ITRM Guideline SEC508-00
Effective Date: 04/18/2007

COMMONWEALTH OF VIRGINIA

Information Technology Resource Management

INFORMATION TECHNOLOGY CONTINGENCY PLANNING GUIDELINE

Virginia Information Technologies Agency (VITA)

ITRM Publication Version Control

ITRM Publication Version Control: It is the user's responsibility to ensure that he or she has the latest version of the ITRM publication. Questions should be directed to the Associate Director for Policy, Practice and Architecture (PPA) at VITA's IT Investment and Enterprise Solutions (ITIES) Directorate. ITIES will issue a Change Notice Alert when the publication is revised. The Alert will be posted on the VITA Web site. An email announcement of the Alert will be sent to the Agency Information Technology Resources (AITRs) at all state agencies and institutions, as well as other parties PPA considers interested in the publication's revision.

This chart contains a history of this ITRM publication's revisions:

Version	Date	Purpose of Revision
Original	04/18/2007	Base Document

Publication Designation

ITRM Guideline SEC508-00

Subject
Information Technology Data Protection

Effective Date
April 18, 2007

Scheduled Review
One (1) year from effective date

Authority
Code of Virginia § 2.2-603(F)
(Authority of Agency Directors)

Code of Virginia, §§ 2.2-2005 – 2.2-2032.
(Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO))

Scope
This *Guideline* is offered as guidance to all Executive Branch State agencies and institutions of higher education (collectively referred to as "agency") that manage, develop, purchase and use information technology (IT) resources in the Commonwealth.

Purpose
To guide agencies in the implementation of the information technology contingency planning requirements defined by ITRM Standard SEC501-01.

General Responsibilities
(Italics indicate quote from the Code of Virginia)

Chief Information Officer
In accordance with *Code of Virginia* § 2.2-2009, the CIO is assigned the following duties: "*the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures, and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits.*"

Chief Information Security Officer
The CIO has designated the Chief Information Security Officer (CISO) to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity and availability of the Commonwealth of Virginia's IT systems and data.

IT Investment and Enterprise Solutions Directorate
In accordance with the *Code of Virginia* § 2.2-2010, the CIO has assigned the IT Investment and Enterprise Solutions Directorate the following duties: *Develop and adopt policies, standards, and guidelines for managing information technology by state agencies and institutions*."

All State Agencies
In accordance with § 2.2-603, § 2.2-2005, and §2.2-2009 of the *Code of Virginia*,, all Executive Branch State agencies are responsible for complying with all Commonwealth ITRM policies and standards, and considering Commonwealth ITRM guidelines issued by the CIO of the Commonwealth.

Definitions
Agency All Executive Branch State Agencies and institutions of higher education that manage, develop, purchase and use IT resources in the Commonwealth of Virginia (COV).

Agency Control - If an agency is the Data Owner of the data contained in a Government database, that agency controls the Government database.

BIA - Business impact analysis – The process of determining the potential consequences of a disruption or degradation of business functions.

Contingency – An unanticipated event that causes a disruption of normal business.

COOP – Continuity of Operations Plan – A set of documented procedures developed to provide for the continuance of essential business functions during an emergency.

Crisis – See Contingency.

.**Data** - Data consists of a series of facts or statements that may have been collected, stored, processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information. Information can be processed and used to draw generalized conclusions or knowledge

Data Communications - Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate COV data between and among computer systems, including the hardware, software, interfaces and protocols required for the reliable movement of this information. As used in this Guideline, Data Communications is included in the definition of government database herein.

Data Owner - An agency manager responsible for the policy and practice decisions regarding data. For business data, the individual may be called a business owner of the data

Emergency – See Contingency.

Information Security Officer (ISO) - The individual who is responsible for the development, implementation, oversight and maintenance of the agency's IT security program.

IT System - An interconnected set of IT resources and data under the same direct management control.

Recovery Point Objective (RPO) – the point in time to which data must be restored in order to successfully resume processing.

Recovery Time Objective (RTO) – The maximum amount of time to recover and restore a business process which an organization can tolerate.

Sensitive Data - Any data of which the compromise with respect to confidentiality, integrity and/or availability could adversely affect COV interests, the conduct of agency programs, or the privacy to which individuals are entitled.

Sensitive IT Systems - COV IT systems that store, process, or transmit sensitive data.

System Owner -An agency Manager responsible for the operation and maintenance of an agency IT system.

Related ITRM Policy and Standards

ITRM Policy, SEC500-02, Information Technology Security Policy (Effective Date: 07/01/2006)
ITRM Standard SEC501-01: Information Technology Security Standard (Effective Date: 07/01/2006)
ITRM Standard SEC502-00: Information Technology Security Audit Standard (Effective Date: 07/01/2006)

TABLE OF CONTENTS

1 Introduction

1.1 Information Technology Security

In order to provide overall Information Technology (IT) security that is cost-effective and risk based, IT Contingency Planning must be a part of an agency's IT security program. This Guideline presents a methodology for IT Contingency Planning suitable for supporting the requirements of the Commonwealth of Virginia (COV) *Information Technology Resource Management (ITRM) Information Technology Security Policy (ITRM Policy SEC500-02)* and the COV *ITRM Information Technology Security Standard (ITRM Standard SEC501-01)*. These documents are hereinafter referred to as the "Policy" and "Standard," respectively.

The function of the Policy is to define the overall COV IT security program, while the Standard defines high-level COV IT security requirements. This Guideline describes processes agencies may use in implementing the contingency planning requirements of the Policy and the Standard.

1.2 IT Contingency Planning

IT Contingency Planning identifies, exercises[1] and reviews the actions necessary to respond to an unplanned event that renders COV IT systems and data that support the essential business functions defined by the agency's Business Impact Analysis (BIA) unavailable, and to restore and recover these IT systems and data. This Guideline describes recommended processes for agencies to use in satisfying the following requirement of the Standard:

- Development of the IT components of the Continuity of Operations Plan (COOP)
- Development and exercise of the IT Disaster Recovery Plan (IT DRP) within the COOP
- Development and exercise of the IT System Backup and Restoration Plan

[1] *Exercises are events that allow participants to apply their skills and knowledge to improve operational readiness. Exercises allow planners to evaluate the effectiveness of previously conducted tests and training activities. The primary purpose of an exercise is to identify areas that require additional training, planning, or other resources. (VDEM COOP Planning Manual)*

2 Continuity of Operations Plan (COOP)

COV COOP requirements are defined by the Virginia Department of Emergency Management (VDEM). This Guideline describes processes that agencies may use to fulfill the COOP requirements for IT systems and data. Agencies should consult the *Continuity of Operations Planning Manual* published by VDEM, both for non-IT related COOP requirements, and for additional information on IT-related COOP requirements. VDEM defines a COOP as "a set of documented procedures to resume or restore critical business processes following a disruption." Agencies should include the IT DRP in the COOP (described in Section 3) and align the IT DRP with the COOP, so that recovery time objectives (RTOs), described in Section 2.2.1, are consistently addressed as efficiently as possible.

2.1 COOP Focal Point for IT

Agencies must designate an employee as the agency's focal point for any IT aspects of COOP and related Disaster Recovery planning activities. Recommended qualifications for this individual include:

- At least three years of IT Disaster Recovery planning experience; and
- Certification by either the Disaster Recovery Institute International (drii.org) or the Business Continuity Institute (www.thebci.org).

2.2 COOP Documentation Related to IT

The COOP (including associated IT activities) documents the agency's plan to respond to a crisis that threatens the agency's ability to fulfill aspects of its mission. The COOP describes how the agency will either continue or recover essential business functions (as defined by the agency's BIA.)

Elements of the COOP that are related to IT and must be documented in the COOP include:

- Essential business function RTOs;
- Requirements for the recovery of IT systems and data; and

- Contact information for all personnel who may be required to respond to an IT-related contingency.

These IT-related COOP elements are also essential to the development of the IT DRP.

The COOP is sensitive information, and must be protected as such. Copies should be securely stored at agency work locations as wellas at a secure off-site location.

2.2.1 Essential Business Function RTOs and RPOs

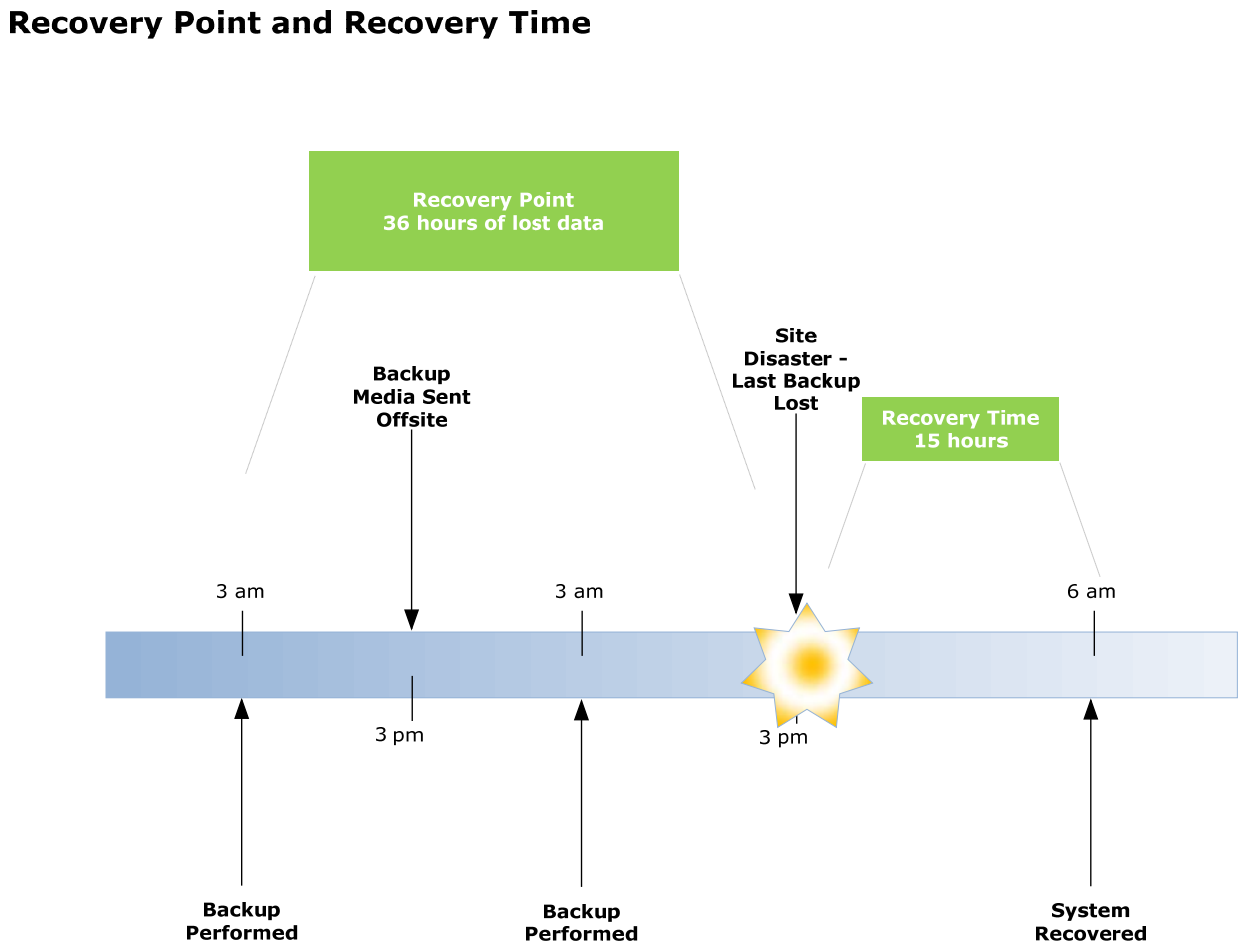
In order to determine the IT requirements to support the COOP, the agency must first determine how quickly essential business functions must be recovered. Use the essential business function RTOs defined during the agency's BIA[2]. The RTO of each essential business function drives the remainder of COOP IT planning.

Where appropriate, the agency should also understand the need for recovery point objectives (RPO) and determine RPOs for business functions. When a business process is interrupted, transactions and other activities may continue to occur, but may not be properly captured. The RPO is the state, prior to the occurrence of the interruption, which the recovery must recreate. Since most organizations tend to create or receive data during their normal operations, the RPO may be thought of as the amount of data that may be lost before the agency's mission is severely impacted. This amount of data is often measured in terms of time (i.e. minutes, hours or days worth of data.)

As an example, organizations that process monetary transactions, such as agencies that collect revenue, or whose transactions may affect human life, such as emergency responders, may have a zero-tolerance for data loss. Their RPO must be zero. Other organizations can tolerate more data loss, because the time to recover the data may not impact the mission as severely. Figure 1 illustrates the relationship between RTOs and RPOs.

[2] COV BIA requirements are defined in the *Continuity of Operations Planning Manual*, published by VDEM.

Figure 1 - Recovery Point and Recovery Time



As illustrated in Figure 1, an agency that processes permits may lose some number of permit applications that have been accepted, but have not been incorporated into the "permit database". If the business process allows one day of permit transactions to accumulate between data backups, and the "permit IT system" is lost during the latest backup, the required RPO would be prior to the last completed backup. Since up to one day of transactions were not backed up, those transactions may need to be recovered in some other way (i.e. manually.) In the example illustrated in Figure 1, the agency would need to recreate the transactions lost between the time

the last set up backup media was sent off site and the time the disaster occurred. In developing IT Contingency Plans, agencies should evaluate whether existing RPOs are sufficient for the agency to recover its business processes.

2.2.2 IT Recovery Requirements

Once the essential business function RTOs (and RPOs, if needed) have been determined by the BIA, the IT related COOP documentation should be developed to describe the IT systems and data required to support those essential business functions. Then, for each required IT resource, the recovery requirements need to be determined. The IT recovery requirements should describe:

- RTOs and RPOs;
- Hardware platforms (e.g. servers, networks, clients);
- Software (e.g. operating systems, database management systems, applications);
- Data;
- Priority of recovery of each essential IT system;
- Personnel required to recover essential IT systems and data;
- Facility and other resource requirements;
- Regulations to which the agency is subject; and
- Requirements for recovery of the agency.

Worksheets useful for developing IT recovery requirements may be found in the VDEM COOP Worksheets document (www.vaemergency.com/library/coop/resources/COOPWorksheets.doc[3]).

[3] This hyperlink is current as of December 2006

2.2.3 Personnel Contact Information

Personnel required to respond to a contingency should be selected and trained in their contingency response roles prior to any contingency. Contact information should be kept current and available to everyone responsible for responding to incidents, emergencies, and contingencies. A worksheet for developing a contact list may be found in the VDEM COOP Worksheets document (www.vaemergency.com/library/coop/resources/COOPWorksheets.doc[4]).

2.2.4 Contingency Notification Procedures

Prior to any contingency, agencies should determine who, when, and how to notify those who will be responsible for responding to the incident, including Senior Management, and other stakeholders the agency deems necessary to notify. During some contingencies, normal communications channels may be disrupted, so alternate communications methods (phone trees, home visits, media notifications) may need to be considered and procedures developed. Once the notification procedures have been developed, they should be made available to all personnel who will be responding to the incident.

The VDEM COOP Worksheets document contains several worksheets that can aid in planning these procedures.

2.3 COOP IT Exercise

Agencies must conduct an exercise of COOP IT components in order to assess their adequacy and effectiveness, at least annually. This exercise should validate the coordination and operation of the COOP IT components with the rest of the COOP. If the agency is exercising its overall COOP, the COOP IT exercise might be best conducted as part of that overall exercise, as defined by the agency's COOP. The requirement may also be met in the context of exercising the agency's IT DRP. Exercise planning, execution, evaluation, documentation, and revision are described in Sections 3.3 and 3.4.

[4] This hyperlink is current as of December 2006.

2.4 COOP Revision

A COOP should not be a static document, but should be reviewed at least annually, and revised as necessary, so that it continues to support the agency's changing business requirements. Revisions of the COOP must reflect both changing business requirements and changes in IT components. Similarly, results of exercise evaluations and lessons-learned may also dictate the need for revision.

3 IT Disaster Recovery Planning

The process of IT disaster recovery planning identifies the steps necessary to respond to an unplanned event that renders IT systems and data which support essential business functions unavailable, and to restore those IT systems and data. These steps lead to the creation of an IT DRP. The IT DRP should be based on:

- Essential Business Function RTOs and RPOs;
- IT Recovery Requirements, derived from these RTOs and RPOs;
- Personnel Contact Information; and
- Contingency Notification Procedures.

These items are contained in the COOP documentation related to IT described in Section 2.2.

3.1 Develop and Maintain an IT DRP

The IT DRP describes the IT activities and resources required to restore essential business functions according to COOP requirements. The DRP describes the activities at the functional level. The actual step-by-step procedures used to execute the required activities should be developed by the IT personnel who administer the associated IT systems. The IT DRP must be approved by the agency head as part of the COOP.

3.2 Components of an IT DRP

This section describes the components of an IT DRP and the function of each component.

3.2.1 Introduction

Purpose

This section of the IT DRP should describe the goal and objectives of the DRP.

The DRP establishes procedures to evaluate an event that affects agency IT systems and data, evaluate whether these IT systems and data require recovery, and provide any recovery required.. Possible objectives include:

- Effective contingency operations and recovery.
- Identification of activities, resources and procedures required to support contingency operations and recovery.
- Clear assignment of responsibilities to operations and recovery personnel.
- Effective coordination with other organizations who may be responding to the contingency.

Applicability

Describe, in this section of the IT DRP, which elements of the agency's functions, operations, and resources the DRP applies. For example, if the agency has a central office, regional headquarters, and field offices, it might make sense to apply particular DRPs to each of them. The applicability section needs to specify which set of resources will be supported by the IT DRP.

Scope

In this section of the IT DRP, describe the planning principles and assumptions used to create the IT DRP. For example, if the agency has a contract with a disaster recovery facility, describe, at a high level, how that facility will be used. Similarly, list the fundamental assumptions used to create the plan. These assumptions should be derived from the planning principles and might include:

- Conditions that might trigger the plan (e.g. facilities, hardware or software unavailability for more than 24 hours.)
- All required personnel are trained and available to execute the recovery.
- Preventive controls (e.g., uninterruptible power supplies, generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers and fire department assistance) are operational at the time of the contingency.
- Valid, current backups of the applications and data are available at an offsite storage facility (location of the facility should also be described.)
- The equipment, connections and capabilities required to operate the agency's IT systems are available at the alternate site.
- Agreements are in place with all required service providers to support the recovery.

Requirements

Detail the IT recovery requirements (described in Section 2.2.2) in this section of the IT DRP.

3.2.2 Operational Plan Components

System Description

In this section of the IT DRP, provide general descriptions of the agency's IT system architectures and functions. Describe the operating environment, physical locations, general locations of users and any interconnections between IT systems (including those that do not belong to the agency.) Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Include diagrams of all layers of each IT system's architecture (logical, physical and operational). This should include security controls and telecommunications connections.

Decision Making Succession

Identify, in this section of the IT DRP, the individuals who are responsible for making decisions about the recovery. For example, the agency head might be the initial decision-making authority.

If the agency head is not available to make recovery decisions, use this section to document the delegation of authority to make recovery decisions. Be as complete as possible, in this section, so that recovery can begin without having to sort out authorizations.

Responsibilities

Use this section of the IT DRP to list the various teams and their responsibility for IT systems and data recovery. For each team, describe their responsibilities, leadership and coordination with other teams during a recovery operation. Include a diagram that shows the teams and their relationships.

Possible teams include:

- Agency Emergency Response Team – Executes overall responsibility for responding to emergencies affecting agency continuity of operations.
- IT Systems Management Team – Responsible for executing the technical procedures of IT systems and data recovery.
- IT Applications Team – Responsible for making emergency modifications to agency IT applications if conditions demand “work-around”.
- Facilities Management Team – Responsible for readiness at the recovery site, and for managing cleanup efforts.
- Public Affairs and Communications Team – Responsible for communicating with agency stakeholders concerning the agency’s response to the contingency.

Depending on the agency, other teams may exist or need to be established.

Communications

After initial impact assessment, the next most important task is establishment of some channel of communications between and among the contingency teams. Terrestrial telephony may be disrupted. Mobile telephony may be overloaded. This section of the IT DRP should include a

communications plan that is robust enough to mobilize contingency teams under most conditions.

One possible method is to plan mobile phones as primary backup to terrestrial phones, and physical contact as the backup to loss or degradation of mobile communications. This would require secure off-site storage of all team member home addresses, and planned routes/maps to access them. Once the teams have assembled, a good alternate communications channel is land-mobile radio. These are hand-held, fairly secure, and can be configured to provide instantaneous team-wide communication.

3.2.3 Plan Activation

Describe the initial actions to detect and assess damage inflicted by a disruption to agency IT systems in this section of the IT DRP. Determine in advance who will have the authority to activate the IT DRP, based on the assessment. It is important, for most agencies to note, in this section, that protection of life and safety is a priority to be met prior to activation of the IT DRP.

Damage and Impact Assessment

This section of the IT DRP contains procedures to assess the damage and impact of the event. If the agency has an Impact Assessment Team, that team should be called by the first responder to the event. This means contact information for the Impact Assessment Team needs to be available both on and off-site. The impact assessment procedures need to be methodical, and should enable the team to provide enough information to the agency official who will make the decision concerning activation.

Activation Criteria

This section of the IT DRP should define unambiguous criteria for activating the IT DRP, based on the report of the Impact Assessment Team (or whomever the agency has designated to assess impact.) Some example criteria (use agency-specific numbers, based on the agency's BIA and sensitive IT system risk assessments) include unavailability of:

- System A, for X hours (e.g. a severe hardware failure has occurred)
- Facility B, for Y hours (e.g. a toxic gas leak has infiltrated the facility)

- Specified personnel, for Z hours (e.g. a pandemic has sickened so many people, employees refuse to respond, out of concern for family care)

Unavailability is not, necessarily, only a result of physical disruption. Unavailability can also be caused by compromised IT system or data confidentiality or integrity. For example, if a sensitive system is broken into and the data is modified, the agency may decide to keep the system unavailable until the data integrity has been restored. Similarly, if the confidentiality of sensitive data has been compromised, the agency may decide to suspend the business process relying on related data until the leak has been secured.

Activation Procedures

This section of the IT DRP describes the procedures to be followed in order to activate the IT DRP and notify all teams. Example procedures that should be detailed here include:

- How all team leaders will be informed (who will inform and by what means.)
- If relocation is required, how this will be accomplished.
- How team leaders will inform their teams, including alert and mobilization instructions.
- How off-site storage and processing services will be notified a contingency has been declared. This would require requesting the storage provider to ship (or transmit) necessary applications and data to the recovery site, and the recovery site provider to prepare the site for activation.
- How general information about the incident will be communicated to stakeholders.

The above list is merely suggestive. Agencies should develop activation procedures that meet their particular requirements.

3.2.4 Procedures for Recovery

This section of the IT DRP details the procedures for recovering the agency's IT systems and data at an alternate site. This recovery should be in accordance with the agency's COOP, based

on requirements delineated in the agency's BIA. This section does not describe procedures to repair the original system to full operational capabilities.

Include in this section recovery procedures required to meet each recovery goal described in the requirements section of the IT DRP. The steps in each procedure should be listed in the sequence providing the most efficient recovery operations.

3.2.5 Procedures for Return to Normal Operations

This section of the IT DRP details the procedures to restore the agency's IT systems and data at the agency's original or new site. These activities begin when the original or new (non-contingency) facility has been made available. Development of the plans for the recovery of the facility is out of the scope of the IT DRP, but the two plans must be coordinated.

The steps in each procedure required for a return to normal operations should be listed in the sequence providing the most efficient recovery operations. IT systems and telecommunications connections should be tested. Once operations have been restored, agencies should consider operating the IT systems at the contingency site and the restoration site in parallel, until it is proven the primary systems are operating properly.

3.2.6 Plan Deactivation

This section describes procedures for removing, from the contingency site, any equipment, or other materials belonging to the agency. Focus particularly on ensuring the proper removal and handling of sensitive data. Materials, equipment and backup media should be properly packaged, labeled and shipped to the appropriate location(s). The section should also detail the procedures for transporting team members to the original or new site.

Reporting and Revision

To provide for the final step in deactivation of the IT DRP, the IT DRP should provide instructions for developing a written report describing the successes, challenges and lessons-learned during the contingency. Abstracts of operations logs may be very useful as an attachment to this report. The report should be delivered to the agency head and ISO, at a minimum, and protected as sensitive information. The IT DRP should also contain requirements that the IT DRP be revised based on the lessons learned documented in this report.

3.2.7 Recommended IT DRP Appendices

Personnel Contact List

This appendix can be a list, by team, with team member names, phone numbers and home addresses (in case other means of communication are unavailable.)

Vendor Contact List

This appendix should document all service providers, equipment and software maintenance personnel, building or facility maintenance personnel, and any other agency vendors who may need to be contacted.

Customer Contact List

This appendix should document all agency customers.

Equipment and Specifications

This appendix should detail all agency IT equipment that is necessary to execute the DRP. The list should include detailed configuration information.

Internal and External Agreements

This appendix should include copies of all service level agreements, memoranda of understanding, and any other agreement regarding any agency relationships either supported by sensitive agency IT systems or that support those systems.

Standard IT System Operating Procedures

This appendix includes all the procedures the agency (or its service providers) use to operate sensitive agency IT systems under normal (non-contingency) conditions.

3.3 Periodic Review of IT DRP

The agency should review the IT DRP at least annually, and more often as necessary. As part of each review, and more often, as needed, the IT DRP should be revised to reflect changes in essential business functions, services, system hardware and software, and personnel.

3.4 Periodic Exercise of the IT DRP

The IT DRP should be exercised at least annually, and more often as necessary, in order to test the validity of its processes and procedures, and the readiness of the recovery team to execute the plan.

3.4.1 Exercise Planning

To be effective and meaningful, the exercise should be planned to test all aspects of IT supporting essential business functions. An IT DRP exercise plan consists of:

The Scenario

The test scenario is the "script" given to the test participants. It describes:

- The schedule for the exercise.
- The time at which the event described in the scenario is imagined to occur.
- A description of the scenario.
- The impact of the event.
- Details concerning which IT systems have been affected by the event, and how they have been affected.

To adequately test the effectiveness of the IT DRP, exercise planners should develop a test scenario that impacts a significant portion of the agency's sensitive IT systems and data. Loss of a data processing facility is often a common theme.

Exercise Type

Recommended types of IT DRP exercise are:

- A tabletop exercise, which is a validation of the IT DRP. It checks for logical consistency, proper sequencing of activities and procedures and the understanding of the participants of their roles and responsibilities during a contingency. It also provides some limited exercise of decision-making, and can often pinpoint weaknesses in the leadership team. Tabletop exercises are usually relatively low burden and impact. The IT DRP should be validated with a tabletop exercise, and the plan corrected as required, as soon as possible after DRP development, and before committing to a live exercise.

- A live exercise, which is both a validation and verification of the IT DRP. In addition to providing the same checks as a tabletop exercise, a live exercise actually verifies the recovery procedures are both executable, and actually work to recover the IT systems and data. A live exercise is more costly than a tabletop exercise, and incurs some risks, but it is the only way to verify that the IT DRP can be executed.

Evaluation Criteria

The exercise plan should determine what outcomes will be considered successful, and how those outcomes will be measured. For example:

- In a tabletop exercise, one major desired outcome might be that all participants were able to follow the plan, and the sequence of activities made sense to all participants. A metric for this outcome might be that no plan rewrites for consistency are required.

- In a live exercise, one major desired outcome might be that execution of the IT DRP resulted in recovery of all agency sensitive IT systems by a predefined time. A metric for this outcome might be that execution of the IT DRP resulted in recovery of all agency sensitive IT systems by the predefined time.

Participant Roles and Responsibilities

The exercise plan should detail whether or not all team members will need to respond, or only team leadership. Live exercises usually require 100% team participation, while table-top exercises may often be successfully executed with only team leaders as participants. In either

situation, the plan should describe the participants' roles for the exercise, and their responsibilities for exercise execution.

Evaluator Roles and Responsibilities

The exercise plan should describe who the evaluators are, to what extent they can interact with the test teams, and how they should report the exercise results. Evaluators should be experienced IT managers, and their experience should encompass all the IT domains to be exercised. If possible, the evaluators should have no reporting relationship to any of the exercise participants.

3.4.2 Exercise Execution

Participants in IT DRP exercises should be given advance notice of the exercise. While advance notification adds an unrealistic element, it is important that all participants be available. Customer notifications of planned disruption of service may be needed for live exercises. Due to the sensitive nature of IT DRP operations, the agency may prefer to describe the interruption as a maintenance activity.

3.4.3 Exercise Evaluation

Evaluators should record and evaluate the strength and weakness of the exercise. This evaluation should be conducted as soon as practicable following the exercise and should be coordinated with the agency's COOP coordinator. Participants should endeavor to capture and document any lessons learned during the course of the exercise. Exercise evaluations are sensitive information, and should be protected accordingly.

3.5 IT DRP Training

The Standard requires all IT disaster recovery team members be trained on the execution of the IT DRP. This may be conducted as part of the agency's IT security training program. Of course, exercises provide the most realistic training.

4 IT System and Data Backup and Restoration Planning

A critical component to successful disaster recovery is the availability of good quality IT system and data backups. Accurate and complete backups and tested restoration practices protect the

availability and integrity of COV data in case of degradation in the integrity or availability of the IT system or data. Agencies should document a detailed backup and restoration plan to meet these requirements.

4.1 Setting Agency Requirements

The plan should document the IT systems that require backup, and support agency requirements for sensitivity, risk, RTO and RPO. Types and frequency of backups should be described. Types of backups are:

- Full - Includes files whether they have been changed or not;
- Differential - Includes all files changed since the last full backup, whether they have been changed since the last backup operation or not;
- Incremental - Includes only those files that have changed since the last backup operation of any kind.

4.2 Off-Site Storage

The plan should include off-site storage of media in a secured facility, and should document how media will be protected during shipment and storage. Agencies should consider requiring encryption of all data stored off-site, and compartmentalization of data stored off-site according to type and sensitivity of the data.

4.3 Performance of Backups and Restorations

Backups and restorations may only be performed by authorized personnel. It is recommended this authorization be in writing and prominently posted where the operations are performed.

Agency backup and restoration policies, standards, and procedures should specify:

- Personnel who are authorized to request backup copies be sent to the recovery site;
- Personnel who are authorized to request backup copies be returned to the agency;
- Processes for logging data in and out of offsite facilities; and

- Requirements for the security of offsite facilities.

Backup logs that verify the backup plan was properly executed must be maintained and reviewed.

Backup schedules should be designed to support agency requirements. They must be approved by the System Owner.

4.4 Emergency Operations

Agencies should develop a separate plan describing backup and restoration during emergencies. The emergency backup and restoration plan must be approved by the System Owner. This should define what constitutes emergency operations, and detail how the backup and restoration plan changes during emergencies. One common type of emergency operation will be backups and restorations during contingency operations, as described in the IT DRP. The emergency section of the backup and restoration plan will provide a significant input to IT DRP recovery procedures.