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 6.3
Security Information Review

FINAL
Version 1.0
September 4, 2012

Document Number: CMS-CISO-2012-vII-pr6.3

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN SECURITY INFORMATION REVIEW VERSION 1.0

1. Baseline Version.

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 INTRODUCTION

1.1 PURPOSE

The purpose of the *Security Information Review* procedure is to provide Business Owners, Information System Security Officers, and CMS FISMA Controls Tracking System (CFACTS) users with a systematic guide to review and ensure the accuracy and completeness of security related information for systems in CFACTS. The first *Security Information Review* occurs prior to submitting a request for an Authorization to Operate (ATO). Subsequent reviews are scheduled as needed, but no less than once every 365 days.

1.2 BACKGROUND

By law, each CMS FISMA system must obtain an ATO before it can be placed into operation. Therefore, security controls must be operational, effective, managed, and continuously monitored. Controls must also meet all mandatory requirements, as defined in the current *CMS Information Security Acceptable Risk Safeguards (ARS) CMS Minimum Security Requirements (CMSR)*.

Additional security controls may be implemented to lower the risk associated with the use and operation of an individual information system. Additional controls are usually applied to address unique mission/business process needs and to limit the level of certain risks to CMS, the mission/ business process, the system itself or its environment of operation. These controls must also be operational, effective, managed, and continuously monitored.

Information in CFACTS forms the basis for understanding the risk associated with the use and operation of the system at any point in time. This information must be current, credible, accurate, complete, and in accordance with published CMS procedures. The processes that keep information current can be time-driven (e.g., once a week or every 365 days), event-driven (e.g., changes to the system or its environment of operation, personnel changes, business process changes, discovery of new vulnerabilities, or a weakness remediation is completed), or both time-driven and event-driven. The *Security Information Review* deals with time-driven updates.[1] Three examples of time-driven updates are:

- Scheduled reviews and updates that may be required by ARS controls, such as those that are necessary for keeping security plan, risk assessment, or contingency plan information accurate and current.
- The annual attestation process performed throughout the executive branch of the federal government to determine overall and individual FISMA compliance.
- A planned review and update that occurs prior to ATO renewal requests.

Clearly, there are many possible reasons for scheduling a *Security Information Review*. Business Owners can use the reviews within this procedure independently or together. The procedure

[1] Event driven updates are addressed using RMH Volume II, Procedure 7.8, *Key Updates*.

accommodates consolidation of multiple reviews into one and breaking large reviews into multiple smaller ones.

Please note: Because the sequence of reviews in this procedure follows the expected sequence of tasks as defined in the Risk Management Handbook Volume I Chapter 1, *Risk Management in the* X*LC*, information dependencies will generally flow downward, from one review to those that follow it. If an update is needed in an early review step, there is a high likelihood that one or more subsequent steps will require updates.

1.3 HOW TO USE THIS PROCEDURE

The Security Information Review procedure is broken down into two columns: Procedure and Principle. The Procedure column specifically addresses the steps to perform in order to complete the process. The Principle column provides additional information about the procedure to aid understanding.

1.4 RELATED PROCEDURES

Other relevant *Risk Management Handbook* (RMH) documents include:

- RMH Volume I, Chapter 1, *Risk Management in the XLC*. This chapter provides information required to understand the interrelation of information security, risk management, the CMS eXpedited Life Cycle (XLC), and the system life cycle.
- RMH Volume II, Procedure 2.3, *Categorizing an Information System.* This procedure explains how to establish the system's security category in CFACTS.
- RMH Volume II, Procedure 2.6, *Information System Description*. This procedure explains how to create or update system information in CFACTS.
- RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS*. This procedure explains how to document security controls in CFACTS and is a prerequisite for documenting testing of the applicable security control(s).
- RMH Volume II, Procedure 5.6, *Documenting Security Control Effectiveness in CFACTS*. This procedure explains how to document security control testing, and directs the documentation of identified weaknesses.
- RMH Volume II, Procedure 6.2, *POA&M Management*. This procedure explains how to ensure that *Weaknesses* are properly documented and managed in CFACTS.
- RMH Volume II, Procedure 7.8, *Key Updates*. This procedure explains how to ensure that *Weaknesses* are properly documented and managed in CFACTS. This procedure is required to ensure that all *information* in CFACTS is updated to reflect recent events.

Other relevant procedures that are not yet incorporated into the *Risk Management Handbook* include:

- *CMS System Security Plan (SSP) Procedure.*
- *CMS Information Security Risk Assessment (IS RA) Procedure.*

- *CMS Information Security (IS) Contingency Plan (CP) Procedures.*

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

2 PROCEDURE

PROCEDURE	PRINCIPLE

2.1 PROCEDURE USERS

1. CMS Information System Security Officer (ISSO).

2. Business Partner System Security Officer (SSO).

3. Designated CFACTS data entry person.

2.2 INITIAL CONDITION

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

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

PROCEDURE **PRINCIPLE**

2.3 SECURITY INFORMATION REVIEW PROCEDURE

2.3.1 PRIVACY IMPACT ASSESSMENT REVIEW

1. Review the *Privacy Impact Assessment* (PIA) to determine if it is accurate and current for the information that the system stores, processes, or transmits. To update, contact the Privacy Policy and Compliance Group at mailto:pia@cms.hhs.gov to initiate the necessary changes.

2.3.2 SECURITY CATEGORY REVIEW

1. Review and update as necessary the security category of the information system in accordance with RMH Volume II, Procedure 2.3, *Categorizing an Information System.*

2.3.3 INFORMATION SYSTEM DESCRIPTION REVIEW

1. Review and update as necessary system information in accordance with RMH Volume II, Procedure 2.6, *Information System Description, using the Creating or Updating System Information in CFACTS procedure.*

PROCEDURE **PRINCIPLE**

2.3.4 SYSTEM BOUNDARY REVIEW

1. Review and update as necessary system boundary information in accordance with *CMS System Security Plan (SSP) Procedure*, section 3.1.1 and the portion of Appendix A (page 29) entitled "Boundary Issues".

2.3.5 SECURITY CONTROLS REVIEW

2.3.5.1 REVIEW SECURITY CONTROL DESCRIPTIONS

1. Review and update as necessary system information in accordance with RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS.*

2.3.5.2 REVIEW SECURITY CONTROL EFFECTIVENESS

1. Review and update as necessary system information in accordance with RMH Volume II, Procedure 5.6, *Documenting Security Control Effectiveness in CFACTS.*

2.3.6 BUSINESS RISK REVIEW

1. Review and update as necessary the business risk table in accordance with *CMS Information Security Risk Assessment (IS RA) Procedure*, sections 4.3, 4.4 and the portion of Appendix A (pages 36-38) entitled *RISKS AND SAFEGUARDS TABLE*.

PROCEDURE	PRINCIPLE
2.3.7 INFORMATION SYSTEM RISK REVIEW	
1. Review and update as necessary the information system risk table in accordance with *CMS Information Security Risk Assessment (IS RA) Procedure*, sections 4.3, 4.4 and the portion of Appendix A (pages 36-38) entitled *RISKS AND SAFEGUARDS TABLE*.	
2.3.8 CONTINGENCY PLANNING REVIEW	
1. Review business continuity and system contingency planning objectives by evaluating the following:	
a. Evaluate to determine if the *Maximum Tolerable Disruption (MTD)* for the business has changed in the past year.	*The MTD is the maximum time a business can tolerate the absence or unavailability of a particular business function. This includes the maximum time for restoring the IT systems, plus the additional time (not associated with recovering the information technology) necessary to recover the* business *back to a normal state. (MTD=RTO+WRT [see below])*
b. Evaluate to determine if the *Recovery Time Objective (RTO)* for the system has changed in the past year.	*The RTO is the maximum time a business function can be disrupted/not available before it causes serious and irreversible impact.*
c. Evaluate to determine if the *Recovery Point Objective (RPO)* for the system has changed in the past year.	*The RPO is the amount or extent of data loss that can be tolerated by your business functions. For instance, If a system fails, how much data loss can the business tolerate (that might result from recent data collected but not backed-up, thus not recovered)?*

PROCEDURE	PRINCIPLE
d. Evaluate to determine if the *Work Recovery Time (WRT)* for the business has changed in the past year.	*The WRT is the time it takes to get critical* business *functions back up and running once the systems (hardware, software, and configuration) are restored to the RPO. This includes the manual processes necessary to verify that the system has been restored to the RPO, and all necessary processes have been completed to address the remaining lost, or out-of-synch, data or business processes.*
2. Update the *CP*, as required, to address the issues identified from the evaluations performed in Step 1.	
3. Review and update as necessary the Contingency Plan in accordance with *CMS Information Security (IS) Contingency Plan (CP) Procedures.*	
2.3.9 POA&M REVIEW	
1. Review and update as necessary POA&M information in accordance with RMH Volume II, Procedure 6.2, *POA&M Management.*	

3 APPROVED

teresa.fryer@cms.hhs.gov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2012.09.20 13:17:53 -04'00'

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.hhs.gov.

(This Page Intentionally Blank)