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 III
Standard 4.4
Contingency Planning

FINAL
Version 1.0
February 28, 2014

Document Number: CMS-CISO-2014-vIII-std4.4

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN CONTINGENCY PLANNING VERSION 1.0

1. Baseline Version. This document, along with its corresponding *Risk Management Handbook (RMH)*, Volume II Procedure, replaces *Centers for Medicare & Medicaid Services (CMS) Contingency Planning Procedures* dated November 14, 2008.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

(This Page Intentionally Blank)

1 INTRODUCTION

Continuity planning is the practice of ensuring an organization's ability to continue the execution of essential functions through all circumstances and is a fundamental responsibility of all Centers for Medicare & Medicaid Services (CMS) management.

Information Systems[1] play a vital role in CMS' core business processes. It is critical that services provided by CMS remain available and that applications that enable those services continue to operate effectively and with minimal interruption. The information system Contingency Plan (CP) provides instructions, disaster declaration criteria, and procedures to recover information systems and associated services after a disruption. Interim measures, or recovery strategies may run the gamut from hot failover to an alternate processing facility or merely delays in recovery until replacement hardware and/or software can be procured, configured, and brought on line.

1.1 BACKGROUND

CMS is reliant on its information systems for mission fulfillment. Information systems are susceptible to a wide variety of events and threats that may affect their ability to process, store and transmit raw data and information. Contingency planning is one method of reducing risk to CMS' operations by providing prioritized, efficient, and cost effective recovery strategies and procedures for the organizations' Information Technology (IT) infrastructure.

The CMS Contingency Planning Standard is consistent with the guidance of the National Institute of Standards and Technology (NIST) and most specifically with NIST Special Publication (SP) 800-34 revision 1, *Contingency Planning Guide for Federal Information Systems*[2] dated May 2010. Effective contingency planning requires clear and concise:

- Disaster declaration criteria, and
- Recovery prioritization.

These, in turn, require:

- Accurate identification of functions performed by the system,
- Accurately mapping any functions that rely on other systems,
- Determining impact to the organization for loss of any or all functions (and thereby determine functional recovery prioritization),

[1] An *information system* is defined as *"A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information"* in the CMS Risk Management Handbook (RMH), Volume I, Chapter 10, *CMS Risk Management Terms, Definitions, and Acronyms*. *available at* http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

[2] SP 800-34 revision 1, *Contingency Planning Guide for Federal Information Systems is available from* http://csrc.nist.gov/publications/PubsSPs.html

- Determining the recovery requirements for each function, and
- Using the functional prioritization scheme, system reliance, and interdependencies to determine the information system recovery prioritization.

1.2 CONTINGENCY PLANNING REQUIREMENTS

The following requirements apply:

- All business owners must develop CPs for each information system to meet operational needs in the event of a disruption.
- Implementation procedures shall be documented in a formal CP developed by system developers/maintainers, reviewed by the Information System Security Officer (ISSO) or the Contingency Plan Coordinator (CPC), and approved by the business owner with a copy provided to the Chief Information Security Officer (CISO).

Each Business Owner will:

- Actively participate in the determination of Maximum Tolerable Downtime (MTD) [3], Recovery Time Objective (RTO) [4], Recovery Point Objective (RPO) [5], and Work Recovery Time (WRT) [6] determinations;
- Review each of their CPs annually and ensure either the ISSO or CP Coordinator updates plans as necessary.
- Ensure CPs assign specific responsibilities to designated staff and elements of the CP recovery team to facilitate the recovery of each system within approved recovery periods.
- Ensure the necessary resources are available to ensure a viable recovery capability.
- Ensure that personnel who are responsible for systems recovery are trained to execute the contingency procedures to which they are assigned.
- Ensure CPs are exercised annually.

The CPCs and/or ISSOs shall observe all exercises and document instances where appropriately trained personnel were unable to complete the necessary recovery procedures. Such shortcomings are caused by weaknesses in the plan and contingency plans will be adjusted to correct the identified plan deficiencies.

[3] MTD *(Maximum Tolerable Downtime)* is the amount of time mission/business process can be disrupted without causing significant harm to the organization's mission. (SP 800-34)
[4] RTO *(Recovery Time Objective)* is the overall length of time an information system's components can be in the recovery phase before negatively affecting the organization's mission or mission/business processes. (SP 800-34)
[5] RPO is the point in time to which data must be recovered after an outage. SP 800-34 (revision 1) dated May, 2010. RPO is the requirement for data currency and validates the frequency with which backups are conducted and off-site rotations performed.
[6] WRT *(Work Recovery Time)* 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.

Annual exercises will be used to verify the viability of each CP and are not intended to test the technical competence of individual personnel. The primary purposes of annual CP exercises are:

- Identify weaknesses in each plan
- Train personnel in their recovery responsibilities to ensure viable recovery capabilities.

2 CONTINGENCY PLANNING PHASES

There are four basic phases in contingency planning: *Preparedness, Alert and Notification, Recovery, and Reconstitution*.

2.1 PREPAREDNESS PHASE

The ***Preparedness Phase*** is the process of establishing policies, processes, procedures, agreements, and preparatory analysis that are the necessary foundations for all aspects of recovery planning.

By establishing contingency policies, procedures and agreements in advance, and conducting up-front requirements analysis, CMS management can determine and implement the most cost effective and efficient recovery strategies. Within the CMS environment, this *Standard* and the associated Risk Management Handbook (RMH) *Procedures* lay the foundations for CP implementations.

The best way to recover from an event is to have strategies in place that preclude the impacts of an event from becoming a disaster in the first place. Prevention and mitigation strategies will be based on the information obtained from business risk assessments, information system risk assessments, and any applicable system Business Impact Analysis (BIA), subject to program constraints, cost-benefit analysis, and operational experience.

Some events cannot be avoided such as hurricanes, tornadoes, and regional power outages. However, there are others (e.g. unintentional human error) that can be avoided or, at least, have the likelihood of occurrence reduced to "acceptable" levels. It is incumbent upon all business owners to take the following steps to minimize the number and impact of events that could lead to a disaster declaration:

- Include major threat factors that cause disruptions in business risk analyses and maintain current the potential impact of resulting risks as well as the status of mitigations to reduce such risks;
- Formulate, maintain, and communicate business disruption risks in the form of a business risk posture to guide system efforts relating to handling system disruptions;
- Develop and implement recovery policies and procedures;
- Assimilate recovery-related and recovery-mitigation procedures into daily operations;
- Promote cross training to reduce reliance on single individuals who may or may not be available should an event occur;

- Coordinate with the hosting infrastructure (data center) to ensure backups are conducted and moved to an off-site location commensurate with RPO requirements;
- Ensure backups are available within designated time frames to support overall recovery objectives; and
- Verify back-up and recovery procedures. Business owners and ISSOs should be aware of backup storage locations, and know who has access to backups.

2.1.1 CRITICAL RECOVERY METRICS

Business owners should establish and have a clear understanding of the functions, processes, and applications that are critical to CMS and the point in time when the impact(s) of the interruption or disruption becomes unacceptable to the entity. These timeframes or recovery goals are the factors that drive recovery options (strategies) and cost. These recovery goals are:

- MTD of each mission/business process;
- RTO of each system that is used to enable each of those functions;
- RPO of the data; and
- The WRT for each function;

Recovery requirements for each function include but are not limited to:

- Personnel/skill sets;
- Essential records;
- One-off work stations;
- Specialized office equipment;
- Short term impact on delivery of services to beneficiaries;
- Short term impact on delivery of services to providers;
- Short term operational impact to system users;
- Short term operational impact to all databases for which the application provides either raw data or information;
- Cost of lost productivity;
- The backlog that may accrue for every hour or day that the system is unavailable;
- The length of time it would take to catch up with all backlogged transactions while still processing new requirements (or until new requirements can be processed);
- The point in time when it may be necessary to shift resources from other functions to assist with clearing the backlog, causing a “domino effect” of the disaster; and
- The point in time at which too much data or too many transactions have been lost, causing public recognition of the disaster and negative impact to the reputation of CMS.

2.1.1.1 MAXIMUM TOLERABLE DOWNTIME (MTD)

The foundation of all recovery planning is the prioritization of business processes and functions. The MTD for each business process/function is established during the Information System Description task of the NIST Risk Management Framework. This task occurs during the Initiation, Concept, and Planning phase of the eXpedited Life Cycle (XLC), as explained in the *Risk Management Handbook (RMH) Volume I Chapter 1 Risk Management in the XLC*. Each business owner ensures identification of the following information:

- The relevant business process(es) and function(s),
- A quantified statement of the potential Impact an outage has on the business process, and
- The MTD for each individual business process.

Table 1 is an example of the MTD determination for a hypothetical function.[7]

Table 1 MTD Determination

Business Function	Potential Impacts	Maximum Tolerable Downtime
Claims Processing	Operations – more than 1000 customers affected nationally	72 hours
	Reputation –congressional interest	30 hours
	Reputation – media interest	36 hours
	Customer Service – Over 500 beneficiary complaints	36 hours

Document results in the business risk assessment during the Initiation Concept, and Planning phase of a project. Later in the project, during development of the system contingency plan, place the MTD values in Appendix G.

2.1.1.2 RECOVERY TIME OBJECTIVE (RTO)

Determining the information system resource RTO is crucial for selecting appropriate technologies that are best suited for ensuring IT system recovery to support the functional MTD. The RTO determination occurs during the Requirements Analysis and Design phase of a project as required by *RMH Volume I Chapter 1 Risk Management in the XLC*. The RTO must be fast enough to ensure that the MTD can be attained. IT infrastructure **cannot have an RTO longer than the shortest RTO of any application that is hosted on it**. If a function can be recovered without a given system, then that system's RTO may be longer than the function MTD. However, if the function cannot be recovered for any length of time without the given system, the RTO must be significantly shorter than the MTD because:

- It takes time to reprocess data that is restored from backups. The additional processing time must be added to the RTO to stay within the time limit established by the MTD; and

[7] The following data points are for example only and are not meant to represent an actual situation.

- It takes time to process data created after the last backup that was taken off-site.

The RTO will be documented in the information system description during the Requirements Analysis and Design Phase of the project. Once the RTO is determined, add it to CP Appendix G when developing that document.

2.1.1.3 RECOVERY TIERS

A clearly defined RTO and associated recovery tier will be applied to each system in accordance with the table below. Table 2 depicts the Enterprise Data Center (EDC) recovery tier structure to assist in enterprise-wide recovery planning.

Table 2 Recovery Tiers

Tier	Recovery Time Objective (RTO)
Tier 1	less than 1 day
Tier 2	1 - 5 days
Tier 3	6 - 29 days
Tier 4	30 days or more

2.1.1.4 RECOVERY POINT OBJECTIVE (RPO)

The RPO, expressed as a time (e.g. 24 hours' worth of data) defines the maximum acceptable amount of data that can be lost due to a disruptive event. The RPO validates or repudiates the current back up schema and determines the data backup strategy. The Business Owner and the IT infrastructure maintainer must both agree to the RPO.

Regarding backup strategies:

- Shorter RPOs have fewer strategies that can meet those requirements and those strategies are more expensive than strategies that support longer RPOs.

The MTD is impacted by the RPO and the requisite backup strategy, because the amount of data loss directly affects the amount of work and processing that must be done after the system is restored, before business operations become current. Generally:

- Longer RPOs require longer WRTs before a function is fully recovered.
- Shorter RPOs have shorter WRT efforts before a function is fully recovered.

2.1.1.5 WORK RECOVERY TIME (WRT)

It is relatively easy to determine functional MTDs and IT system RTOs. However, determining WRT may not be as easy, as there is no federal regulation or guidance that addresses this concept. The best way to determine WRT is first to have an approved functional MTD, which will be the longest timeframe for any recovery requirement.

The relationship between RTO, WRT and MTD can be stated as a simple equation, i.e. RTO + WRT = MTD. **Any system RTO and functional WRT combined cannot exceed the function MTD.**

Then take into account the amount of *acceptable* data loss (established by the RPO), backlog accrual since the recovery point, data validation, and any other operational procedure that impedes the ability to bring back a function to the point of processing new transactions on a current basis. For an example[8] the following tables are provided as notional scenarios with the following parameters:

- The functional MTD is three (3) days;
- The system RTO is one (1) day;
- The RPO of 96 hours is based (in this example) on the backup scheme in the host data center in which daily backups are maintained onsite for three days at which time the tapes are sent to the offsite storage facility; and
- For every day the function is not performed, 1 day of work accrues.

Some examples that illustrate how RPO, WRT, and RTO can affect meeting the MTD requirement are illustrated in scenarios 1 through 5 that are contained in Table 3 through Table 7, respectively.

Table 3 Work Recovery Scenario 1

Days	1	2	3	4	5	6 (Saturday)	7 (Sunday)
Backlog	5	6	7	8	9	9	9
Recovery Work Achieved	0	1	2	3	4	5	6
Cumulative Backlog	5	5	5	5	5	4	3

Scenario 1 above depicts a **standard eight-hour day, but working 7 days per week.** The initial five-day backlog assumes the only available backups are those that are stored at the offsite facility, i.e. worst-case scenario. Since the only adjustment was to work through the weekend, fully recovered functionality would not be achieved until the following weekend. **The functional MTD would not be met.**

Table 4 Work Recovery Scenario 2

Days	1	2	3	4	5	6 (Saturday)	7 (Sunday)
Backlog	5	6	7	8	9	9	9
Recovery Work Achieved	0	2	4	6	8	9	----
Cumulative Backlog	5	4	3	2	1	0	----

[8] The following data points are for example only and are not meant to represent an actual situation.

Scenario 2 reflects **implementing 16 hour days through two 8-hour shifts.** It would take halfway through the sixth day to clear the backlog and achieve a fully recovered function. **The functional MTD would not be met.**

Table 5 Work Recovery Scenario 3

Days	1	2	3	4	5	6 (Saturday)	7 (Sunday)
Backlog	3	4	5	6	7	7	7
Recovery Work Achieved	0	1	2	3	4	5	6
Cumulative Backlog	3	3	3	3	3	2	1

Scenario 3 shows the results of **maintaining 8-hour workdays but reducing the RPO to 24 hours by moving backup tapes to offsite storage within 48 hours.** It would take halfway through the following Saturday to clear the backlog and achieve a fully recovered function. **The functional MTD would not be met.**

Table 6 Work Recovery Scenario 4

Days	1	2	3	4	5	6 (Saturday)	7 (Sunday)
Backlog	3	4	5	5	----	----	----
Recovery Work Achieved	0	2	4	5*	----	----	----
Cumulative Backlog	3	2	1	0	----	----	----

Scenario 4 **depicts an RPO reduction to 24 hours by moving backup tapes to offsite storage within 48 hours and implementing a 16-hour day with two 8-hour shifts**. It would take until halfway through day 4 to clear the backlog and achieve a fully recovered function. **The functional MTD would be met.**

Table 7 Work Recovery Scenario 5

Days	1	2	3	4	5	6 (Saturday)	7 (Sunday)
Backlog	5	6	7	8	----	----	----
Recovery Work Achieved	0	3	6	8*	----	----	----
Cumulative Backlog	5	3	1	0	----	----	----

Scenario 5 shows the results of **maintaining an RPO of 96 hours and implementing three 8-hour shifts**. With this implementation, the backlog would not be cleared and full functionality would not be achieved until the first shift on the third day. **The functional MTD would be met.**

2.1.1.6 CYCLICAL RECOVERY TIME OBJECTIVE (RTO) ADJUSTMENTS

Should this system incur an operational *peak* where the RTO becomes shorter, or an operational *ebb* where recovery can be delayed, the RTO adjustment will be annotated as indicated in Table 8. Operational peaks and ebbs do not invalidate system RTOs that have been determined. The CP will identify the "normal" RTO as well as any cyclical adjustments in Appendix G.

Table 8 RTO Adjustments

Reliant Function	**When does the RTO shift** (i.e. time of month, quarter, year)	**Modified RTO**

2.1.2 DISASTER DECLARATION CRITERIA

Declaring a disaster will be based on the length of time the impact(s) of the event is/are expected to persist when compared to system RTOs. It is critical to remember the initial indications of a disaster may not be readily apparent. For instance, a single user reporting system anomalies to the help desk may not appear to be a significant issue.

However, multiple users of a system reporting such anomalies may be an indication of a systemic issue that escalates to a disaster. It is incumbent upon business owners and ISSOs to ensure supporting infrastructure help desk personnel receive necessary training to support system continuity requirements.

The clock for reestablishing functions and IT systems within their RTOs and MTDs begins at the time of the event, not from the completion of the damage assessment or the formal disaster declaration. Therefore, the RTO must account for (i.e., include) the time necessary to conduct the damage or outage assessment.

2.1.3 DISASTER TYPES

The purpose for identifying types of disasters is only to quickly identify the scope of the disaster. It is not for providing the disaster declaration criteria nor is it an attempt to identify the specific event that caused disaster. Three types of disaster may occur: Type A, Type B or Type C. Each of these three types is defined below.

2.1.3.1 TYPE A DISASTER

This level of disaster is one that affects a single application affecting a single line of business. Neither the supporting infrastructure nor the hosting system would be physically damaged or

rendered inoperable. The problem is correctable with minimal resources and the recovery teams specified in the CP, while placed on alert, may not be activated. The declaration authority for a Type A disaster is the business owner.

2.1.3.2 TYPE B DISASTER

This type of disaster involves a portion of the enterprise whose impact encompasses multiple applications, systems or multiple lines of business. A Type B disaster will either affect; an entire system with impact to all hosted applications, or a major centrally accessed database, the loss of which affects a significant portion of CMS' mission. The declaration authority for a Type B disaster may be the affected business owners (to include the supporting infrastructure business owner).

2.1.3.3 TYPE C DISASTER

This type of disaster will render most of the supporting infrastructure inoperable. A Type C Disaster will require the transition of all supporting infrastructure functions and services to the alternate processing facility and the implementation of CPs in priority order as directed by the supporting infrastructure Business Owner.

Table 9 summarizes the disaster types.

Table 9 Disaster Types

Disaster Type	Description
Type A	Affects a single application affecting a single line of business.
Type B	Involves a portion of the enterprise whose impact encompasses multiple applications, systems or multiple lines of business.
Type C	Renders most of the supporting infrastructure equipment inoperable.

2.1.4 RECOVERY STRATEGY ANALYSIS

The business owner will require identification and implementation of viable and effective strategies commensurate with meeting business process MTD as part of a new system project. For existing systems, the business owner needs to make sure a viable strategy is in place and effective.

When considering recovery requirements a shorter MTD requires a shorter RTO, thus reducing the applicable strategies that are available and increasing the cost of those strategies.

The following four impacts (either individually or in combination) constitute the only consequences of any disaster and therefore must be addressed in any recovery strategy analysis:

- Loss of personnel;
- Loss of computing (to include hardware or software and/or data);
- Loss of telecommunications; and

- Denial of facility access.

Because the four impacts can occur in combination, all should be considered when selecting recovery strategies.

Business owners must conduct their own research in order to implement the most effective strategies that meet their individual requirements. Although it may seem expedient to implement the strategies associated with the shortest RTO, bear in mind that this "default" approach would probably not be the most cost-effective. In addition, business owners implementing new systems at existing IT infrastructure may have lower costs for the strategy than they would have if system deployment were at a new IT infrastructure facility, stemming from sharable components and resources. **Partial lists of potential strategies** for Loss of computing are included in Table 10 through Table 13.

Table 10 Facility (Work Area) Recovery Strategy Matrix

Recovery Tier/RTO	Strategies
Tier 1: 0 - 1 hour	Fixed hotsite (processing, work area and data storage). Telework (work area only).
Tier 2: 1 - 12 hours	Mutual support agreement (processing, work area, and data storage).
Tier 5: >3 days	Warm site, cold site. Mobile trailer-transported hotsite (processing). Defer recovery until reconstitution completion.

Table 11 Hardware Recovery Strategy Matrix

Recovery Tier/RTO	Strategies
Tier 1: 0 - 1 hour	Cloud computing (for IT systems migrated to the cloud). Redundant, mirrored system. Redundant system in standby mode.
Tier 3: 13 - 24 hours	Mutual support agreement.
Tier 4: 1 - 3 Days	Fixed hotsite. Internal swap-out scheme. Quick-ship contract.
Tier 5: >3 days	Mobile trailer-transported hotsite. Defer recovery until reconstitution completion.

Table 12 Software Recovery Strategy Matrix

Recovery Tier/RTO	Strategies
Tier 1: 0 - 1 hour	Redundant, mirrored system.
Tier 2: 7 - 12 hours	Redundant system in standby mode. Disk mirroring. Recover from system backups.

Table 13 Data Recovery Strategy Matrix

Recovery Tier/RTO	Strategies
Tier 1: 0 - 1 hour	Redundant, mirrored system. Redundant system in standby mode.
Tier 2: 1 - 12 hours	Data mirroring.
Tier 5: >3 Days	Data vaulting. Tape backups.

Telecommunications recovery is completely reliant on the Service Level Agreements (SLAs) identified in the service contract(s) with the telecommunications provider(s). Business owners must coordinate with supporting infrastructure providers to ensure telecommunications SLAs meet required MTD and RTO requirements.

Loss of Personnel can only be mitigated through either robust cross-training, accurate-and-thorough desk guides, or relocating personnel from other field offices with identical skill sets and similar experience of the personnel who must be replaced.

Denial of Facility Access may be alleviated through teleworking or the use of pre-designated alternate operating facilities.

Recovery of essential records is accomplished through diligent analysis and by providing backups at all alternate processing and operating locations. Network access to essential records is not sufficient for an event that includes a telecommunications outage, or other impact that precludes network access. Alternate means for effective access to essential records must be included in all CPs.

2.1.4.1 DISASTER MITIGATION STRATEGIES

In some cases, outage impacts identified in the risk assessments may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to disaster declaration and CP implementation.

Identification and implementation of mitigating controls will be conducted during recovery strategy identification and determination activities. Some common measures are:

- Appropriately-sized Uninterruptible Power Supplies (UPS);
- Alternate commercial power feeds;
- Clustered servers and/or Storage Area Network (SAN) as hardware fault tolerance mechanisms;
- Backup generators;
- Fire suppression systems;
- Smoke and water detectors/sensors;
- Heat-resistant and waterproof containers for backups and vital records;

- Offsite backups that are conducted frequently enough and rotated offsite on a timely basis to support RPOs and MTDs; and
- Cross training personnel to mitigate any personnel Single Points of Failure (SPOFs).

2.1.4.2 RECOVERY TO A TRUSTED STATE

When developing recovery procedures, each Business Owner and ISSO will ensure the system can be recovered to the last trusted state.

The trusted state means all controls, control enhancements and compensatory controls are restored to operation and verified as part of the recovery process contained in the CP. Validation of the system, its data, and all controls occur prior to access being granted to the user community.

2.2 CONTINGENCY PLAN DEVELOPMENT

This standard provides the information for developing the five main components of CMS CPs. Each plan should provide all pertinent recovery-related information. **Contingency Planners should refrain from citing other documents and artifacts when developing CPs**. ISSOs and CPCs who rely on referencing other publications will hinder recovery operations by forcing IT technical staff to sift through multiple documents and publications when the availability of streamlined, easy to use procedures is critical to recovery operations. Additionally, not all systems have identical documentation which could result in referencing non-existent documents through the over use of pre-existing "boilerplates". A CP can only be completed after the MTD, RTO, RPO, WRT, and recovery strategies have been established and approved.

2.2.1 PLANNING COORDINATION

Continuity and contingency planning are critical components of emergency management and organizational resilience but are often confused in their use. Continuity planning normally applies to the mission/business itself and is focused on recovering functions and processes during and after an emergency event.

Contingency planning applies to single information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency. Because there is an inherent relationship between an information system and the mission/business process it supports, there must be coordination between each plan during development and throughout each plan's shelf life to ensure that recovery strategies and supporting resources neither negate nor duplicate efforts.

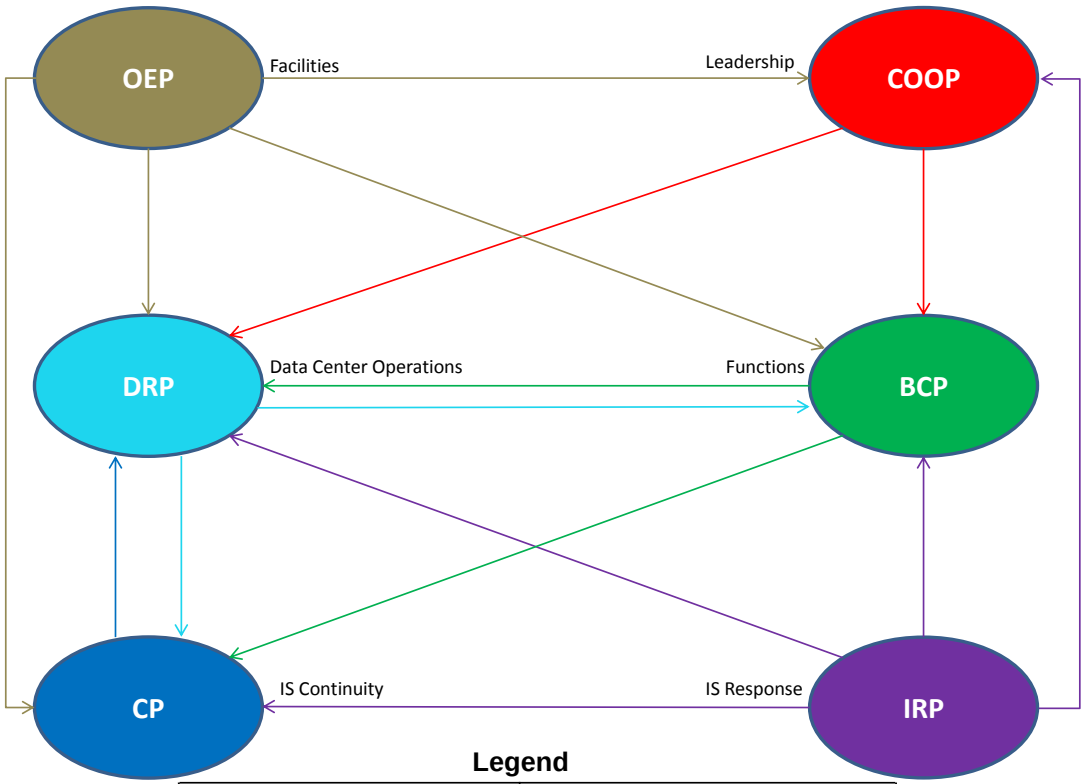
The following figure provides a graphic depiction of the relationships between the different types of response plans. By following the color-coded lines, the sequence of "if/then" for plan implementation is provided. For example, if the Disaster Recovery Plan (DRP) is activated it may require implementation of the Business Continuity Plan (BCP) the Continuity of Operations (COOP) Plan or both.

Each business owner will ensure recovery planning is coordinated across all necessary resources to promote and maintain a CMS-wide integrated recovery capability. Inter-plan integration is critical as any plan implementation may cause the activation of another plan. The most common response plan relationships are:

- Occupant Emergency Plan (OEP) activation could cause the activation of: COOP, BCP DRP, or one or more CPs;
- A DRP could cause an activation of: COOP, BCP or one or more CPs;
- A single CP could cause the activation of the DRP;
- Multiple CPs may cause the activation of the DRP;
- COOP could cause the activation of: DRP or BCP;
- BCP could cause the activation of the DRP or one or more CPs; and
- Incident Response Plan (IRP) activation could cause the activation of: COOP, BCP, DRP or one or more CPs.

Figure 1 presents a graphical representation of these response plan relationships.

Figure 1 Response Plan Relationships



2.2.2 PLANNING ASSUMPTIONS

All CPs will annotate the assumptions under which the plan and included procedures have been developed. When testing plans, business owners will ensure those assumptions are still valid. The following is a partial list for consideration by Business Owners, System Developers/ Maintainers and ISSOs:

- Recovery leadership will be available, either through the normal chain of command, or authorized succession;
- All personnel assigned to recovery teams have received initial training in their responsibilities upon designation in the recovery organization and receive continuing (annual) refresher training;
- All personnel assigned to recovery organization teams will be available for training, exercises and response to actual events/disasters unless on travel, injured or ill;
- Trained and qualified substitutes for essential personnel are not available and Subject Matter Expert (SME) losses will significantly impact recovery operations;
- All personnel assigned to recovery organization teams will be able to travel and successfully reach their assigned alternate processing and operating locations;
- All recovery procedures are up-to-date and current;
- Exercises are conducted on a regular basis and the CP is updated with all "lessons learned" from exercises and actual implementation;
- Accurate and current documentation for all systems and interconnections is available;
- CMS supporting infrastructure will be available either directly from the primary or alternate processing facility;
- Data backups will be available at alternate facilities and compatible with both primary and backup systems;
- Adequate telecommunications connectivity to users and customers will be available subsequent to a disaster, regardless of recovery facilities used;
- Adequate recovery resources (i.e. minimum essential resources, not necessarily resources to restore full capability) will be available to all recovery teams;
- CP requirements are adequately resourced;
- All partners, vendors, and contractors will meet all contracted service and product delivery SLAs.

2.2.3 PLAN FORMAT

Each CP will be formatted to accommodate three phases of contingency planning: *Alert and Notification*, *Recovery*, and *Reconstitution*. CPs will use checklists wherever possible to maximize clarity, enhance efficiency, and minimize extraneous verbiage when identifying specific procedural steps. All checklists will be in chronological order.

Each CP will have five (5) sections and seven (7) appendices.

- Section 1 Introduction;

- Section 2 Concept of Operations (CONOPS);
- Section 3 Alert and Notification Phase;
- Section 4 Recovery Phase;
- Section 5 Reconstitution Phase; and
- Appendix A: Personnel Contact Information
- Appendix B: Vendor Contact Information
- Appendix C: Damage Assessment, Recover and Reconstitution Procedures
- Appendix D: System Description, Diagrams, Hardware and Software Inventories and Vital Records
- Appendix E: Interconnections Table and Points of Contact
- Appendix F: Exercises and Plan Maintenance
- Appendix G: Business Impact Analysis (BIA) Results

The CP format provided in SP 800-34 recommends 12 specific appendices that provide either procedures or amplifying recovery-related information. Through consolidation and structuring, the CMS CP simplifies the format by requiring only seven (7) appendices. For traceability and audit purposes, Table 14 presents the crosswalk between SP 800-34 appendices and CP appendices.

Table 14 Traceability Matrix for CP Appendices: SP 800-34 and CMS

SP 800-34 Appendix	CMS CP Appendix
Appendix A - Personnel Contact Information	Appendix A - Personnel Contact Information
Appendix B - Vendor Contact Information	Appendix B - Vendor Contact Information
Appendix C - Detailed Recovery Procedures	Appendix C - Damage Assessment, Recovery and Reconstitution Procedures
Appendix D - Alternate Processing Procedures	Appendix C - Damage Assessment, Recovery and Reconstitution Procedures
Appendix E - System Validation Test Plan	Appendix C - Damage Assessment, Recovery and Reconstitution Procedures
Appendix F - Alternate Storage Site and Telecommunications	Appendix C - Damage Assessment, Recovery and Reconstitution Procedures
Appendix G - Diagrams	Appendix D - System description and diagrams, Hardware and Software Inventories
Appendix H - Hardware and Software Inventory	Appendix D - System description and diagrams, Hardware and Software Inventories
Appendix I - Interconnections Table	Appendix E - Interconnections Table and Points of Contact
Appendix J - Test and Maintenance Schedule	Appendix F - Exercises and Plan Maintenance
Appendix K - Associated Plans and Procedures	Appendix E - Interconnections Table and Points of Contact
Appendix L - Business Impact Analysis	Appendix G - Critical Recovery Metrics (Business Impact Analysis Results)

2.2.3.1 ALERT AND NOTIFICATION PHASE

This phase of the recovery process defines the initial actions to take in order to assure effective communication, provide for adequate staffing, and to conduct a damage assessment for the purposes of determining response scope. The Alert and Notification Phase of each CP shall include clear instructions for alerting recovery personnel, conducting a damage assessment, and implementing recovery procedures (if required).

Initial alert stage procedures include, but are not limited to:

- A clear list of personnel who will be contacted in the event a system is operating in an anomalous fashion, as well as the timeframe in which the notification will be made. These personnel will be called to determine the nature of the anomaly and to determine if any additional personnel must be notified. This initial cadre should include the applicable help desk, system administrator, or ISSO.
- Escalation procedures within the System Operation Procedures (SOPs) so that, if an event cannot be resolved within a reasonable amount of time, the CPC and/or the ISSO can be notified. Escalation will continue until either the problem is resolved or the disaster declaration authority is appraised of the situation.
- A methodology to ensure that, at each point in the escalation process, the time at which the event will be escalated to the next level is clearly identified. The total time of all damage/ outage assessment activities will be structured so that a disaster may be declared and the appropriate recovery strategies implemented before the system's RTO is exceeded.
- A format for providing a briefing to all members of all recovery teams which contains the following elements:
  - Type of event;
  - Location and time of occurrence;
  - Cause of the occurrence (if known);
  - Damage assessment status;
  - Building access status; and
  - Location and contact telephone number(s) of the management team.
- Elements to be included in the damage assessment stage are:
  - Potential for additional disruptions or damage;
  - Status of physical infrastructure
  - Status of essential records, as identified through the BIA process;
  - Status of hardware and items to be replaced;
  - Status of software and software to be replaced;
  - Status of data;
  - Status of telecommunications; (which may require coordination with the supporting infrastructure to obtain the information);
  - An Estimated Time to Repair (ETR); and

- A recommendation for implementing the CP/declaring a disaster based on the ETR when compared to the RTO of the system(s) involved.

The *Alert and Notification Phase* is complete when the outage assessment has been completed, when the decision to declare or not to declare a disaster is made, and when the recovery team personnel have been mobilized. Since many systems will not be recovered for several days, a week or longer, the progression from the *Alert and Notification Phase* to the *Recovery Phase* for those systems will be delayed.

2.2.3.2 RECOVERY PHASE

When recovering a complex system involving multiple independent components, recovery procedures should reflect system priorities based on the RTOs that were determined and approved. Recovery procedures should be clearly presented in a step-by-step logical sequence in a checklist format so systems and sub-systems may be recovered in a logical manner. When recovering an application, procedures must address the following as applicable;

- The approved recovery strategies for:
  - Hardware recovery;
  - Software recovery;
  - Data recovery;
  - Personnel replacement for critical skill sets; and
  - Alternate operating and processing facilities if warranted based on functional MTD and the system's RTO and RPO.
- Hardware configuration;
- Operating system recovery to include installation and configuration;
- Operating system verification;
- Application software installation and configuration;
- Data recovery and validation;
- Verification of interdependencies with other systems for either upstream data requirements necessary for input to the system or downstream customer requirements;
- Verification of telecommunications connectivity to the primary users of the system from the telecommunications service Point of Contact (POC);
- Inter and intra team communication requirements;
- Customer reporting; and
- Status reporting procedures.

If recovery strategies include personnel relocation; then, in addition to the technical recovery procedures, other instructions may be necessary. If personnel relocation is part of the approved recovery strategy, then recovery procedures must include guidance on;

- What should be included in each employee's deployment suitcase or “fly-away kit”;
- Who will coordinate all issues regarding travel;

- Travel expense policies and procedures;
- Available emergency medical and dental care at the alternate facility;
- Contact information for relocating personnel; and
- Lodging accommodations and dining facilities.

2.2.3.3 RECONSTITUTION PHASE

According to SP 800-34 Revision 1, the Reconstitution Phase consists of:

- Validating data at the alternate facility. Data validation consists of comparing the pre-disaster data with the recovered data to ensure the available data in the recovered system is accurate, complete and effectively supports the reliant functions.
- Validating system functionality at the alternate facility. System validation ensures that the system can effectively and accurately process the data in the same manner as before the disaster.
- Validating full operational capabilities of the functions that rely on the system that declared the disaster. This final step is verification by the business owner that the business function(s) that rely on the recovered system are fully recovered, that all backlogs have been cleared, and normal operations have been resumed.

Once the above activities have been completed, contingency operations are considered completed. Notification that the plan has been completed must be sent to all affected parties.

2.2.3.4 NORMALIZATION

The impact(s) of the disaster that caused the CP implementation may not be fully mitigated and migration back to the primary facility may be delayed, which brings us to normalization. There is no need to develop a second CP for the return to a primary facility[9] because the return will be addressed as a business unit project. However, the key decision point is the sequence and the CP should be used as the framework for the step-by-step process that is used to implement the return to the primary facility. The fail over to an alternate facility is conducted based on RTO determinations. The decision for the failback sequence does not have to be made beforehand as long as the criteria for choosing each of the sequences are documented and available within the plan.

When returning to the primary facility the declaration authority must decide to either:

- Failback in the same sequence which allows the longest time for all functions at the alternate processing facility before the second disruption; or

[9] The term "primary facility" is used to denote the permanent processing facility after normalization. The primary facility may be the restored original facility, a facility procured after the disaster, or the organization may designate the facility where current processing is hosted (e.g. what had been the alternate facility before the disaster.)

- Failback in reverse order, causing major disruption to the lesser critical processing but allowing additional opportunity for the most critical functions to continue processing before the second disruption; or
- Failback in an order that provides the most benefit to the organization.

2.2.3.5 APPENDICES

Appendix A Personnel Contact List

Contact information should be included for each person with a recovery role or recovery-related responsibility for plan activation, implementation, or coordination.

Appendix B Vendor Contact list

Contact information for all key maintenance or support vendors should be included in this appendix as well as emergency phone numbers, contact names, contract numbers, and contractual response and response time SLAs.

Appendix C Damage Assessment, Recovery, and Reconstitution Procedures

This appendix includes the operational assessment and detailed recovery procedures for the system, which will include, at a minimum the following:

- Assessment forms for hardware, software and connectivity issues;
- Keystroke-level recovery procedures;
- System installation instructions from the applicable storage media (i.e. tape, CD);
- Required configuration settings or changes;
- Recovery of data from applicable media and audit logs;
- Security controls configurations;
- System and Data Validation Procedures;
- Other system recovery procedures, as appropriate; and
- Stand-down procedures for return to normal operations.

If the system relies on another group or system for its recovery and reconstitution (such as a mainframe system), then information provided should include contact information and locations of detailed recovery procedures for that supporting system as well as connectivity configurations.

Appendix D System Diagram, Hardware and Software Inventories and Vital Records

The purpose of this appendix is to document not only system architecture, but also input/output, and other technical or logical diagrams that may be critical to system recovery. It is incumbent on business owners to ensure input and output interconnectivity with other systems is

documented clearly and thoroughly. The information in this appendix should map directly to the interconnections table in Appendix H.

This appendix provides a complete list of the system hardware and software. Inventory information will include server types and quantities, processors, memory requirements, storage requirements, and any other pertinent configuration details. The software inventory will include the operating system (including service pack or version levels), other applications necessary to operate the system such as database software and finally, commercial software registration keys (itemized for each copy).

Appendix E Interconnections Table

This appendix includes information on other systems that directly interconnect or exchange information with the system. Interconnection information should include the type of connection, information transferred, contact information for the primary and secondary points of contact for that system, and other pertinent information from the Interconnection Security Agreement (ISA).

Appendix F Exercise and Maintenance Schedule

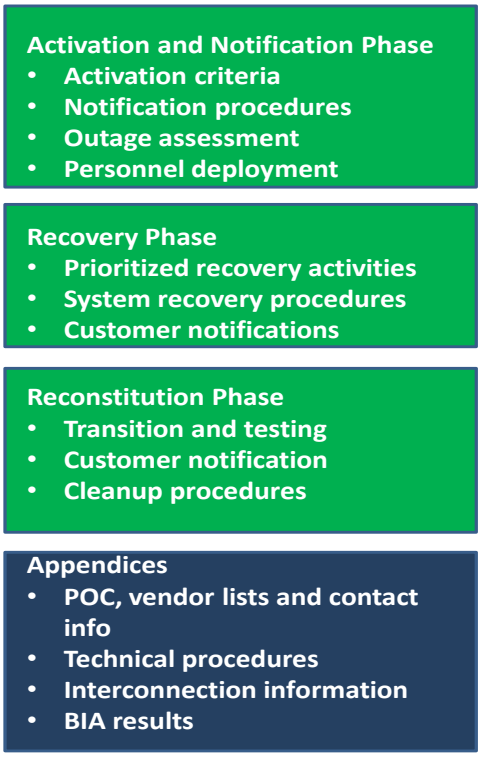
All CPs will be reviewed and exercised annually. Appendix F information will include the dates of all exercises and the points of contact for each exercise conducted for the current year and the two previous years.

Appendix G Critical Recovery Metrics

Include the critical recovery metrics from the current risk assessments, the most current business risk assessments, information system risk assessments, and any applicable BIA in this appendix. Additional required information will include:

- The MTDs of the functions supported by this system;
- RTO validation;
- Component or sub-system prioritization within the system RTO;
- RPO validation;
- The expected WRT; and
- Single Points of Failure and mitigation activities taken or planned. Planned actions for SPOF mitigation should also appear as Plans of Actions and Milestones (POA&Ms) in the CMS Federal Information Security Management Act (FISMA) Control Tracking System (CFACTS).

Figure 2 CP Format



2.3 EXERCISING AND TRAINING

An organization can only maintain a viable recovery capability if all personnel are knowledgeable in their responsibilities and duties, are trained to implement approved recovery strategies, and if those strategies and capabilities are tested to ensure functionality. Therefore, every Business Owner and ISSO will implement a robust CP training and exercise program.

2.3.1 EXERCISING

- Each system CP should be exercised to identify and rectify deficiencies and planning shortfalls, NOT to ascertain the technical competence of personnel with recovery responsibilities. The Business Owner, System Developer/Maintainer, CPC and ISSO shall establish criteria for validating/exercising CPs on an annual schedule, once every 365 days. This process will also serve as training for personnel who will be called upon to execute the CP. Exercises should include the following areas[10]:
  - Notification and escalation procedures;
  - System recovery on an alternate platform from backup media;
  - Internal and external connectivity;

[10] SP 800-34 Revision 1

- Actual operational functional support from the recovered system; and
- System restoration and smooth resumption of normal operations.

Exercise results will be used to for plan updates addressing any identified shortcomings. The types of exercises include tabletop and functional exercising. CPs for all systems must be exercised in accordance with CMS Minimum Security Requirements (CMSR) for contingency planning. **Note: Actively exercising the system CP as part of a larger, coordinated technical exercise of the hosting system satisfies the annual requirement.**

Each exercise will be coordinated through a pre-developed exercise plan approved by the business owner prior to the event. All exercise plans will include:

- Exercise facilitator for central exercise management;
- Observers/Monitors for objective exercise evaluation;
- Exercise participants;
- Exercise objectives;
- Exercise metrics to determine how well objectives were met;
- Required materials;
- Exercise timeline;
- Any assumptions; and
- Exercise scenario to include scripts and injects.

2.3.1.1 TABLETOP EXERCISES

Tabletop exercises are designed to facilitate a conversation by the participants where procedures and their roles and responsibilities are discussed within the framework of the exercise scenario and objectives. The primary objective of the tabletop exercise is to validate the information in the plan and ensure designated personnel understand the information available in the CP. Tabletop exercise objectives will include, at a minimum:

- Validation of RTOs and functional MTDs;
- Validation of response and recovery procedures;
- Guidelines and procedures for coordinated, timely, and effective response and recovery;
- Call tree information verification;
- Verification of recovery procedures; and
- Discovery of any weaknesses in the CP.

2.3.1.2 FUNCTIONAL EXERCISES

Functional exercises include actual system fail-over through the implementation of approved recovery strategies. The primary objective of the functional exercise is ensure the effective operational fail-over/recovery of the application to include:

- Ability to continue functional processing in backup mode;

- Application/system interdependencies and data flow verification;
- Compatibility of data backups with the primary and backup systems;
- Data storage and recovery processes; and
- The ability to extend the system to users at alternate processing and telework sites.

2.3.2 TRAINING

Contingency Plan Coordinators will develop a training program for all personnel assigned to recovery responsibilities. Training will be provided within 120 days of assignment to recovery responsibilities with refresher training conducted at least annually thereafter. All training will be coordinated and centrally documented with the ISSO. Training will include, but will not be limited to the following:

- Emergency Response;
- Disaster declaration criteria and declaration authorities;
- Functional recovery prioritizations and RTOs of interdependent IT systems;
- Validation of the approved recovery strategies and strategy implementation;
- Verification of CP implementation procedures; and
- Validation of recovery personnel assignments, roles and responsibilities.

3 ROLES AND RESPONSIBILITIES

This section identifies the key personnel who are responsible for supporting and/or implementing CPs as well as standard recovery organizations. Designation of key planning personnel may need to be modified at the time of the event for enhanced situation response. Additionally, any personnel assigned directly or indirectly to any of the below positions, groups or teams are considered essential for purposes of dismissal and recall.

3.1 PERSONNEL ROLES AND RESPONSIBILITIES

3.1.1 CHIEF INFORMATION SECURITY OFFICER (CISO)

The CMS CISO will:

- Ensure business owners plan for and designate adequate IT systems, facilities and personnel to support alternate operating locations and telework capabilities;
- Establish CP standards, policies and procedures for CMS and provide methods that enable business owners to develop, implement and maintain contingency plans for systems and infrastructure within those frameworks ;
- Verify compliance within CMS standards during the FISMA Assessment and Authorization (A&A) process;

- Ensure business owners develop, implement and maintain strategies, plans, and procedures for mitigation, emergency response, system recovery and connectivity capabilities, and system restoration of failed IT systems to full operational capability;

3.1.2 BUSINESS OWNERS

All business owners are responsible for the following:

- Develop, distribute and maintain CPs for all applications and systems for which they are responsible;
- Review all CPs at least once every 365 days or whenever there is a significant change to the system or operating environment;
- Ensure each plan under their purview is tested at least annually;
- Ensure a technical test for each system is conducted at least every other year;
- Review and correct plan deficiencies in a timely manner;
- Investigate and implement the most cost effective, efficient and available recovery strategies;
- Ensure the annual plan review includes an analysis of the identified recovery strategies to ensure recovery strategies take full advantage of all possible cost savings and efficiencies;
- Obtain appropriate resourcing to include funding and staffing, for recovery planning requirements;
- Ensure all personnel with recovery responsibilities are trained to consider recovery preparedness part of their normal duties;
- Determine and manage information system and data backup storage and alternate processing facility agreements;
- Ensure each contingency plan is distributed to all personnel who are assigned recovery responsibilities and maintained in current status;
- Ensure a copy of the most current CP is maintained at the alternate processing location;
- Ensure stringent change control is maintained over the application/system and the CP;
- Should an event occur, contact recovery team members or escalate to senior management depending upon the severity of the event in accordance with section 1.3.2 of this document; and
- Delegate recovery responsibility as necessary during an actual event to ensure expeditious and accurate information system recovery.

3.1.3 CONTINGENCY PLAN COORDINATORS

The CPC will:

- Assist the business owner in conducting all phases of contingency planning;
- Assist the business owners in recovery strategies development and implementation;
- Manage CP development and execution;
- Oversee the system CP process;

- Ensure CPs meet all federal government requirements;
- Provide application sanitization requirements for primary and alternate processing facilities;
- Oversee and coordinate all CP exercises;
- Oversee and coordinate the recovery-related training and awareness program for all personnel;
- Coordinate recovery team staffing with the business owners, CISO's office and Emergency Preparedness and Response Operations (EPRO) Office; and
- Assist ISSOs in event response until it is determined that contingency execution is not warranted.

3.1.4 SYSTEM DEVELOPERS/MAINTAINERS

All system developers/maintainers will:

- Conduct a preliminary failure assessment when directed;
- Determine the level or type of event and make recommendations regarding appropriate recovery responses to the business owner;
- Assist in all response and recovery activities as required by contract or as directed by the business owner; and
- Assist with any hardware/software incompatibilities and data validation issues that may arise before, during and after an event or exercise.

3.1.5 INFRASTRUCTURE SUPPORT/DATA CENTER

Data centers are responsible for:

- Restoration of systems and applications that are covered by contract at the primary or alternate supporting infrastructure dependent upon the nature and scope of the disaster;
- Recovering original application processing functions at the primary or alternate processing facility; and
- Ensuring sanitization of primary and alternate processing facilities.

3.2 RECOVERY TEAM ROLES AND RESPONSIBILITIES

The recovery organization for a single system or application will be limited to a small management team and system recovery team. However, should an infrastructure-wide disaster occur that requires implementation of the DRP, the enterprise-level recovery organization and its staffing requirements take precedence. Business owners must prepare for the possibility of losing recovery personnel to the enterprise-level recovery teams. Business owners must also ensure effective inter-team communications regardless of the nature of the outage.

3.2.1 CP MANAGEMENT TEAM

The CP Management Team is comprised of the business owner, the ISSO, CPC, and other personnel deemed necessary by the business owner. The CP Management Team is responsible for:

- Ensuring a thorough and rapid failure assessment is conducted to accurately declare a disaster and fast enough to ensure recovery within the established Recovery Time Objectives (RTOs);
- Declaring a disaster when a specific event warrants such action;
- Adjusting the RTO as necessary to accommodate cyclical operational peaks and ebbs;
- Ensuring effective implementation of the CP when necessary;
- Coordinating with the CMS Disaster Recovery Management Team throughout the recovery process;
- Tracking the status of all recovery efforts within the scope of the CP;
- Coordinating all travel and lodging requirements for relocating recovery team personnel;
- Coordinating and obtaining approval for all recovery-related procurement actions; and
- Coordinating and authorizing the migration back to the primary facility.

3.2.2 CP RECOVERY TEAM

The CP Recovery Team is comprised of the system developers/maintainers, a representative of the business process managers, and other personnel deemed necessary by the business owner. The CP Recovery Team is responsible for:

- Conducting the failure assessment and recommending disaster declaration status to the business owner;
- Implementing mitigation actions for impact reduction;
- Coordinating repair and salvation action;
- Recovering application/system functionality at the alternate processing facility in RTO order unless modified by the CP Management Team or higher authority;
- Coordinating with the alternate facility and the CP Management Team to resolve any telecommunications connectivity issues to include extending the system to the users;
- Ensuring all required system cyber security controls are in place throughout the recovery and reconstitution phases;
- Shutting down operations at the alternate facility when directed and replenishing any expended supplies;
- Ensuring the most current data is shared with the primary facility so the restored system is up to date; and

- Ensuring all systems are transitioned to backup mode[11] when directed to do so by the CP Management Team.

4 APPROVED

Teresa Fryer

Digitally signed by Teresa Fryer
DN: cn=Teresa Fryer, o, ou, email=teresa.fryer@cms.hhs.gov, c=US
Date: 2014.03.04 09:20:39 -05'00'

Teresa Fryer
Director, Enterprise Information Security Group (EISG)
Chief Information Security Officer (CISO)

This document will be reviewed periodically, but no less than annually, by the CISO, and updated as necessary to reflect changes in policy or process. If you have any questions regarding the accuracy, completeness, or content of these procedures, please contact EISG at ciso@cms.hhs.gov.

[11] Backup mode is defined as the state at which the primary system has been configured to assume operational processing, and the backup system is in its normal subordinate state.