ADMINISTRATIVE COMMUNICATIONS SYSTEM

UNITED STATES DEPARTMENT OF EDUCATION

Office of Management, Executive Office

400 Maryland Avenue; Washington, DC 20202

Transmittal Sheet #:	2005-0012	*Date:*	July 12, 2005
Distribution:	All ED employees	*Distribution Approved:* *Directives Management Officer:*	/s/ Tammy Taylor

Action: Pen and Ink Changes

Document Changing: Handbook OCIO-10, *Handbook for Information Technology Security Contingency Planning Procedures*, dated 06/12/2003

Summary: The purpose of this document is to provide Department system owners with guidance on developing IT contingency plans for their general support systems and major applications.

Pen and Ink Changes: The following pen and ink changes were made.

Page	*Section*	*Changed*	*To*
All	Date	06/12/2003	07/12/2005
1	Superseding Information	Information described above	Information described above
All	All	Several corrections were made to the document including formatting changes, punctuation changes, and title changes. No technical changes were made to the document.	

ADMINISTRATIVE COMMUNICATIONS SYSTEM
UNITED STATES DEPARTMENT OF EDUCATION

Handbook

Distribution:
All Department of Education Employees

Approved by: /s/ (06/12/2003)
William J. Leidinger
Assistant Secretary
Office of Management

Handbook for Information Technology Security Contingency Planning Procedures

For technical questions concerning information found in this ACS document, please contact Kathy Zheng on (202) 245-6447 or via e-mail.

Supersedes Handbook OCIO-10, Handbook for Information Technology Security Contingency Planning Procedures, dated 06/12/2003.

DEPARTMENT OF EDUCATION
INFORMATION TECHNOLOGY SECURITY

Handbook for Information Technology Security Contingency Planning Procedures

July 2005

TABLE OF CONTENTS

1. Introduction 1

1.1 Authority 1
1.2 Purpose 1
1.3 Scope 1
1.4 Applicability 1
1.5 Document Structure 1

2. IT Contingency Planning Concepts 3

2.1 Why Develop an IT Contingency Plan? 3
2.2 When Should a Plan be Developed? 3
2.3 How Does the Contingency Plan Feed into the C&A Process? 3
2.4 Who is Responsible for Developing the IT Contingency Plan? 4
2.4.1 Contingency Planning Coordinator 4
2.4.2 Management Team 4
2.4.3 Coordination of GSS and MA Contingency Plans 4
2.5 What are the Different Types of Contingency Plans for IT Systems? 5
2.5.1 Continuity of Support 5
2.5.2 Disaster Recovery Plan 6
2.6 How is the Required Level of Effort for a Contingency Plan Determined? 6
2.6.1 What Type of Contingency Plan is Required for Your IT System? 6

3. IT Contingency Planning Process 8

3.1 Review Department Contingency Planning Policy 8
3.2 Conduct Business Impact Analysis 8
3.2.1 Identify Essential IT Resources 8
3.2.2 Identify Disruption Impacts and Allowable Outage Times 8
3.2.3 Develop Recovery Priorities 9
3.3 Identify Preventive Controls 9
3.4 Develop Recovery Strategies 10
3.4.1 Backup Methods 10
3.4.2 Alternate Sites 12
3.4.3 Equipment Replacement 14
3.4.4 Personnel Roles and Responsibilities 14
3.5 Develop the Plan 15
3.6 Plan Testing, Training, and Exercising 15
3.6.1 Plan Testing 15
3.6.2 Personnel Training and Exercises 16
3.7 Plan Maintenance 17
3.7.1 Distribution of the Plan and Version Control 17
3.7.2 Supporting Documentation 18

4. IT Contingency Plan Structure and Development 19

4.1 Supporting Information 19
4.1.1 Introduction 19
4.1.2 Concept of Operations 19
4.2 Notification/Activation Phase 20

4.2.1 Notification Procedures 20
4.2.2 Damage Assessment 22
4.2.3 Plan Activation 22
4.3 Recovery Phase 23
4.3.1 Sequence of Recovery Activities 23
4.3.2 Recovery Procedures 23
4.4 Reconstitution Phase 24
4.5 Plan Appendices 25

Appendix A. ACRONYM LIST A-1

Appendix B. Glossary of Terms and Definitions B-1

Appendix C. Sample Contingency Plan Template C-1

Appendix D. References D-1

1. Introduction

1.1 Authority

This procedures document is based on the *Handbook for Information Assurance Security Policy*, the *Information Assurance Program Management Plan (IAPMP)*; National Institute for Standards and Technology (NIST) Special Publication (SP) 800-34, *Contingency Planning Procedures for Information Technology Systems*; Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources;* and other Federal information technology (IT) security laws and regulations.

1.2 Purpose

The purpose of this document is to provide U.S. Department of Education (Department) system owners with guidance on developing IT contingency plans for their general support systems (GSS) and major applications (MA). This procedures document will describe requirements for contingency planning and provide information on preventative controls, recovery methods, and the appropriate format for a contingency plan. This information is intended to assist Department staff in determining the most appropriate contingency planning methodology and documenting a contingency plan specifically for each GSS and MA.

1.3 Scope

This procedures document includes sections describing an IT contingency plan, why a contingency plan is important, how a contingency plan feeds into the certification and accreditation (C&A) process, and the basic requirements for developing a contingency plan. The focus of this procedures document is Continuity of Support (COS) and Disaster Recovery Planning (DRP) that emphasizes the technical recovery of systems. This procedures document does not concentrate on recovery of business functions as covered in Business Resumption Plans (BRPs), Continuity of Operations (COOP) Plans, or Occupant Evacuation Plan (OEP).

1.4 Applicability

Contingency plans as described in this procedures document are required for all GSSs and MAs[1]. The system owner should ensure that the plan developed for his/her system addresses all of the requirements set forth in this procedures document. *Sections 2.4* and *2.5* provide details regarding the specific type of plan necessary for each GSS/MA.

1.5 Document Structure

This procedures document is organized into four (4) major sections. **Section 1** introduces the IT contingency planning process. **Section 2** provides an overview of the major IT contingency planning concepts as well as how the IT contingency planning process is related to the C&A process. **Section 3** describes the IT contingency planning process, including how to:

- Conduct a business impact analysis (BIA);

[1] *Handbook for Information Technology General Support Systems and Major Applications Inventory Procedures* can be used to help determine if a particular system is a GSS or MA.

- Identify preventative controls;
- Develop recovery strategies;
- Develop the IT Contingency Plan;
- Train team and subteam members; and
- Test, exercise and maintain the plan.

Section 4 develops the IT Contingency Plan structure, walking through the notification/activation phase, recovery phase, and reconstitution phase. Supporting this procedures document are four (4) appendices:

- Appendix A. Acronym List;
- Appendix B. Glossary of Terms and Definitions;
- Appendix C. Sample Contingency Plan Template; and
- Appendix D. References.

2. IT Contingency Planning Concepts

2.1 Why Develop an IT Contingency Plan?

An IT Contingency Plan is an essential component in the overall strategy of a business or public service organization to ensure the successful recovery of operations and functionality of essential IT resources in the event of an emergency or service interruption. Effective IT contingency planning results in an organization's ability to quickly and cost effectively recover essential IT resources following a service disruption or outage. An IT Contingency Plan will provide the system manager procedures for handling system disruption or outage to avoid any adverse impact on the Department's ability to fulfill its mission. These procedures will assist key personnel through the notification, recovery, and reconstitution of system phases in the event of an emergency.

2.2 When Should a Plan Be Developed?

IT contingency planning should be integrated into all aspects of the system development life cycle (SDLC). The IT Contingency Plan should be an active document that is tested and updated as needed throughout the entire SDLC.

- *Project Initiation and Requirements Specifications Phases.* During the project initiation and requirements specification phases of a new system, the system owner should consider contingency requirements based on the criticality of the new system. These requirements include measures to reduce the impact to the system in the event of a service interruption and to estimate potential future costs for providing recovery needs such as an alternate processing location. This initial evaluation will help determine the depth and level of effort required to adequately cover contingency planning.
- *Design Phase.* Contingency planning details should be incorporated into the design phases of the system development. Testing of the plan should occur concurrently with system testing, with updates made to the plan as necessary.
- *Maintain Phase.* During the maintain phase of the system life cycle, contingency planning activities such as training, testing, and regular updates to the plan should occur.
- *Disposal Phase.* Finally, the IT Contingency Plan should remain active through the disposal phases of a system, until the new or replacement system has its own fully developed and tested contingency plan.

2.3 How Does the Contingency Plan Feed into the C&A Process?

The C&A process requires contingency plan development as part of *Phase 1: Definition,* described in the *Handbook for Information Technology Security Certification and Accreditation Procedures*. A GSS or MA that lacks a contingency plan will not fulfill all the documentation requirements of the C&A process, thus resulting in the Certifier recommending that the Designated Approving Authority (DAA) deny accreditation.

During the contingency plan development, recovery procedures are identified and incorporated into the plan to ensure the availability of GSSs or MAs in the event of a natural or man-made disruption. It is important to align the contingency plan with the results of the risk assessment

(RA) process and baseline security requirements (BLSR) that are reviewed as part of that process. The system manager should ensure that the contingency plan provides security controls commensurate with the system's requirements. Security should not be sacrificed to save time or money in the recovery process. For example, a system requiring encryption under normal circumstances should ensure that operations in recovery mode are also operating on systems with equivalent protective measures, i.e., encryption.

2.4 Who is Responsible for Developing the IT Contingency Plan?

2.4.1 Contingency Planning Coordinator

The system manager, working closely with the business manager, is responsible for developing an IT Contingency Plan for each GSS or MA under his or her control. The system manager should act as, or appoint and oversee, a contingency planning coordinator (CPC). The CPC will be responsible for organizing subteams with system specific expertise, including but not limited to the system security officer (SSO), database administrator (if applicable), system owner, and functional subject matter experts (SME) such as service vendors and contractor support personnel. Listed below are types of subteams that may be necessary to include in the disaster recovery process:

- Management
- Damage Assessment
- Server Recovery
- Application Recovery
- Alternate Site Recovery
- Media Relations
- Legal Affairs
- Physical/Personnel Security

The number and size of subteams will depend on the complexity of the system and whether it is a GSS or MA. The system manager should use these, and any other system-specific criteria, to set up a sufficient number of subteams that will allow contingency operations to function as effectively and efficiently as possible.

It is important to consider how a GSS plan will coordinate or overlap with the contingency plans for MAs. Each system owner should fully understand his or her responsibilities for contingency planning and how the system ranks in terms of priority for recovery. A CPC for a MA may appoint staff that will be responsible for coordinating contingency planning with the GSS that hosts the system. Likewise, the CPC for a GSS may assign staff to work with the CPCs of MAs that it supports. Regular training and plan testing will enable the staff to fully understand their roles and responsibilities, as well as identify deficiencies in the plan.

2.4.2 Management Team

The Management Team serves as the central contact point for all contingency operations. The Management Team will activate contingency plans in the event of a disruption or outage and coordinate and facilitate communications between teams. The Management Team will also arrange to test and exercise the plan throughout the year. It is recommended that a senior management official, such as the Principal Officer, serve as the head of the Management Team.

2.4.3 Coordination of GSS and MA Contingency Plans

Contingency plans developed for Department MAs should be well coordinated with all associated GSS contingency plans throughout each stage of the plan, from development to implementation to testing and updating. Coordination with the GSS owner can be achieved

through the use of a Memorandum of Understanding (MOU) or a Memorandum of Agreement (MOA).

2.5 What are the Different Types of Contingency Plans for IT Systems?

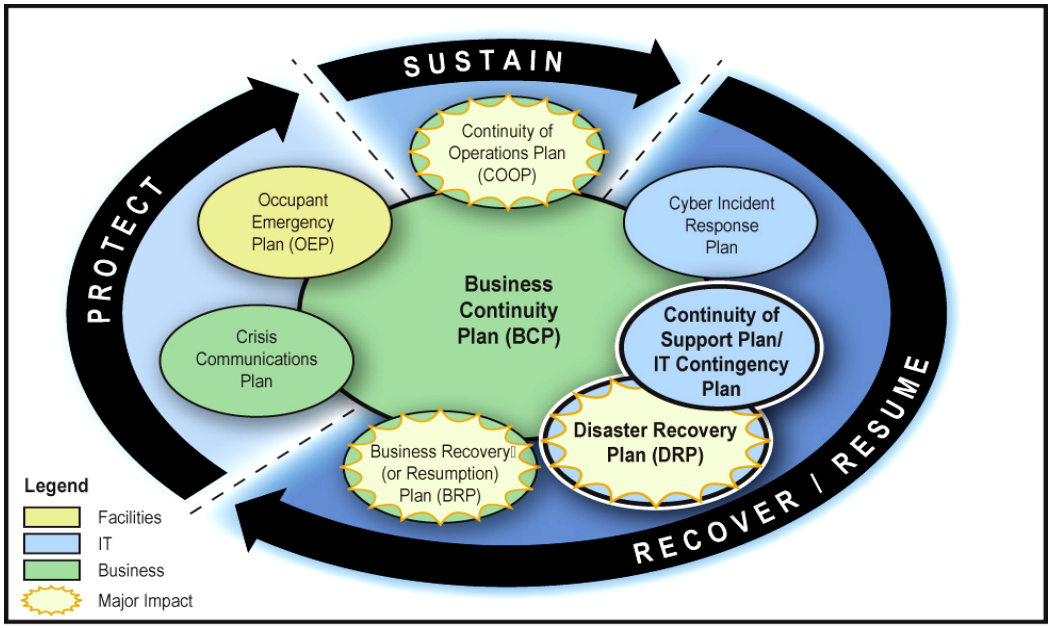
Contingency planning represents a broad scope of activities designed to sustain and recover IT systems following a disaster or service interruption. An organization must plan for the continuity of business operations, facilities support, and IT support. In order to do this, several types of plans can be created to address these issues (see *Table 2-1* below).

Types of Contingency Related Plans		
Business Operations Support	***Facilities Support***	***IT Support***
Continuity of Operations Plan (COOP)	Occupant Evacuation Plan (OEP)	Continuity of Support Plan
Business Recovery/Resumption Plan (BRP)		Disaster Recovery Plan
Crisis Communication Plan		Cyber Incident Response Plan

00757b

Table 2-1. Contingency Plans

Figure 2-1 shows how the various plans relate to each other, each with a specific purpose. This procedures document will focus on guidance for the Continuity of Support and the Disaster Recovery Plan. See Sections *2.5.1* and *2.5.2* for detailed descriptions of these types of plans.



00758

Figure 2-1. Business Continuity Planning

2.5.1 Continuity of Support

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires the development and maintenance of continuity of support plans for GSSs and IT contingency plans for MAs. Continuity of Support Plans are intended to provide guidance for

short-term service interruptions (less than 48 hours) that do not require relocation to an alternate processing site. Examples of short-term interruptions that do not require relocation include print server outages or a temporary loss of power. These plans need to be as detailed as necessary to support the system based on the system's security tier level and degree of criticality. (See Section 2.6 for further explanation of how a system's tier level effects the contingency planning requirements.) The plan will include any preventative measures for protecting the IT systems as well as procedures for restoring any system disruption.

Note: OMB Circular A-130, *Appendix III*, requires continuity of support plans for general support systems and contingency plans for major applications. *NIST SP 800-34* considers continuity of support planning to be synonymous with IT contingency planning.

For the remainder of this document, we will use the term "Continuity of Support" to refer to short-term IT Contingency Plans, and "IT Contingency Planning" to refer to the whole process.

2.5.2 Disaster Recovery Plan (DRP)

DRPs are necessary for reacting to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of a COS; however, the DRP is focused on long-term outages (over 48 hours) that require relocation to an alternate processing site. The DRP does not address minor disruptions that do not require relocation. Generally, a DRP is included as part of the IT Contingency Plan if it is required based on system criticality and data sensitivity.

2.6 How is the Required Level of Effort for an IT Contingency Plan Determined?

Each Department GSS and MA has been categorized into one of four certification tiers (e.g., Tier 1, Tier 2, Tier 3, or Tier 4). The tier levels have been determined as part of an earlier C&A activity, based on the system criticality and sensitivity levels (determined by confidentiality, integrity, and availability).[2] The certification tier of the GSS or MA determines the level of effort required for contingency planning. For example, a Tier 3 or 4 system (with high criticality and high data sensitivity) will require **a fully documented, detailed analysis** of contingency planning activities in a stand-alone document that contains both the COS and a DRP. Systems classified as Tier 1 and Tier 2 only need a COS and may include this as part of their System Security Plans (SSP) if appropriate.

2.6.1 What Type of Contingency Plan is Required for Your IT System?

The system manager will base the type of contingency plan required for the system on its risk assessment and tier level. *Table 2-2* below highlights what is required for each system based on its tier level.

Certification Tier	Required Level of Effort for IT Contingency Planning
1	Only Continuity of Support Plan

[2] *Refer to the Handbook for Certification and Accreditation Procedures, Appendix E and Section 2.7.1, for detailed information on how the certification tier is determined for the GSS or MA.*

2	Only Continuity of Support Plan
3	Continuity of Support Plan PLUS Disaster Recovery Plan
4	Continuity of Support Plan PLUS Disaster Recovery Plan

Table 2-2. Required Level of Effort for IT Contingency Planning

3. IT Contingency Planning Process

3.1 Review Department Contingency Planning Policy

Before developing the IT Contingency Plan, the system manager shall review the Department's Contingency Planning requirements, found in the *Handbook for Information Assurance Security Policy* to determine requirements and responsibilities. The certification and accreditation tier level is determined by the *Handbook for Information Technology General Support Systems and Major Applications Inventory Procedures*; and the *Handbook for Information Technology Security Certification and Accreditation Procedures* provides the manager with proper guidance to identify the level of effort required for developing the contingency plan.

3.2 Conduct Business Impact Analysis (BIA)

The purpose of the BIA is to correlate specific information resources with the essential services that they provide. Based on that information, the consequences of a disruption to the system and the business components it supports can be determined. Steps in the BIA process include identifying essential IT resources, identifying disruption impacts and allowable outage times, and developing recovery priorities. Results from the BIA will be appropriately incorporated into the systems contingency plans. A sample BIA can be found in the IT Contingency Plan template, available on *ConnectED* under the Information Assurance Policies/Procedures/Guides link of the Computer Security page.

3.2.1 Identify Essential IT Resources

During this stage, essential functions performed by the system and resources required to support them are identified. The CPC will coordinate with all internal and external points of contact (POC) associated with the system to identify the way that each one depends on or supports the system. Security, managerial, technical, and operational requirements are all key areas to include when identifying IT resources. The CPCs for GSSs and the MAs that it supports will work together to determine the extent to which the GSS is responsible for IT resources the MA uses and vice versa. A clear delineation of responsibilities and expectations must be fully documented as part of the plan.

After the support groups are identified, the CPC will link these services to system resources, specifically infrastructure requirements. The infrastructure requirements identified will be as specific as possible including electric power, telecommunications, environmental controls, and IT resources such as routers, servers, and firewalls.

3.2.2 Identify Disruption Impacts and Allowable Outage Times

During this phase of the BIA, the CPC will analyze the essential resources defined in the previous step and determine the impact on IT operations if a given resource was disrupted or damaged. The impact will be evaluated based on both its effects *over time* and *across related resources*. The maximum allowable time that a resource may be down before affecting the performance of an essential function is to be determined and documented. Determining the cascading effects of how a system outage may disrupt other systems is also a key aspect of this step. Cascading effects of a system outage may be more detailed when analyzing a GSS, and the

appropriate amount of time will be spent to adequately document the results. Impact across related resources may be less prevalent for an outage of an MA, but should nonetheless be taken into consideration.

The timing of the outage may also play a critical role in determining allowable outage times. Some business functions rely on a specific GSS or MA during specific times of day, month, or year to carry out their mission. These factors must be taken into consideration when conducting the BIA and later, in developing the plan.

3.2.3 Develop Recovery Priorities

After identifying the disruption impacts for each system, the CPC will develop the recovery strategy that takes into account the priority of system to be recovered based on their allowable outage times and effects across related systems. In addition to prioritizing system recovery needs, the CPC will also evaluate the most efficient and cost-effective method of system recovery. For example, systems that rely on the same or similar resources can be recovered together to create a cost efficiency. Having a predefined recovery strategy will save time, effort, and costs in the event of an actual emergency.

3.3 Identify Preventive Controls

In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost effective, implementing preventive methods is preferable to actions that may be necessary to recover the system after a disruption.

The following is a list of common preventative measures:

- Uninterruptible power supplies (UPS) provide short-term power to all systems to allow time for a graceful shutdown of systems that should minimize data loss. A UPS should be able to support the system for at least 30 minutes to one hour.
- Gasoline- or diesel-powered generators to provide long-term backup power;
- Fire suppression system;
- Fire and smoke detectors;
- Water sensors in ceiling and floor of computer room;
- Emergency master shutdown switch;
- Frequent, scheduled backups;
- Heat-resistant and waterproof containers for backup media;
- Off-site storage location for backup media; and
- Redundant hardware.

This is not a comprehensive list of all potential preventative controls. The CPC will work with the system managers to determine the type and extent of preventive measures to take based on the system.

All preventive measures in place must be maintained and tested periodically to ensure their effectiveness. In addition, reassessing the preventive measures needed on an annual basis will ensure that the system continues to have an adequate level of protection and can take advantage of any new preventive measures that become available, if necessary.

3.4 Develop Recovery Strategies

The recovery strategies developed for the system will address the disruption impacts and allowable outage times as identified in the BIA. Several alternatives must be considered when developing the strategy, including cost, personnel requirements, system sensitivity and classification, allowable outage time, security, and integration with larger, organization-level contingency plans.

The recovery strategy that is selected and incorporated into the contingency plan must address the potential impacts identified in the BIA. The strategy must also be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy must include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. The appropriate recovery strategy for the system will depend on the incident, the type of system, and its operational requirements. Consideration should be given to data backup, recovery site, and equipment replacement needs.

3.4.1 Backup Methods

Backing up data and storing it off-site is a key aspect of effective contingency planning. As part of each system's contingency plan, the comprehensive backup policy and supporting procedures must be fully documented. The backup policy must include the backup frequency, backup storage time frame, and details on the off-site storage location. Data can be backed up onto a variety of media, including magnetic disk, tape, and optical disk (CD). The system manager will decide the type or combination of media types based upon system requirements.

3.4.1.1 Backup Frequency

The backup policy will include details as to the frequency of the backups. The most commonly used methods are full, incremental, differential, or a combination of the three.

Full Backup. A full backup captures all files on the system each time it is performed. This method is beneficial in guaranteeing the backup of all files and providing ease of locating the files. However, this method can require a large number of the backup media (CDs, tapes, or disks), take a long time to complete, and may not be cost effective.

Incremental Backup. An incremental backup captures files that were created since the last backup, regardless of the backup type (full or incremental). Incremental backups use less backup media and take less time than full backups. Recovery time can be slower with incremental backups, because both the last full backup and all the incremental backups since that point must be loaded.

Differential Backup. A differential backup stores files that were created or modified since the last full backup. If a file is changed after the previous full backup, the differential backup will save this file each time it is run until the next full backup is performed. This method requires fewer media and takes less time than a full backup, but takes longer than an incremental backup because the amount of data to store increases each day until the next full backup is performed.

Many organizations choose to use a combination of these methods. Common backup policies involve weekly full backups and either incremental or differential backups on a daily basis. Restoration of this backup data should be tested at regular intervals to ensure that not only has

data been stored, but it can also be restored. Full backups should be performed on a quarterly, half yearly, and yearly basis.

3.4.1.2 Retaining Backups

It is important to determine how long to keep each set of backup tapes and how often tapes may be reused. Restore procedures will be tested regularly as well. These details will be included in the backup procedures. An example of this is shown in *Table 3-1*.

Type of Backup	Storage Length
Annual	3-5 years
Semiannually	3-5 years
Monthly	6 months
Daily	1 month

Table 3-1. Retaining Backups

Keep in mind the above table is only an example. It is important for the system manager, CPC, and contingency planning team to determine how long backups are required based on system-specific criteria or any federal regulations.

3.4.1.3 Off-Site Storage

It is essential to store backup tapes at an off-site location to ensure that they are intact and available when needed. The system operations staff is generally responsible for performing the backups, labeling the media, and making them available for off-site storage. Often, a vendor is responsible for picking up the backups and returning any tapes that no longer need to be stored off-site. The following are some factors that must be considered when selecting an off-site storage location:

- **Geographic proximity.** Proximity to the organization must not be so close as to increase the possibility that the off-site location will be affected by the same disaster as the organization.
- **Accessibility.** The length of time it will take to retrieve the data from storage and the storage facility's operating hours must be considered.
- **Security.** The security of the facility and the level of clearance held by the employees of the off-site vendor will be commensurate with those required by the system based on the data sensitivity.
- **Environment.** The off-site storage vendor will furnish detailed specifications of the structural and environment controls at the facility.
- **Cost.** The cost of shipping, operational fees, and any other services that the off-site storage vendor provides will be within the means of the system requirements.
- At no time will a staff member's home be considered for off-site storage.

3.4.2 Alternate Sites

Each Tier 3 and Tier 4 system will have plans for recovering operations at an alternate facility. An alternate site will be selected based on the party responsible for maintaining the site and the operational readiness of the site. Based on these two factors, a number of alternate facility solutions options can be identified, each differing in cost, equipment, and location. The system manager, CPC and contingency planning team must use the information provided by the BIA to determine what type of facility can adequately support the system in the event of an emergency.

There are three (3) common options available when selecting the party responsible for running the alternate site.

1. The Department or the Principal Office (PO) that owns the General Support System within which the system resides may own and operate the alternate site (internal recovery). This method provides the greatest assurance that the specifications always meet the system requirements and that the site is always available.

2. The Department or the PO may enter into a formal agreement with another organization or agency with similar IT needs for joint use of an alternate site. This type of agreement is beneficial in reducing costs to the organization as the costs are shared with another entity. It is important for each organization to test sufficiently the systems and to include any necessary prioritization requirements or special needs into the formal agreement. If choosing this option, participating organizations must ensure that there is enough space at the facility to support all systems concurrently in the event of a disaster or outage affecting all participants.

3. The Department or the PO may opt to use a commercially leased facility as the alternate processing location. When contracting with a commercial vendor, all aspects of the recovery process (testing needs, work space, security requirements, infrastructure requirements, and support services) must be negotiated and included in the contract. Further, the system manager must be aware of whether other organizations in nearby locations might be using the same vendor. Contract negotiations must include any prioritization requirements to ensure that the system is available as needed.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, identifies five commonly used types of recovery sites that vary based on the operational readiness they provide. From most basic to most complex, the types are described below.

Cold Sites typically consist of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system. The space may have raised floors and other attributes suited for IT operations. The site does not contain IT equipment (such as servers) and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities. This is the least expensive alternative to maintain, but it also requires the greatest amount of time to set up following a disaster.

Warm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status ready to accommodate the relocated system. The site may need to be prepared before receiving the system and recovery personnel. In many cases, a warm site may serve as a normal operational facility for another system or function, and in the event of contingency plan activation, the normal activities are displaced temporarily to accommodate the disrupted system.

Hot Sites are office spaces appropriately sized to support system requirements and configured with all the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, 7 days a week. Hot site personnel begin to prepare for the system relocation as soon as they are notified that the contingency plan has been activated. This is the more expensive to maintain than a cold or warm site, but provides a faster response time to a disaster.

Mobile Sites are self-contained, transportable shells custom-fit with specific telecommunications and IT equipment necessary to meet system requirements. These sites are available for lease through commercial vendors. The facility often is contained in a tractor-trailer and may be driven to and set up at the desired alternate location.

Mirrored Sites are fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data is processed and stored at the primary and alternate site simultaneously. These sites typically are designed, built, operated, and maintained by the organization.[3] This is the most expensive to maintain but provides seamless response to disasters.

Table 3-2 depicts the key characteristics and highlights the key distinguishing feature of each type of alternate site. The "Distinguishing Feature" column provides the key factor that sets one site apart from the others and what is most likely to be the driving force for selection.

Site	Cost	Hardware Equipment	Telecommu-nications	Setup Time	Location	Distinguishing Feature
Cold Site	Low	Partial	Partial	Long	Fixed	Inexpensive
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed	Combination of Hot and Cold Site Attributes
Hot Site	Medium/High	Full	Full	Short	Fixed	Full Resource Accessibility
Mobile Site	High	Variable*	Variable*	Variable*	Not Fixed	Flexible Location
Mirrored Site	High	Full	Full	None	Fixed	Instant Availability

*Mobile site can be configured as a cold, warm, or hot site depending on organization's requirements.

Table 3-2. Alternate Processing Locations

The CPC will use the BIA to make an informed decision as to which type of site should be selected for alternate processing of the system. Regardless of what type of site is chosen, the organization must also decide how many staff the site can support. The CPC will base this decision on the BIA that must address how many personnel are necessary to operate the system and keep business operations functional during the recovery phase at the alternate site.

[3] NIST SP 800-34, *Contingency Planning Guide for Information Technology (IT) Systems*, June 2002.

3.4.3 Equipment Replacement

In the event that only the equipment at the primary site is destroyed and rendered inoperable or unavailable, but the site is still available for use, it is necessary to procure new hardware and software. There are three strategies for equipment replacement available—vendor agreements, equipment inventory, and existing compatible equipment. The system manager/CPC must incorporate the impact analysis from the BIA stage when determining which method to use.

Vendor Agreements. As the contingency plan is being developed, Service Level Agreements (SLAs) with hardware, software, and support vendors may be made for emergency maintenance service. The SLA must specify how quickly the vendor must respond after being notified. The agreement must also give the organization priority status for shipping replacement equipment over equipment being purchased for normal operations. SLAs must further discuss what priority status the organization will receive in the event of a regional or catastrophic disaster involving multiple clients of the vendor. In such cases, organizations with health- and safety-dependent processes will often receive the highest priority for shipment. The details of these negotiations will be documented in the SLA, which must be maintained with the contingency plan.

Equipment Inventory. Required equipment may be purchased in advance and stored at a secure off-site location. These offsite locations include an alternate site where recovery operations will take place (warm or mobile site) or at another location where the equipment will be stored and then shipped to the alternate site. This solution has certain drawbacks, however. An organization must commit financial resources to purchase this equipment in advance and the equipment could become obsolete or unsuitable for use over time because of changing system technologies and requirements.

Existing Compatible Equipment. Equipment currently housed and used by the contracted hot site or by another organization within the agency may be used by the organization. Agreements made with hot sites and reciprocal internal sites stipulate that similar and compatible equipment will be available for contingency use by the organization. The system manager must ensure the equipment is fully compatible, especially with regard to security controls. Security controls on the existing compatible equipment will be commensurate with security requirements and will not be sacrificed to save time or money in the recovery process.

3.4.4 Personnel Roles and Responsibilities

Section 2.4 discussed the types of teams that may need to be involved in contingency planning. The same teams, and others if necessary, will also need to be included as part of the overall recovery team. For example, if there were a database recovery team that developed the procedures for recovering the database, this team would also be a key recovery team subteam.

The Management Team will be the central point for all contingency and recovery activities. Each subteam will have a team lead and an alternate team lead, who are responsible for the rest of the team and act as a liaison to the Management Team. An appropriate team leads for the database recovery team would be the database administrator and a suitable alternate would be a backup database administrator. Other subteams may include staff with these areas of expertise:

- Management
- Damage Assessment

- Server Recovery
- Application Recovery
- Alternate Site Recovery
- Media Relations
- Legal Affairs
- Physical/Personal Security
- GSS/MA Coordination Team
- Personnel Security

Members of these teams may include, but are not limited to, the SSO, database administrator (if applicable), system owner, and function SMEs such as service vendors and contractor support personnel.

Cross team training can be very beneficial to an organization that has staff located in more than one location. In the event that an emergency prevents or delays staff in one location from performing their assigned recovery duties, a team that has been cross-trained to assist can be used in their place. To address this issue, the CPC may identify cross teams at the two locations and train each team in the overall contingency plan, as well as in each individual's specific responsibilities in executing the contingency plan. In the event that cross-training is used, the contingency plan should clearly define the conditions for each team's use.

All team members must be trained to fully understand the policy and procedures of the contingency plan and be ready to activate the plan when necessary. Each team member must also clearly understand his or her specific responsibilities and the necessary procedures to execute the plan. It is important that the Management Team conducts training and plan testing at least annually. This will ensure the effectiveness of the contingency plan and allow the recovery teams to gain practical experience in coordinating their activities and working together.

3.5 Develop the Plan

Once all the preceding steps have been completed, the system manager must develop the plan in accordance with the policies and guidance developed by the Department to include this document. Section 4 details the key sections of what must be included in an IT Contingency Plan.

3.6 Plan Testing, Training, And Exercising

Plan testing is an essential element of a viable contingency capability. This enables plan deficiencies to be identified and addressed prior to implementation during a disruption or disaster. Each plan element must be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. Effective plan testing will cover different test scenarios, will occur regularly (especially when changes are made to the system), and will be performed by all necessary personnel including vendors and contractors as applicable.

Testing will also help evaluate the ability of the recovery staff to implement the plan quickly and effectively. Prior to plan testing, appropriate training must be provided to all Department personnel, including contractor staff, who bear responsibility for system recovery and continuity.

3.6.1 Plan Testing

Plan testing begins with the development of working groups that will meet before conducting the plan testing to discuss ideas regarding the most appropriate method for the testing. Based on the Contingency Plan and any feedback from the working groups, test procedures will be developed.

Detailed procedures will contain information for conducting the test, guidelines for when the test will be run, and under what conditions (i.e., rules of engagement), and how any weaknesses or inefficiencies will be documented and reported back to the system's management.

Specific, measurable test objectives must be developed as the driving force behind the test procedure. An example of a specific test objective would be to "Recover XYZ Database within # of hours." These test objectives can fall in the following categories:

- System recovery on production platforms using backup tapes;
- System recovery on alternate platforms using backup tapes;
- Coordination among recovery teams;
- Internal and external recovery;
- System performance using alternate equipment; and
- Restoration of normal operations.

After defining the test objective, the detailed test procedure can be developed.

Before conducting the actual test procedure, a walk-through of the test must be conducted. The walk-through will be designed to validate the test script and correct any identified flaws prior to the test. This stage in the process is designed to ensure that the full-scale test is run smoothly and cost effectively.

Once the walk-through is complete, modifications to the script will be made and the test will be conducted. During the test, any weaknesses identified will be documented and reported to the Management Team and CPC for correction. Once the script and recovery procedures have been updated and approved, the CPC will arrange a second test (and using the same process described above for the first test) to ensure that areas for improvement identified in the initial test have been addressed. The focus of the second test will be to identify additional areas for improvement and check the adequacy of corrective measures implemented as a result of the initial test. The second test will focus on the same scenario tested during the first test.

All test results must be documented in detail and reviewed by the test team. Lessons learned from the test plans and results will be incorporated into the latest version of the Contingency Plan and used when developing future test plans.

3.6.2 Personnel Training and Exercises

Specialized training for all individuals involved with contingency planning and disaster recovery is essential. Training must be provided at least annually and will complement the plan testing that occurs. If a new hire is to be given responsibilities involving the contingency plan, he or she must be trained soon after their start date; management must ***not*** wait for these staff members to attend the next annual training. Each disaster recovery team member must be familiar with his or her roles and responsibilities and be able to execute them without the aid of the Contingency Plan in the event that the document is unavailable during the emergency event.

Recovery personnel will be trained on the following elements:

- Purpose of the plan;
- Cross-team coordination and communication;

- Reporting procedures;
- Security requirements;
- Team specific processes during the activation/notification, recovery, and reconstitution phases; and
- Individual responsibilities during the activation/notification, recovery, and reconstitution phases.

Training can be accomplished using a variety of means, including review of the Contingency Plan in a classroom setting and functional exercises that include plan tests and simulations.

3.7 Plan Maintenance

The system manager will maintain and update the plan as necessary at least annually or whenever significant changes to the system occur. As deficiencies in the plan are identified through testing and through exercises, the system manager must identify and implement corrective measures and provide updates to appropriate Department personnel, as defined in the *Handbook for Information Assurance Security Policy* and the *Information Technology Security Compliance Guide*.

Plan reviews will focus on the following:

- Operational requirements;
- Security requirements;
- Technical procedures;
- Hardware, software, and other equipment;
- Names and contact information of team members;
- Names and contact information of vendors; and
- Alternate and off-site storage facility requirements.

The system manager and the CPC will define the frequency that the plan or its elements must be reviewed. In addition to the yearly review, the CPC may elect to review some portions of the plan more frequently. For example, an office that experiences high turnover or changes physical office locations frequently may choose to review the contact lists on a quarterly basis.

The CPC for a GSS will coordinate contingency plan tests and updates with the CPCs for any MAs that the GSS supports. If either a GSS or MA makes a change to their contingency plan that would affect the other, it is necessary that the appropriate persons are aware of this change so that the affected system can update its contingency plan accordingly. A review of the existing coordination between related GSS and MA contingency plans must be conducted annually at a minimum.

3.7.1 Distribution of the Plan and Version Control

The plan will be distributed in accordance with Department policies regarding sensitive documentation. Only authorized personnel and contractors with appropriate security clearances should have access to view any contingency plan with sensitive information. The system manager and the CPC will maintain a list of all personnel that have a copy of the IT Contingency Plan. Copies of the IT Contingency Plan and all supporting documentation must also be stored at an off-site storage facility.

All changes to the IT Contingency Plan must be authorized by the CPC, who then assigns a staff person to make the change. This control ensures that multiple persons do not change the document simultaneously. Plan modifications and changes must be recorded in a record of changes table within the document, noting the page number of the change, a brief description of the change, the date and the name of the person making the change. *Table 3-3* provides an example of a record of change.

Record of Changes			
Page Number	**Description of Change**	**Date**	**Name**
15	Updated Joe Smith's contact information in the call tree	7/20/02	Jane Jones

Table 3-3. Record of Changes

3.7.2 Supporting Documentation

In addition to updating the Contingency Plan frequently, the system manager will ensure that all supporting documentation is reviewed annually and updated as necessary. Some examples of supporting documentation include:

- Contracts for the alternate processing site, off-site storage facility, and equipment; replacement vendors;
- Software licenses;
- MOUs;
- Hardware and software requirements; and
- Training awareness materials.

It also may be necessary to periodically update the BIA, especially when major changes are made to the system or critical components.

4. IT Contingency Plan Structure and Development

4.1 Supporting Information

The supporting information component includes an *Introduction* and *Concept of Operations* sections that provide essential background or contextual information that makes the IT Contingency Plan easier to understand, implement, and maintain. These sections will include a brief description of the purpose, scope, and applicability of the IT Contingency Plan. In addition, supporting information will provide a description of the different sections of the document and any documents that were referenced in developing the plan.

4.1.1 Introduction

This section must includes the following:

- **Purpose:** Establishes the reason for developing the IT Contingency Plan and defines plan objectives.
- **Applicability:** Documents the organizations impacted by the IT Contingency Plan.
- **Scope:** Addresses the issues, situations, and conditions that are both addressed and not addressed by the plan. The level of detail and extent of the plans would be documented in this section.

Planning Principles: This section will describe the preventive controls that have been taken by the organization to support the system. Preventive controls include backup methods, alternate processing sites, and equipment replacement plans. Key information to include would be what type of controls are in place, how they are executed, where off-site locations exist, and other applicable details. Any vendor contracts or MOUs must be referenced and included in an appendix to the IT Contingency Plan.

Key Assumptions: COS assumes a short-term outage (less than 48 hours) that does not require relocation to an alternate site. DRPs assume a long-term outage (greater than 48 hours) that will require relocation to an alternate site. Any assumptions taken must be documented. These assumptions can include assumptions regarding the state of operational controls and personnel availability.[4] Assumptions, however, must not be a substitute for adequate planning. For example, it would be inappropriate to assume that disruptions would only occur during business hours.

References/Requirements: Identifies federal or agency requirements for contingency planning.

Record of Changes: Contains a list of all modifications made to the document since its inception. (An example of Record of Changes is provided in *Section 3.7.1*.)

4.1.2 Concept of Operations

This section will provide additional details about the IT system and the contingency planning framework. The following elements may be included:

[4] *NIST SP 800-34, Appendix A, provides several detailed examples of contingency plan assumptions.*

- **System Description.** This description will include the IT system architecture, location, and any applicable diagrams.
- **Line of Succession.** The order of succession identifies personnel responsible to assume authority for executing the contingency plan in the event the designated person is unavailable or unable to do so.
- **Responsibilities.** The responsibilities section will present an overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. Roles must be assigned to team positions rather than specific individuals. This will help reduce confusion and the need to constantly update the plan whenever an individual changes roles. *Sections 2.4* and *3.4.4* of this document provide a high-level overview of possible teams and team roles.

4.2 Notification/Activation Phase

The Notification/Activation Phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel (including when key Department personnel are unreachable), assess system damage, and implement the plan. At the completion of the Notification/Activation Phase, Department staff will be prepared to perform contingency measures to restore system functions on a temporary basis, as defined in the plan.

4.2.1 Notification Procedures

Events requiring activation of the IT Contingency Plan may occur with or without prior notification. In either situation, notification procedures in the IT Contingency Plan must be detailed and include methods (e-mail, phone, pager, and mass media) to contact people during both business and non- business hours.

A call tree is an effective tool for notifying all necessary personnel of a disaster event and activating the plan. See *Figure 4-1* on the following page for an example of a call tree.

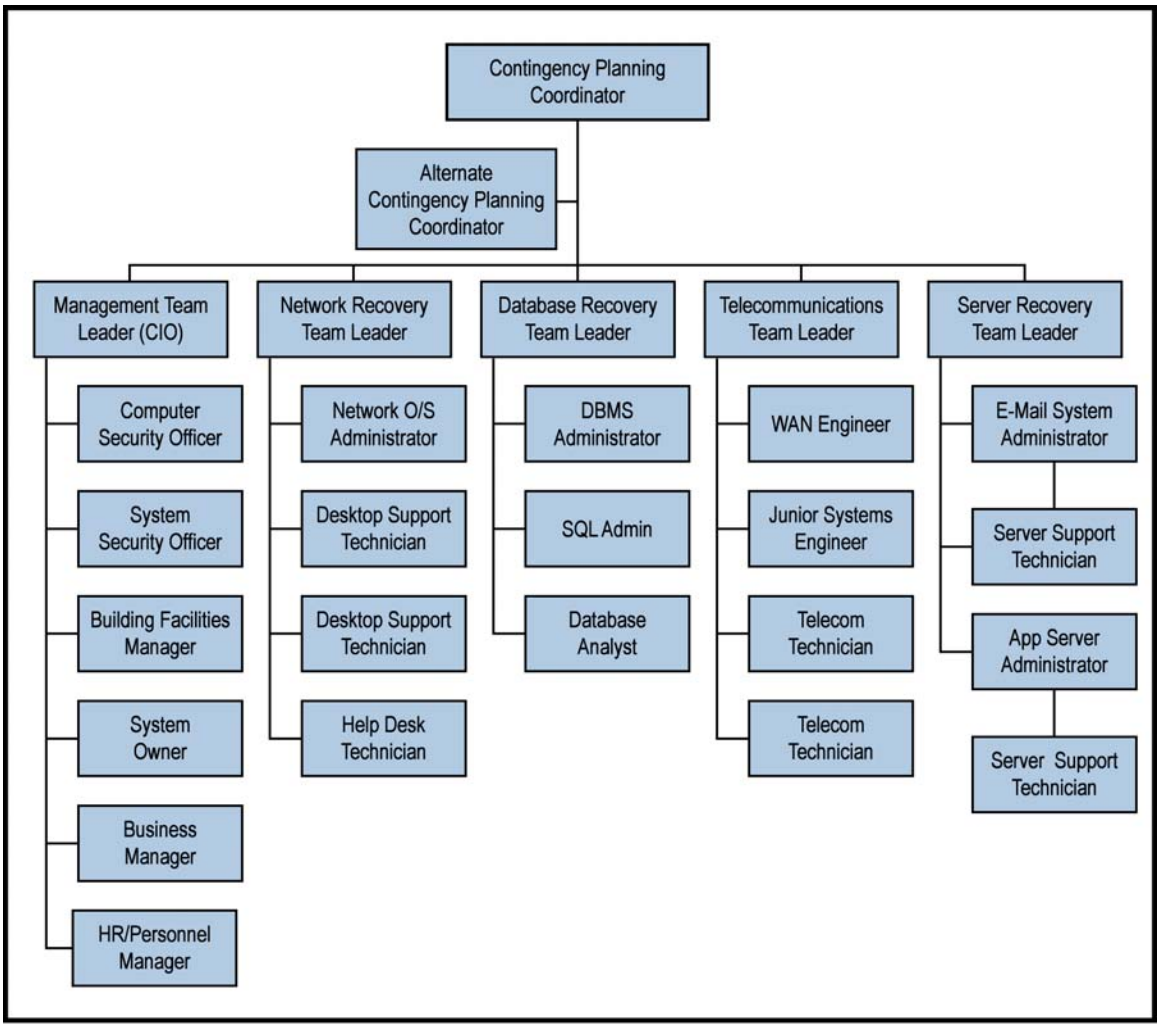


Figure 4-1. Example of a Call Tree

Each position in the call tree will be linked (either within the tree itself or as an attachment) to an individual record containing all pertinent contact information for person, as shown in *Figure 4-2*.

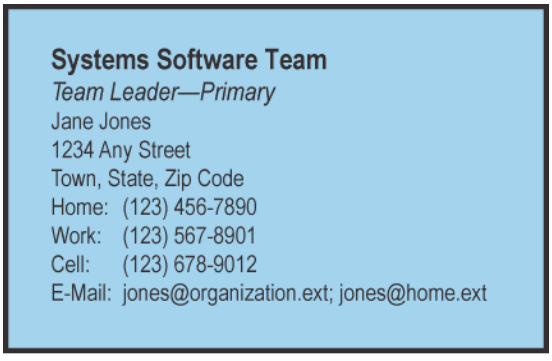


Figure 4-2. Contact Information Reference

External organizations, such as vendors or those with interconnected systems, must also be included in the call tree and notified during this step.

The notification strategy will include the type of information to provide to each person on the call tree. Information can include:

- Nature of the incident that has occurred or will occur;
- Loss of life or injuries;
- Known damage estimates;
- Response and recovery details;
- Where and when to convene for briefing; and
- Instructions to prepare for relocation.

4.2.2 Damage Assessment

As discussed in *Section 2.4*, a damage assessment team will be part of the overall recovery strategy. This team's main responsibility is to perform the damage assessment as soon as possible after the event has occurred. Damage Assessment Team members must be the first staff notified and must include staff in the closest physical proximity to the main processing site where the event would have occurred.

All systems may have different requirements for the damage assessment. The following areas are some examples of what could be addressed by the damage assessment team:

- Cause of the emergency or disruption;
- Potential and additional disruptions or damage;
- Area affected by the emergency;
- Status of the physical infrastructure (structural integrity, telecommunications, power, ventilation, heating, air-conditioning);
- Inventory and functional status of IT equipment;
- Type of damage to IT equipment and data;
- Items to be replaced; and
- Estimated time to restoration of normal services.

4.2.3 Plan Activation

During this phase, the CPC will analyze the results of the damage assessment and determine whether the criteria for plan activation are met. The criteria will be defined and documented based on system-specific requirements and may include:

- Safety of personnel;
- Extent of damage to the facility;
- Extent of damage to the system;
- Criticality of the system (mission critical, important, or supportive); and
- Anticipated duration of the disruption.

If the criteria have been met, the CPC will activate the plan to the extent necessary. Different events may require the plan to be activated to different levels, or only portions of the plan to be activated. For example, a loss of data might require the recovery of backup tapes, but the destruction of the area surrounding the facility might require a move to the alternate processing

location. The recovery teams needed to execute the plan after activation must be notified accordingly.

4.3 Recovery Phase

Recovery phase activities focus on contingency measures to execute temporary IT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery Phase, the IT system will be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing[5], recovery and operation on an alternate system, or relocation and recovery at an alternate site.

4.3.1 Sequence of Recovery Activities

The sequence of activities in the recovery phase must follow the sequence defined in the IT Contingency Plan, based on the BIA. Procedures for recovery must be documented in a detailed manner with step-by-step instructions.

It is vital that during the recovery phase all teams are kept informed of the status of operations. The Contingency Plan must include instructions as to how each team is to coordinate with other teams. Teams are to be notified when:

- An action is not completed within the expected time frame;
- A key step is complete;
- Item(s) must be procured; and
- Any other system-specific concerns are raised.

In addition to detailed recovery procedures, the Contingency Plan will also include instructions and lists of needed equipment, directions to the off site locations, and how to ship or receive materials.

4.3.2 Recovery Procedures

Recovery procedures must be detailed and written in an easy-to-understand manner to facilitate a quick and efficient recovery. While writing procedures, nothing should be assumed or omitted. Any format for the procedures can be used as long as it is clear, concise, and detailed. A checklist format or flowchart fulfills these requirements. *Figure 4-3* below provides a flowchart example of a recovery procedure.

[5] *As stated in OMB A-130, manual procedures are generally NOT a viable backup option. Managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure.*

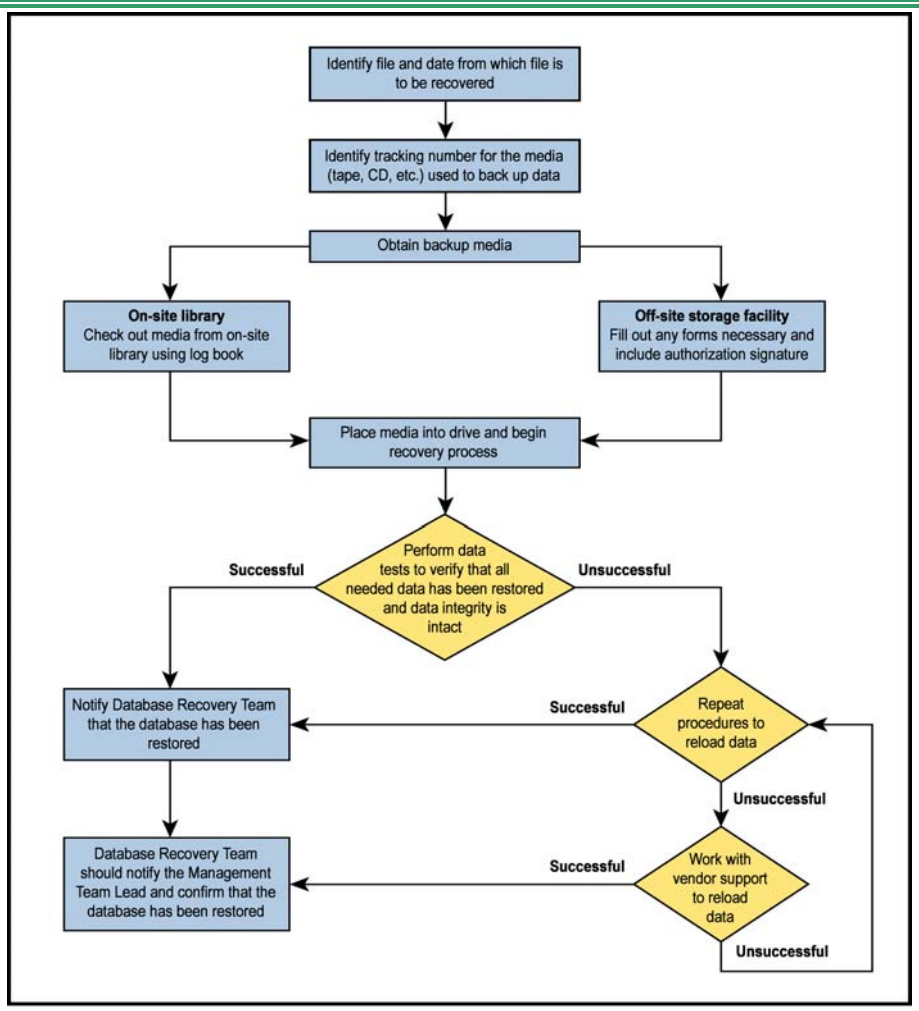


Figure 4-3: Example of a Recovery Procedure

4.4 Reconstitution Phase

In the Reconstitution Phase, recovery activities are terminated and normal operations are transferred back to the organization's facility. Until the primary system is restored and tested, the contingency system will continue to be operated.

Teams will be designated to specifically assist in reconstitution activities that may be occurring at the same time as recovery procedures at an alternate site. The potential for recovery and reconstitution activities to overlap should be considered when planning the number of teams and personnel required.

The following are some of the major activities that may occur during the reconstitution phase:

- Ensuring adequate infrastructure support (electric, water, and telecommunications);
- Installing system hardware, software, and firmware;
- Establishing connectivity and interfaces with network components and external systems;
- Testing system operations to ensure full functionality;
- Backing up operational data on the contingency system and uploading to restored system;
- Terminating contingency operations;

- Shutting down contingency system;
- Removing and/or relocating all sensitive materials at the contingency site; and
- Arranging for recovery personnel to return to the original facility.

Procedures for reconstitution activities must be detailed, descriptive, and easy to follow. The same consideration should be taken with reconstitution procedures that are taken for recovery procedures. While writing procedures, nothing will be assumed or omitted. Any format for the procedure can be used as long as it is clear, concise, and detailed. A checklist format fulfills these requirements.

4.5 Plan Appendices

Appendices to the Contingency Plan will provide specific contact information for staff and vendors, alternate site information, BIA documentation, and acronyms used in the plan.

Appendix A. Acronym List

BIA	Business Impact Analysis
BLSR	Baseline Security Requirements
BRP	Business Resumption Plan
C&A	Certification and Accreditation
COOP	Continuity of Operations
COS	Continuity of Support
CPC	Contingency Planning Coordinator
DAA	Designated Approving Authority
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards
GSS	General Support System
IATO	Interim Approval to Operate
IT	Information Technology
MA	Major Application
MOA	Memorandum of Agreement
MOU	Memorandum Of Understanding
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OEP	Occupant Evacuation Plan
OMB	Office of Management and Budget
PO	Principal Office
POC	Point of Contact
RA	Risk Assessment
SDLC	System Development Life-Cycle
SLA	Service Level Agreement
SME	Subject Matters Expert
SP	Special Publication
SSO	System Security Officer
SSP	System Security Plan
UPS	Uninterruptible Power Supply

Appendix B. Glossary of Terms and Definitions

Continuity of Support Plan: Continuity of Support Plans are intended to provide guidance for short-term service interruptions (less than 48 hours) that do not require relocation to an alternate processing site. Examples of short-term interruptions that do not require relocation include print server outages or a temporary loss of power. The plan should include any preventive measures for protecting the IT systems as well as procedures for restoring any system disruption.

Disaster Recovery Plan (DRP): DRP identifies recovery procedures in the event of natural or man-made disasters or catastrophes affecting the availability of normal facility for an extended period. Frequently, DRP refers to an IT focused plan designed to restore operations to the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of an IT Contingency Plan; however, the DRP is focused on long-term outages (over 48 hours) that require relocation to an alternate processing site. The DRP does not address minor disruptions that do not require relocation. Generally, a DRP is included as part of the Continuity of Support Plan if it is required based on the system criticality and sensitivity. This plan is tested annually to ensure the continued effectiveness and adequacy of the plan.

General Support System (GSS): An interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network, including smart terminals that support a branch office; an agency-wide backbone; a communications network; a departmental data processing center, including its operating system and utilities; a tactical radio network; or a shared information processing service organization. See the *Handbook for Information Technology General Support Systems and Major Applications Inventory Procedures* for more details.

Major Application (MA): A MA that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of the information in the application. *Note*: All Federal applications require some level of protection, however certain applications—because of the information in them—require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the GSS in which they operate. See the *Handbook for Information Technology General Support Systems and Major Applications Inventory Procedures* for additional details.

Appendix C. Sample Contingency Plan Template

DEPARTMENT OF EDUCATION

Name of Principal Office

Contingency Planning Procedures For Name of

Date

Document Configuration Control

Version	Release Date	Summary of Changes

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Authority

1.2 Purpose

1.3 Scope

1.4 Applicability

1.5 Document Structure

2. IT CONTINGENCY PLANNING CONCEPTS

2.1 Why Develop an IT Contingency Plan?

2.2 When Should a Plan Be Developed?

2.3 How Does the Contingency Plan Feed into the C&A Process?

2.4 Who is Responsible for Developing the IT Contingency Plan?

2.4.1 Contingency Planning Coordinator

2.4.2 Management Team

2.4.3 Coordination of GSS and MA Contingency Plans

2.5 What Are the Different Types of Contingency Plans for IT Systems?

2.5.1 Continuity of Support

2.5.2 Disaster Recovery Plan (DRP)

2.6 How Is the Required Level of Effort for An IT Contingency Plan Determined?

2.6.1 What Type of Contingency Plan is Required for Your IT System?

3. IT CONTINGENCY PLANNING PROCESS

3.1 Review Department IT Contingency Planning Policy

3.2 Conduct Business Impact Analysis (BIA)

3.2.1 Identify Essential IT Resources

3.2.2 Identify Disruption Impacts and Allowable Outage Times

3.2.3 Develop Recovery Priorities

3.3 Identify Preventive Controls

3.4 Develop Recovery Strategies

3.4.1 Backup Methods

3.4.1.1 Off-Site Storage

3.4.2 Alternate Sites

3.4.3 Equipment Replacement

3.4.4 Personnel Roles and Responsibilities

3.5 Develop the Plan

3.6 Plan Testing, Training, and Exercising

3.6.1 Plan Testing

3.6.2 Personnel Training and Exercises

3.7 Plan Maintenance

3.7.1 Distribution of the Plan and Version Control

3.7.2 Supporting Documentation

4. IT Contingency Plan Structure and Development

4.1 Supporting Information

4.1.1 Introduction

4.1.2 Concept of Operations

4.2 Notification/Activation Phase

4.2.1 Notification Procedures

4.2.2 Damage Assessment

4.2.3 Plan Activation

4.3 Recovery Phase

4.3.1 Sequence of Recovery Activities

4.3.2 Recovery Procedures

4.4 Reconstitution Phase

4.5 Plan Appendices

Appendix D. References

Handbook for Information Assurance Security Policy

Handbook for Information Technology Certification and Accreditation Procedures (to be updated).

Handbook for Information Technology General Support Systems and Major Applications Inventory Procedures

Information Technology Security System Development Lifecycle Guide

Information Assurance Program Management Plan (IAPMP)

Information Technology Security Compliance Guide

NIST SP 800-26 National Institute of Standards and Technology (NIST), Security Self-Assessment Guide for Information Technology Systems, November 2001 (http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf)

NIST SP 800-34 National Institute of Standards and Technology (NIST), Contingency Planning Guide for Information Technology Systems, June 2002 **(**http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf)

NIST SP 800-53 National Institute of Standards and Technology (NIST), Recommended Security Controls for Federal Information Systems, February 2005 (http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf)

OMB A-130 Office of Management and Budget (OMB) Management of Federal Information Resources Circular A-130, Appendix III, November 2000 (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)