CENTERS for MEDICARE & MEDICAID SERVICES
Enterprise Information Security Group
7500 Security Boulevard
Baltimore, Maryland 21244-1850

ESG
Enterprise Information
Security Group
Risk Management, Oversight,
And Monitoring

Risk Management Handbook
Volume II
Procedure 4.5
Contingency Plan Exercise

FINAL
Version 1.0
November 6, 2014

Document Number: CMS-CISO-2014-vII-proc4.5

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *CONTINGENCY PLAN EXERCISE* PROCEDURE VERSION 1.0, DATED NOVEMBER 6, 2014

1. Baseline Version. This document, along with its corresponding Risk Management Handbook (RMH), Volume III Standard, replaces *CMS Contingency Plan Tabletop Test Procedures*, dated July 25, 2007, and its imbedded *CMS CP Tabletop Test - After Action Report.*

(This Page Intentionally Blank)

TABLE OF CONTENTS

(This Page Intentionally Blank)

1 INTRODUCTION

1.1 PURPOSE

The purpose of the *Contingency Plan Exercise* procedure is to provide Centers for Medicare & Medicaid Services (CMS) Business Owners, Information System Security Officers (ISSOs) and Contingency Plan Coordinators (CPCs) a systematic guide to developing, coordinating, conducting, and reporting Contingency Plan (CP) exercises.

This procedure provides guidance for consistently performing the following steps:

- Developing exercise objectives.
- Developing viable exercise scenarios.
- Determining participating personnel.
- Determining exercise logistics.
- Conducting an exercise.
- Developing the requisite After Action Report (AAR).

1.2 BACKGROUND

As custodians of citizen-based and other federal information, CMS Business Owners share the responsibilities to protect information and systems. Regular testing of information system CPs is one of the primary ways of ensuring that this responsibility is met. A critical factor for maintaining on-going compliance with the *Federal Information Security Management Act of 2002 (FISMA)* is for Business Owners, in coordination with appropriate technical personnel, to annually test their CPs and dedicate sufficient resources to accomplish this test. These resources include budget (if external resources are to be used to support the testing), and person hours (if internal personnel are to be engaged in this activity). Business Owners are required to schedule and perform the CP test; and oversee the development and completion of corrective action plans for vulnerabilities noted during the testing.

The processes provided in this procedure provide the instructions for developing, executing, and documenting CP testing. The processes provided in this procedure require specific actions on the part of the CMS Business Owners, System Developers/Maintainers, and ISSOs.

Business Owners are required to address CP testing as part of the annual attestation. Copies of each year's CP Exercise Plan and AAR are uploaded to the appropriate repositories in the *CMS FISMA Controls Tracking System (CFACTS)*. It is expected that Business Owners will rely on System Developers/Maintainers and ISSOs to assist in meeting these testing and reporting requirements.

1.3 HOW TO USE THIS PROCEDURE

This 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 applicable information about the specific procedural step to aid understanding. However, it is assumed that the user possesses a minimal understanding of the subject-matter.

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 Risk Management Framework and the interrelation of information security, risk management, the CMS XLC, and the system life cycle.
- 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 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 is required to create or update system information in CFACTS.
- RMH Volume II, Procedure 4.2, *Documenting Security Controls in CFACTS*. This procedure is required 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 is required to document security control testing, and directs the documentation of identified weaknesses.
- 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 6.3, *Security Information Review*. This procedure provides a systematic guide to review and ensure the accuracy and completeness of security related information for systems 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.
- RMH Volume III Standard 4.4 *Contingency Planning Standard*. This standard provides the overarching policies.

Other relevant procedures that are not yet incorporated into the RMH include:

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

Other relevant guidance may be found in SP 800-84 *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.*

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 PROCEDURES

PROCEDURE **PRINCIPLE**

2.1 CONTINGENCY PLAN EXERCISES

2.1.1 PROCEDURE USERS

1. CMS Business Owners.

2. CMS Information System Security Officer (ISSO).

3. CMS Contingency Plan Coordinator (CPC).

4. CP Exercise Facilitator.

PROCEDURE **PRINCIPLE**

2.1.2 INITIAL CONDITIONS

1. The Business Owner has approved the *Maximum Tolerable Downtime (MTD)* of the function(s) that is/are supported by the system, the *Recovery Time Objective (RTO)* of the system, the *Recovery Point Objective (RPO)* of the associated data, and the Work Recovery Time (WRT) of the associated functional processes[1].

Every CMS information system and application is required to have an associated recovery prioritization.

The recovery prioritization is determined through identifying the criticality of the functions that are performed and the reliance of those functions on the supporting systems.

Within the XLC, the business MTD must be determined first, from which system RTOs and data RPOs must be identified. All of this occurs in the Initiation, Concept, and Planning Phase and finalized during the Requirements Analysis segment of the Requirements Analysis and Design Phase.

The RMH Volume 1, Chapter 1 Risk Management in the XLC is available in the Information Security Library.

2. An up-to-date CP for the system has been developed and approved by the CMS Business Owner.

Every CMS information system is required to have an Information System Contingency Plan (CP). Every CP must be reviewed and updated in accordance with the CMS Acceptable Risk Safeguards (ARS).

Within the XLC, CP development starts during the Concept segment of the Initiation, Concept, and Planning Phase and completes during the Development segment of the Development and Test Phase. RMH Volume I Chapter 1 Risk Management in the XLC *provides further guidance.*

[1] The concepts and definitions associated with MTD, RTO, RPO, and WRT are described in detail in RMH Volume III, Standard 4.4, *Contingency Planning*. These metrics are critical CP items. If these have not been established in the CP, then meaningful testing of the CP cannot be completed.

PROCEDURE	PRINCIPLE
3. Personnel with information system recovery responsibilities have been trained in their responsibilities. Exercises may be leveraged to fulfill CP training requirements.	*Personnel with recovery roles and responsibilities are to be assigned to teams.* *All team members must be trained and ready to respond in the event of a disruptive situation requiring plan activation.* *Training refers to instilling skills in personnel with regards to their roles and responsibilities.*

2.1.3 CP EXERCISE PREPARATION

1. Review the CFACTS CP control descriptions to ensure the plan as exercised is consistent with existing control requirements and implementation descriptions.	*If there have been any changes to any of the CP control requirements, there may be a need to update the approved recovery strategies.*
2. Review the documented information system and business risks for any changes to the business process MTD, threats, vulnerabilities, or likelihood of occurrence for existing threats	*If there have been any changes to the MTD or risk posture of the system, there may need to be a change to the approved system recovery metrics.* *It is more meaningful to exercise participants to use realistic events with a high likelihood of occurrence when developing exercise scenarios and conducting the actual exercise.*
3. Determine the type of exercise in accordance with *RMH Volume III Standard 4.4 Contingency Planning.*	*Verify the type of exercise to be conducted with the Business Owner and the ISSO.*
4. Determine and plan for the necessary logistics and supplies.	*Logistics and supplies may include: conference room, teleconference bridge, white board and markers, note sheets for the data gatherers, etc.*

2.1.4 DEVELOPING THE CP EXERCISE PLAN

PROCEDURE	PRINCIPLE
1. Determine the objectives of the exercise and document them in Section 2.3, *Tabletop Exercise Scenario and After Action Report* , as follows:	*This step is based on the information obtained from the initial research into CP controls, recovery metrics and exercise type. RMH Volume III Standard 4.4* CP Standard *provides the minimum objectives for each type of exercise.*
a. The *objectives* of the exercise must include but are not limited to validation of the following:	*Objectives should be succinct statements of intent against which exercise success can be measured, (e.g. the purpose of an exercise is to: Validate the information and procedures in the CP; Determine if the plan must be updated; and Train personnel assigned to recovery roles).*
(1) MTD.	*Functional recovery is the purpose behind all recovery planning* *All CP exercises must ensure all functional MTDs can be met and if not, either adjust the MTD(s) or upgrade the recovery procedures to reduce the amount of time permitted for the RTO.*
(2) RTO.	*In order to ensure functional recovery, critical systems must be recovered quickly enough to allow for system operations, data loading and validation and backlog processing.* *If the system cannot be recovered quickly enough to meet the functional MTD(s) then the recovery strategy must be upgraded to reduce the time required for the RTO*

PROCEDURE	PRINCIPLE
(3) RPO.	*In order to ensure functional recovery, within the approved MTD, the maximum acceptable amount of data loss, expressed as a time from the last backup, cannot exceed this time value.* *If data recovery and validation are insufficient to support the functional MTD(s) then the data backup strategy must be upgraded to support a more current (shorter) RPO.*
(4) WRT.	*In order to ensure the functional MTD(s) can be met, the time it takes to validate recovered data, update all data to current day and time and clear any transaction backlogs must be addressed* *If an exercise determines that the functional MTD cannot be met after the system is recovered within its RTO, and the data is recovered within its RPO, then all recovery strategies may need to be upgraded. See section 2.1.1.5 of the CP Standard RMH Volume III, Standard 4.4 for examples of work recovery scenarios as they pertain to WRT.*
(5) Validation of response and recovery procedures.	*WRT must be validated to ensure that the RTO and the processes necessary to achieve a normal state of functionality to include transactions are properly validated and do not exceed the MTD.*
(6) Verification of Call tree information.	*Valid names and contact information are needed. Corrections to this list should also be made to the plan document.*
(7) Identify weaknesses in the CP.	*A weakness is defined as any inaccuracy or error.*

PROCEDURE	PRINCIPLE
2. Determine the time-frames for the exercise.	*Each exercise requires two time-frames. The actual time that is set aside for the exercise (normally 1 to 4 hours) and the elapsed time, which must be of sufficient length to encompass the system RTO, data RPO and the MTD of the function that relies on the system being tested.*
a. Determine the amount of time the exercise will take.	
b. Determine the virtual timeline to ensure the scenario is of sufficient length to exercise the approved CP recovery strategies.	*The actual CP may take five days to complete. However during the exercise, participants may have only one hour to complete the test. Therefore, the elapsed time for the exercise must be sufficient to accommodate the entire scenario.*
3. Based on the objectives and time frame, determine the personnel who are required to attend in accordance with the CP and *RMH Volume III Standard 4.4 Contingency Planning*.	*Exercise roles should include, but not be limited to the following:* *- Facilitator* *- Data Gatherers* *- Participants*
4. The personnel involved in the exercise are those who are designated with recovery roles in the CP.	
a. The exercise *facilitator* is the Business Owner or designee. The facilitator is responsible for:	
(1) Obtaining approval for the CP Exercise Plan.	*Approval shall be granted by the Business Owner.*
(2) Ensuring all personnel involved with the exercise are notified.	
(3) Providing pre-exercise and post-exercise briefings as required.	
(4) Conducting the exercise in accordance with the exercise plan;	
(5) Developing the AAR.	

PROCEDURE	PRINCIPLE
b. Data gatherers should be the ISSO, CPC or their designees and other functional experts as appropriate. They are responsible for:	*The data gatherers may be participants but have the additional requirement to observe and collect information on the execution of the exercise.*
(1) Reviewing and being familiar with all information and procedures in the CP.	
(2) Reviewing and being familiar with the business processes that rely on the system to be exercised.	
(3) Reviewing and being able to determine, with the participants, when recovery procedures or other information in the CP do not meet the requirements of an effective CP.	
c. The participants are those personnel who have recovery responsibilities that are germane to the scope of the exercise as determined by the facilitator and approved by the Business Owner.	
5. If the exercise is a technical exercise, coordinate with appropriate Information Technology (IT) infrastructure personnel for technical recovery expertise.	*The term, "technical exercise" denotes an exercise in which an actual failover/recovery will occur on the alternate system*
6. Determine the assumptions or other limitations under which the exercise will be conducted.	

PROCEDURE	PRINCIPLE
7. Develop the exercise injects.	*Injects in this case refer to the Master Scenario Events List (MSEL) as defined in SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.* *Injects are prompts that are given to the participants at appropriate points in the exercise that enable the exercise to continue in the absence of actual recovery activities.* *Examples of exercise injects are:* *Anomalous system behaviors as reported by the user community that require follow up and damage assessment,* *Damage assessment results,* *The "all clear" from the fire department,* *Telecommunications connectivity issues and report of service restoration.*
8. Record the exercise information in the scenario format in Section 2.3, *Tabletop Exercise Scenario and After Action Report* .	
9. Establish a day-and-time for the exercise and obtain approval from the Business Owner and the ISSO/CPC.	

2.1.5 CONDUCTING THE CP EXERCISE

1. Ensure all personnel who have been identified in the exercise plan are present. For any absentees, ensure a viable replacement is present.	*A viable replacement is someone with the same knowledge base, skill level, and expertise of the individual who was initially identified.*
2. Ensure all personnel have the requisite information.	*Facilitator should have; the CP, exercise scenario, Injects, and evaluation sheets.* *Participants should come to the exercise with their own copy of the CP. If they do not, this should be recorded as a deficiency/finding.*

PROCEDURE **PRINCIPLE**

3. The facilitator kicks off the exercise by presenting the senior participant with the initial inject.

4. The team will follow the documented CP step by step.

5. As the participants respond to the first inject and each subsequent inject, the facilitator facilitates discussion (regarding the recovery procedures in the CP) until normal operations would have been restored.

6. Upon conclusion, the facilitator should have a quick discussion with the data gatherers to determine when their notes are due.

Data gatherers' notes should be submitted quickly enough to allow the facilitator to submit the rough AAR to the data gatherers in order to receive feedback and subsequently submit the final report to the Business Owner on or before the due date.

2.2 POST EXERCISE ACTIVITIES

2.2.1 PROCEDURE USERS

1. CMS ISSO.

2. CMS CPC.

2.2.2 INITIAL CONDITIONS

1. The CP exercise has been completed.

The person who has control over the exercise will declare exercise completion.

PROCEDURE **PRINCIPLE**

2.2.3 POST EXERCISE PROCEDURE

1. Conduct an initial out-brief with all persons identified in the scenario and record any lessons learned in the format provided in Section 2.3, *Tabletop Exercise Scenario and After Action Report* .

2. Collect all logs and exercise-related documentation from all personnel who participated.

3. Review all narrative comments.

4. In the event of a discrepancy between two participants (or data gatherers) giving different results for the same objective, discuss the results with them and, if possible, come to agreement.

On occasion, individuals may have totally different perceptions regarding the results. This is valid.

5. When all results conflicts have been resolved, develop the AAR with significant results.

6. Include in the AAR any recommendations for improvements to any area of the system’s recovery plan or overall recovery capability

7. Attach the completed *Exercise Scenario* to the AAR.

8. Submit the AAR to the Business Owner for review and approval

9. Update the CP with the exercise results, lessons learned, and any comments provided by the Business Owner.

10. Update CP training materials to reflect necessary changes to the CP as a result of the exercise and lessons learned.

2.3 TABLETOP EXERCISE SCENARIO AND AFTER ACTION REPORT FORMAT

2.3.1 EXERCISE SCENARIO FORMAT

System:	Date:
Type of Exercise:	Planner:

Exercise Facilitator(s) (Sample)

Facilitator Name
Facilitator Name

Exercise Data Gatherers (Sample)

Data Gatherer’s Name
Data Gatherer’s Name

Exercise Participants (Sample)

Name	Role
Name	Role
Name	Role
Name	Role
Name	Role

Timelines

Actual exercise time:
Exercise (simulated) time:

Exercise Objectives (Sample)

Objective 1
Objective 2
Add additional objectives as necessary:

Exercise Scenario (Sample)

Incident:
Impact to system(s):
Impact to Operation(s):

Required Supplies and Documentation (Sample)

Assumptions:

- Assumption 1
- Assumption 2
- Assumption 3
- Assumption 4

Lessons Learned

Objective Fulfillment (Sample)

Objective 1	This objective was/was not met. Specifically;
Objective 2	This objective was/was not met. Specifically;
Add additional objectives	as necessary

Evaluation Sheet (Sample)

Objective 1:
Comments:
Objective 2:
Comments:

(Note: add additional objectives as necessary)

____

(Print data gatherer's name)

____

(Data Gatherer's signature and date)

2.3.2 AFTER ACTION REPORT FORMAT

INTRODUCTION

A Tabletop Exercise was conducted for the <System Name> (<system acronym>) Information System Contingency Plan (CP) on <date>. The participants and their assigned roles are listed below.

Name	Organization	Roles/Responsibility	Phone number
		Exercise Facilitator.	
		CP Coordinator. Ensures accurate damage assessment, and recovery.	

Name	Organization	Roles/Responsibility	Phone number
		Exercise Data Gatherer	
		Recovery Management Team Member. Ensures accurate damage assessment, and system recovery.	
		<System name> Technical lead. Ensure <system> is recovered to trusted state and verifies all processing and data integrity.	

The CP tabletop exercise was conducted in accordance with the <insert system name> CP Exercise Plan, dated <insert Exercise Plan date>. The exercise plan was developed around the following scenario:

<Provide a synopsis of the scenario>

The exercise was developed to determine the following <Insert objectives below>:

- Determine weaknesses in the contingency plan.
- Objective 2.
- Objective 3.
- Add additional objectives as necessary.

The CP exercise evaluated the status of contingency planning for the system and provided a forum for identifying outdated contingency planning information and for providing updates as required. The exercise plan and detailed results are contained in the Appendix to this report.

1. Summary of Exercise Results

Significant results from the exercise were:

- Result one.
- Result two.
- Result three.
- Etc.

2. Recommendations

The following recommendations are provided as a result of the exercise:

- Recommendation one.
- Recommendation two.
- Recommendation three.
- Etc.

Submitted by:

____

<Name of the facilitator> Date

Facilitator

____

Approved by

____

<Name of CMS Business Owner> Date

<Insert System Acronym> Business Owner, <title>

< Insert Appendix material here>

<End of Formats>

3 APPROVED

Teresa Fryer

Digitally signed by Teresa Fryer
DN: cn=Teresa Fryer, o, ou, email=teresa.fryer@cms.hhs.gov, c=US
Date: 2014.11.13 13:44:53 -05'00'

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.gov*.*