

Opens the Linking Weakness to Controls screen.

(c) If a link exists for the applicable *Test Number*, click on the *Delete* link for the applicable *Test Number*, and then click *OK*.

If the link is not appropriate for this failed assessment procedure, then it should not be linked. Delete any links to inappropriate Test Numbers.

PROCEDURE	PRINCIPLE
(d) Click on the <i>Close</i> button.	<i>Returns to the Edit Weakness screen.</i>
(2) If the <i>Weaknesses</i> description and the <i>Milestones with Completion Dates</i> are appropriate for this failed assessment procedure:	“Appropriate” means that the weakness milestones (corrective actions) can be relied upon to correct the issues identified in the failed assessment procedure.
(a) Click on the <i>Weaknesses</i> link.	<i>Opens the Edit Weakness screen.</i>
(b) Click on the button in the <i>Link to Control Title</i> field.	<i>Opens the Linking Weakness to Controls screen.</i>
(c) If the applicable control <i>Test Number</i> is not listed:	<i>If the link is appropriate for this failed assessment procedure, then it should be linked. Link the weakness to the appropriate Test Number.</i>
i. Click on <i>New</i> .	<i>Opens the Manage Controls Associated with Weakness screen.</i>
ii. Select from the <i>Control</i> dropdown the appropriate <i>Control</i> .	
iii. Select from the <i>Test Number</i> dropdown the appropriate <i>Test Number</i> .	
iv. Click the <i>Save</i> button.	<i>Saves the new linked information.</i>
v. Click the <i>Close</i> button.	<i>Returns to the Edit Weakness screen.</i>
(d) Click on the <i>Close</i> button.	<i>Returns to the Self-Assessment screen.</i>
(e) Click on <i>Save</i> .	<i>Updates the information on the Self-Assessment screen.</i>
(f) Perform one of the following:	
i. If the <i>View weakness for a failed control</i> link does not exist, proceed to Step 10, or	<i>If the link does not exist, then all possibly-applicable weaknesses have been deemed to be not-appropriate. A new weakness must be created.</i>

PROCEDURE

PRINCIPLE

ii. If the link exists, click on the *View weakness for a failed control* link.

Opens the Weakness Details Report screen to process any remaining weaknesses

(3) Perform **one** of the following:

(a) If another open *weakness* exists, return to the above Step c.

Continue to verify the appropriateness of every weakness on the list. More than one may be appropriate.

(4) If at least **one** of the open weaknesses was deemed appropriate for this failed assessment procedure, perform the following:

“Appropriate” means that the weakness milestones (corrective actions) can be relied upon to correct the issues identified in the failed assessment procedure.

(a) If open, close the *Weakness Details Report* screen.

Returns to the Self-Assessment screen

(b) On the *Self-Assessment* screen, click on *Save*.

Updates the information of the Self-Assessment screen.

(c) Proceed to Step 13.

This means that (at least) one weakness is properly linked to this failed assessment procedure. No additional weaknesses need be created.

(5) If **none** of the open weaknesses were deemed appropriate for this failed assessment procedure, proceed to Step 10.

“Appropriate” means that the weakness milestones (corrective actions) can be relied upon to correct the issues identified in the failed assessment procedure. If this condition is met, a new weakness must be created.

CAUTION:

Do not create a *Finding*. Proceed directly to creating a *Weakness*.

CMS does not desire Findings to be created for failed assessment procedures. Instead, create a Weakness directly from the failed Test Case.

10. In the *Failed Test Options* field, click on the *Create weakness for failed test case* link, then click *OK*.

Opens the Add Weakness screen.

PROCEDURE

PRINCIPLE

11. Document the weakness details in accordance with the *Documenting a Weakness in CFACTS* procedure in RMH Volume II, Procedure 6.2, *POA&M Management*, then **return to this step**.

This procedure is required to ensure that Weaknesses are properly documented and managed in CFACTS.

12. If a *Finding* exists for the *failed control*, proceed as follows **for each listed finding**:

a. Click on the *View finding(s) for failed control* link.

Opens the List of Security Assessment Findings screen.

b. If the *finding* is **not** already linked to the failed *Test Case*, perform the following:

If the Link to Control(s)/Test Case(s) column contains the Test Number in brackets (e.g., "AC-2 Account Management [AC-2.1]") then it is already linked.

(1) Click on the *Edit* link.

Opens the Edit Finding screen

(2) If the described *Finding* is **not** appropriate for the failed *Test Case*, perform the following:

"Appropriate" means that the Finding accurately describes the failure identified in the failed assessment procedure.

(a) Click on the *Close* button.

Returns to the Self-Assessment screen.

(b) Click on the *View finding(s) for failed control* link.

Opens the List of Security Assessment Findings screen.

(c) Return to Step 12 to address any other *Findings* listed.

(3) If the described *Finding* **is** appropriate for the failed *Test Case*, click on the button in the *Link to Control* field.

*Opens the Linking Weakness to Controls screen. Note that this screen is **also** used to link Findings to Controls.*

(4) Click on the *New* link.

Opens the Manage Controls Associated with Weakness screen.

(5) Select from the *Control* dropdown the appropriate *Control*.

(6) Select from the *Test Number* dropdown the appropriate *Test Number*.

PROCEDURE	PRINCIPLE
(7) Click on <i>Save</i> .	
(8) Click on <i>Close</i> .	<i>Returns to the Self-Assessment screen.</i>
(9) Click on the <i>View finding(s) for failed control</i> link.	<i>Opens the List of Security Assessment Findings screen.</i>
c. Click on the <i>Link to Weakness</i> link for the applicable finding.	<i>Opens the Link Finding to Weakness screen.</i>
d. From the <i>Weakness</i> dropdown, select the <i>Weakness</i> created in Steps 10 and 11.	<i>Links the finding to the applicable weakness.</i>
e. Click on the <i>Add</i> button, then click <i>Close</i> .	<i>Saves the linkage.</i>
f. Click on the <i>Close</i> button.	<i>Returns to the Self-Assessment screen.</i>
g. Click in the <i>Save</i> button.	<i>Refreshes the Self-Assessment screen information.</i>
13. Perform one of the following steps:	
a. Return to Step 5 to create a <i>weakness</i> for other failed assessment procedures, or	
b. Exit this procedure, or	
c. Add additional <i>Milestones</i> to the applicable weakness as follows:	
(1) Click on the <i>View weakness for a failed test case</i> link.	
(2) For the applicable <i>weakness(es)</i> :	
(a) Click on the <i>Weaknesses</i> filed link.	
(b) Add additional milestones in accordance with RMH Volume II, Procedure 6.2, <i>POA&M Maintenance</i> , then return to the beginning of Step 13.	

PROCEDURE

PRINCIPLE

2.3 CREATING A FINDING FROM A FAILED ASSESSMENT

WARNING:

CMS does NOT create Findings from Failed Test Procedures. Instead, proceed to Section 2.2, Remediating a Failed Control Assessment.

*Failed assessment procedures are converted **directly** into Weaknesses and an appropriate POA&M (action plan) must be created.*

Findings that are uploaded from a CMS initiated Audit/Review are converted to Weaknesses by the EISG. Contact EISG at <mailto:ciso@cms.gov>.

2.4 UPLOADING FINDINGS DIRECTLY

*This procedure is used **ONLY** by CMS EISG staff for the purposes of uploading audit and review findings prepared by authorized assessment teams.*

2.4.1 PROCEDURE USERS

1. CMS EISG staff with *CMS-Admin* privileges.

Only CFACTS users with CMS-Admin roles have user access rights necessary to load findings from Finding upload files.

2.4.2 INITIAL CONDITIONS

1. A CMS initiated audit or review has been completed.

*Typically, CMS requires that assessments document **ALL** assessment procedures—including those that Fail. These are then converted directly into Weaknesses. However, some CMS assessors may generate only Findings during the assessments. These must be loaded as Findings, then converted to weaknesses within CFACTS.*

2. A CMS *Findings* spreadsheet has been finalized and submitted to the EISG for data entry into CFACTS.

PROCEDURE

PRINCIPLE

**2.4.3 UPLOADING FINDINGS
DIRECTLY PROCEDURE**

1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.
2. Click on the *Administration* tab.
3. On the *Administration* tab, click on the *edit* link next to the *Upload Findings* field.
4. On the *Findings Upload* screen, click on the *Browse* button.
5. On the *Choose File to Upload* form, navigate and select the applicable Findings upload file.
6. On the *Findings Upload* screen, click on the *Import* button.
7. Convert the uploaded *Findings* to *Weaknesses* in accordance with Section 2.5, *Creating a Weakness from an Existing Finding*.

- Activates the Administration tab.*
- Opens the Findings Upload screen.*
- Opens the Choose File to Upload form.*

- Loads the applicable Findings from the Findings Upload file into CFACTS.*
- This procedure converts Findings directly to Weaknesses, utilizing the information stored within the Findings data fields. Typically, only EISG staff personnel perform a direct Finding conversion to a corresponding Weakness.*

**2.5 CREATING A
WEAKNESS FROM AN
EXISTING FINDING**

2.5.1 PROCEDURE USERS

1. EISG Staff.

PROCEDURE

PRINCIPLE

2.5.2 INITIAL CONDITIONS

1. User has authorized access to the applicable CMS system in CFACTS.

Some user roles may not have the necessary access rights to enter vulnerabilities into CFACTS. Contact the EISG at <mailto:ciso@cms.gov> with questions regarding user roles and their access limits.

a. Refer to RMH Vol II, Procedure 1.1, *Accessing the CFACTS*, for further guidance on gaining authorized access to CFACTS.

2. An applicable *Finding(s)* exists in CFACTS that must be directly-converted to *Weakness(es)*.

Typically, this occurs when a CMS-initiated audit or test results in Finding(s) that are loaded directly into CFACTS using the procedure in Section 2.4, Uploading Findings Directly. Only EISG staff personnel perform a direct Finding conversion to a corresponding Weakness.

3. User has been directed by another procedure to perform actions in this procedure.

2.5.3 CREATING A WEAKNESS FROM AN EXISTING FINDING PROCEDURE

1. Log into CFACTS using RMH Volume II, Procedure 1.1, *Accessing the CFACTS*.

2. Click on the link for the applicable system from either the *Home* screen or the *Browse* Screen.

Opens the applicable system to the Identification tab.

3. Click on the *SA&A Tracking* tab.

Redirects the user to the SA&A tracking screen.

4. Scroll down to the *Risk Assessment* section.

5. In the *RA Wizard* field, click on the *RA Wizard* (ellipsis) button.

Opens the Risk Assessment Wizard screen.

PROCEDURE

PRINCIPLE

6. Scroll down to the *Risk and Safeguards* section, and click on the *Risk Assessment Findings* link.

Opens the List of Security Assessment Findings screen.

7. For each listed Finding to be converted to a weakness, perform the following:

a. Click on the *Accept Finding (Create Weakness)* link.

Opens the Add Weakness screen.

b. Document the weakness details in accordance with the *Documenting a Weakness in CFACTS* procedure in RMH Volume II, Procedure 6.2, *POA&M Management*, then ***return to this step.***

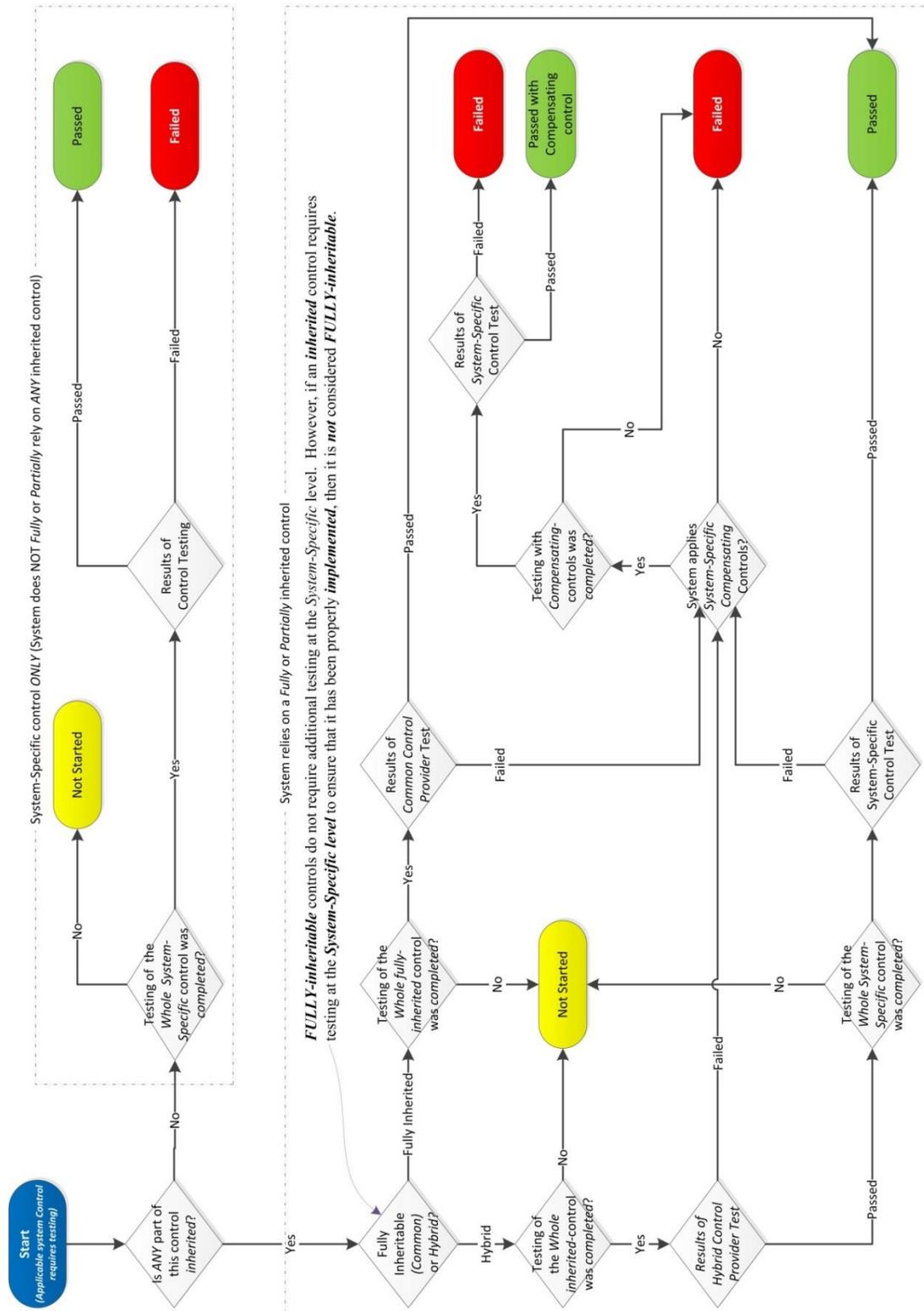
c. Perform one of the following:

(1) Return to Step 4 and repeat for other applicable *Finding(s)*, ***or***

(2) Exit this procedure.

2.6 FIGURES

Figure 1 “Test Result” Logic Diagram



3 APPROVED

Teresa Fryer
CMS Chief Information Security Officer and
Director, Enterprise Information Security Group

This document will be reviewed periodically, but no less than annually, by the Enterprise Information Security Group (EISG), and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of this document, please contact the EISG at <mailto:ciso@cms.gov>.

(This Page Intentionally Blank)