

Information Technology Contingency Planning Guide Draft Release

October 1, 2001

CONTRACT NUMBER SPO 700-98-D-4002, DO 86



IATAC

Information Assurance Technology Analysis Center (IATAC)
3190 Fairview Park Drive • Falls Church, VA 22042

Distribution A

Approved for public release, distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No.
0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

| | | | | | |
|---|--|-----------------------------------|---|---|--|
| 1. REPORT DATE (DD-MM-YYYY) 01-10-2001 | | 2. REPORT TYPE | | 3. DATES COVERED (FROM - TO) xx-xx-2001 to xx-xx-2001 | |
| 4. TITLE AND SUBTITLE Information Technology Contingency Planning Guide (Draft) Unclassified | | | 5a. CONTRACT NUMBER | | |
| | | | 5b. GRANT NUMBER | | |
| | | | 5c. PROGRAM ELEMENT NUMBER | | |
| 6. AUTHOR(S) | | | 5d. PROJECT NUMBER | | |
| | | | 5e. TASK NUMBER | | |
| | | | 5f. WORK UNIT NUMBER | | |
| 7. PERFORMING ORGANIZATION NAME AND ADDRESS Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA22102 | | | 8. PERFORMING ORGANIZATION REPORT NUMBER | | |
| 9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS National Institute of Standards and Technology , | | | 10. SPONSOR/MONITOR'S ACRONYM(S) | | |
| | | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) | | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT APUBLIC RELEASE | | | | | |
| 13. SUPPLEMENTARY NOTES Per conversation with Abe Usher, IATAC, performing organization is Booz Allen & Hamilton. | | | | | |
| 14. ABSTRACT See report. | | | | | |
| 15. SUBJECT TERMS IATAC COLLECTION | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19. NAME OF RESPONSIBLE PERSON | |
| | | Same as Report (SAR) | 88 | EM145, (blank) lfenster@dtic.mil | |
| a. REPORT Unclassified | | b. ABSTRACT Unclassified | c. THIS PAGE Unclassified | 19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007 | |
| | | | | Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39.18 | |

REPORT DOCUMENTATION PAGEForm Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

| | | | | |
|--|---|--|---|--|
| 1. AGENCY USE ONLY (Leave blank) | | 2. REPORT DATE 10/1/01 | 3. REPORT TYPE AND DATES COVERED Report 10/1/01 | |
| 4. TITLE AND SUBTITLE Information Technology Contingency Planning Guide (Draft) | | | 5. FUNDING NUMBERS | |
| 6. AUTHOR(S) | | | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102 | | | 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Institute of Standards and Technology | | | 10. SPONSORING / MONITORING AGENCY REPORT NUMBER | |
| 11. SUPPLEMENTARY NOTES | | | | |
| 12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution is unlimited | | | 12b. DISTRIBUTION CODE A | |
| 13. ABSTRACT (Maximum 200 Words) Information technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems be able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures to enable a system to be recovered quickly and effectively following a service disruption or disaster. | | | | |
| 14. SUBJECT TERMS IATAC Collection, information technology | | | 15. NUMBER OF PAGES 86 | |
| | | | 16. PRICE CODE | |
| 17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED | 18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED | 19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED | 20. LIMITATION OF ABSTRACT UNLIMITED | |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

Information Technology Contingency Planning Guide



TABLE OF CONTENTS

| | |
|---|-----------|
| 1. INTRODUCTION | 1 |
| 1.1 AUTHORITY | 1 |
| 1.2 PURPOSE | 2 |
| 1.3 SCOPE | 3 |
| 1.4 AUDIENCE | 4 |
| 1.5 DOCUMENT STRUCTURE | 4 |
| 2. BACKGROUND | 6 |
| 2.1 CONTINGENCY PLANNING AND THE RISK MANAGEMENT PROGRAM | 6 |
| 2.2 TYPES OF PLANS | 8 |
| 2.3 CONTINGENCY PLANNING AND THE COMPUTER SYSTEM LIFE CYCLE | 10 |
| 3. IT CONTINGENCY PLANNING PROCESS | 13 |
| 3.1 DEVELOP THE CONTINGENCY PLANNING POLICY | 13 |
| 3.2 CONDUCT BUSINESS IMPACT ANALYSIS | 14 |
| 3.2.1 <i>Identify Critical IT Resources</i> | 15 |
| 3.2.2 <i>Identify Outage Impacts and Allowable Outage Times</i> | 15 |
| 3.2.3 <i>Develop Recovery Priorities</i> | 16 |
| 3.3 IDENTIFY PREVENTIVE CONTROLS | 16 |
| 3.4 DEVELOP RECOVERY STRATEGIES | 17 |
| 3.4.1 <i>Backup Methods</i> | 17 |
| 3.4.2 <i>Equipment Replacement</i> | 18 |
| 3.4.3 <i>Alternate Sites</i> | 19 |
| 3.4.4 <i>Roles and Responsibilities</i> | 21 |
| 3.4.5 <i>Cost Considerations</i> | 22 |
| 3.5 TESTING, TRAINING, AND EXERCISES | 23 |
| 3.6 PLAN MAINTENANCE | 23 |
| 4. IT CONTINGENCY PLAN DEVELOPMENT | 26 |
| 4.1 SUPPORTING INFORMATION | 27 |
| 4.2 NOTIFICATION / ACTIVATION PHASE | 28 |
| 4.2.1 <i>Notification Procedures</i> | 28 |
| 4.2.2 <i>Damage Assessment</i> | 30 |
| 4.2.3 <i>Plan Activation</i> | 30 |
| 4.3 RECOVERY PHASE | 31 |
| 4.3.1 <i>Sequence of Recovery Activities</i> | 31 |
| 4.3.2 <i>Recovery Procedures</i> | 32 |
| 4.4 RECONSTITUTION PHASE | 32 |
| 4.5 PLAN APPENDIXES | 33 |
| 5. TECHNICAL CONTINGENCY PLANNING CONSIDERATIONS | 34 |
| 5.1 DESKTOP COMPUTERS AND PORTABLE SYSTEMS | 34 |
| 5.1.1 <i>Contingency Considerations</i> | 36 |
| 5.1.2 <i>Contingency Solutions</i> | 36 |
| 5.2 SERVERS | 40 |
| 5.2.1 <i>Contingency Considerations</i> | 40 |
| 5.2.2 <i>Contingency Solutions</i> | 40 |
| 5.3 WEB SITES | 47 |
| 5.3.1 <i>Contingency Considerations</i> | 47 |
| 5.3.2 <i>Contingency Solutions</i> | 48 |
| 5.4 LOCAL AREA NETWORKS | 49 |
| 5.4.1 <i>Contingency Considerations</i> | 51 |

| | | |
|---|---------------------------------|-----------|
| 5.4.2 | Contingency Solutions..... | 51 |
| 5.5 | WIDE AREA NETWORKS..... | 53 |
| 5.5.1 | Contingency Considerations..... | 54 |
| 5.5.2 | Contingency Solutions..... | 55 |
| 5.6 | DISTRIBUTED SYSTEM..... | 56 |
| 5.6.1 | Contingency Considerations..... | 56 |
| 5.6.2 | Contingency Solutions..... | 56 |
| 5.7 | MAINFRAME SYSTEMS..... | 58 |
| 5.7.1 | Contingency Considerations..... | 58 |
| 5.7.2 | Contingency Solutions..... | 58 |
| 6. | SUMMARY | 60 |
| APPENDIX A: SAMPLE IT CONTINGENCY PLAN FORMAT | | 1 |
| APPENDIX B: SAMPLE BUSINESS IMPACT ANALYSIS AND BIA TEMPLATE | | 1 |
| APPENDIX C: GLOSSARY..... | | 1 |
| APPENDIX D: REFERENCES | | 1 |

LIST OF FIGURES

| | | |
|-------------|--|----|
| Figure 2-1: | Contingency Planning an Element of Risk Management | 6 |
| Figure 2-2: | Contingency Planning-Risk Assessment Relationship | 8 |
| Figure 2-3: | Computer System Life Cycle | 11 |
| Figure 3-1: | Contingency Planning Process | 13 |
| Figure 3-2: | Business Impact Analysis Process | 15 |
| Figure 4-1: | Contingency Plan Structure | 26 |
| Figure 4-2: | Sample Call Tree..... | 29 |
| Figure 5-1: | Server Contingency Solutions and Availability..... | 41 |
| Figure 5-2: | Local Area Network..... | 51 |
| Figure 5-3: | WAN Diagram | 54 |

LIST OF TABLES

| | | |
|------------|--|----|
| Table 2-1: | Types of Contingency-Related Plans | 10 |
| Table 3-1: | Alternate Site Criteria Selection..... | 20 |
| Table 3-2: | Recovery Strategy Budget Planning Template | 22 |
| Table 3-3: | Sample Record of Changes | 24 |
| Table 5-1: | LAN Topologies | 49 |

1. INTRODUCTION

Information technology (IT) and automated information systems are vital elements in most business processes. Because these IT resources are so essential to an organization's success, it is critical that the services provided by these systems be able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans and procedures and technical measures to enable a system to be recovered quickly and effectively following a service disruption or disaster.

IT Contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. Contingency planning generally includes one or more of the approaches to restore disrupted IT services:

- Restoring IT operations at an alternate location
- Recovering IT operations using alternate equipment
- Performing some or all of the affected business processes using non-IT (manual) means (typically acceptable only for short-term disruptions)

This document provides guidance to individuals responsible for preparing and maintaining IT contingency plans. The document discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of IT systems, and provides examples to assist readers in developing their own IT contingency plans.

1.1 Authority

This IT Contingency Planning Guide has been developed by the National Institute of Standards and Technology (NIST) in compliance with its statutory responsibility to provide federal computer security standards guidance in accordance with the Computer Security Act of 1987.

Information in this guide is consistent with guidance provided in other NIST documents, including Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, Chapter 11, *Preparing for Contingencies and Disasters*. The guidance proposed within is also consistent with federal mandates affecting contingency, continuity of operations, and disaster recovery planning, including—

- The Computer Security Act of 1987
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, November 2000.
- Federal Information Processing Standards Publication (FIPS PUB) 87, *Guidelines for ADP Contingency Planning*, March 1981
- Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations*, July 1999

- Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operations*, October 1998
- PDD 63, *Critical Infrastructure Protection*, May 1998
- The Federal Response Plan (FRP), April 1999.

Federal Departments and Agencies may be subject to complying with the above federal policies in addition to internal departmental policies. This guidance document presents a methodology and understanding of how to prepare contingency plans for federal computer systems;¹ however, the methodologies are nonbinding and serve only to present a best practice at the current time. It is not subject to copyright.

IT System:

A system is identified by defining boundaries around a set of processes, communications, storage, and related resources (an architecture).

All components of a system need not be physically connected (e.g., [1] a group of stand-alone personal computers (PC) in an office; [2] a group of PCs placed in employees' homes under defined telecommuting program rules; [3] a group of portable PCs provided to employees who require mobile computing capability for their jobs; and [4] a system with multiple identical configurations that are installed in locations with the same environmental and physical safeguards.

** As defined in SP-800-18, Guide for Developing Security Plans for Information Technology Systems*

Nongovernment entities may apply these guidelines to their IT contingency planning efforts on a voluntary basis.

Methodologies presented in this document should not be interpreted to contradict standards and guidelines made mandatory and binding upon federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the Office of Management and Budget, or any other federal official.

1.2 Purpose

This IT Contingency Planning Guide identifies fundamental planning principles and best practices to help personnel develop and maintain effective IT contingency plans. The principles within are developed to meet most organizational needs and recognize that each organization may have additional requirements specific to their own processes. The document provides guidance to help personnel evaluate information systems and operations to determine contingency requirements and priorities. This guidance also provides a structured approach to aid planners in developing cost-effective solutions that accurately reflect their IT requirements and integrate contingency planning principles into all aspects of IT operations.

¹ The Computer Security Act of 1987 defines a Federal computer system as one which is, “operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and (B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949.”

The guidance presented within should be considered by planners throughout the planning life cycle, from the conceptualization of contingency planning efforts through maintenance and disposal. If used as a planning management tool throughout the process, this document and its appendixes should provide users with time- and cost-saving practices.

1.3 Scope

This document is published by NIST as recommended guidance for federal departments and agencies. The document presents contingency planning principles for the following common IT processing systems:

- Desktop computers and portable systems (laptop and handheld computers)
- Servers
- Web sites
- Local area networks (LAN)
- Wide area networks (WAN)
- Distributed systems
- Mainframe systems.

Contingency planning for supercomputers and wireless networks is not covered in this document, although many of the principles presented here may be applied to these systems.

To assist personnel responsible for developing contingency plans, this document discusses common technologies that may be used to support contingency capabilities. However, given the broad range of IT designs and configurations, as well as the rapid development and obsolescence of new products and capabilities, the scope of this discussion is not intended to be comprehensive. Rather, the document describes best practices for applying technology to enhance an organization's IT contingency planning capabilities.

The document outlines planning principles that may be applied to a wide variety of incidents that could affect IT system operations. The scope includes minor incidents causing short-term disruptions to disasters that affect normal operations for an extended period. Because IT systems vary in design and application, specific incident types and associated contingency measures are not provided in this document. Instead, the planning guide defines a process that may be followed for any system to identify planning requirements and develop an effective contingency plan.

This planning guide does not address facility-level or organizational contingency planning, except for those issues required to restore information systems and their processing capabilities. In addition, this document does not address contingency planning for business processes. Although information systems typically support business processes, the processes also depend on a variety of other resources and capabilities not associated with information systems.

1.4 Audience

The principles presented in this document will be used by all levels of management within federal organizations who are responsible for IT security at system and operational levels. This description includes the following personnel:

- **Managers** responsible for overseeing IT operations or business processes that rely on IT systems
- **System administrators** responsible for maintaining daily IT operations
- **Information System Security Officers (ISSO)** and other staff responsible for developing, implementing, and maintaining an organization's IT risk management activities
- **System engineers and architects** responsible for designing, implementing, or modifying information systems
- **Users** who employ desktop and portable systems to perform their assigned job functions
- **Other personnel** responsible for designing, managing, operating, maintaining, or using information systems.

In addition, this document may be used by emergency management personnel who may need to coordinate facility-level contingency or continuity plans with IT contingency planning activities. The concepts presented in this document are not specific to government systems and may be used by private and commercial organizations.

1.5 Document Structure

This document is designed to chronologically lead the reader through the process of designing an IT contingency planning program applicable to a wide range of organizations, evaluating the organization's needs against recovery strategy options and technical considerations, and documenting the strategy into an IT contingency plan. The contingency plan would serve as a "user's manual" for executing the strategy in the event of a disruption. Where possible, examples or hypothetical situations are included to provide greater understanding.

The remaining sections of this document address the following areas of contingency planning:

- **Section 2** provides background information on contingency planning, including the purpose of contingency plans, contingency plan types, and how these plans are integrated into an organization's risk and system life-cycle management programs.
- **Section 3** details the fundamental planning principles necessary for developing an effective contingency capability. The principles outlined in this section are universal to all IT systems. This section presents contingency planning guidance for all elements of the planning cycle, including preliminary actions, business impact analysis, alternate site selection, and recovery strategies. The section also discusses the development of contingency teams and the roles and responsibilities commonly assigned to team personnel.

- **Section 4** breaks down the activities necessary to document the contingency strategy. This documentation becomes the IT contingency plan. Maintenance, testing, training and exercising the contingency plan are also discussed in this section.
- **Section 5** describes contingency planning considerations specific to the IT systems listed in the Scope section above. This section is intended to help contingency planners identify, select, and implement the appropriate technical contingency measures for their given systems.
- **Section 6** summarizes the main concepts presented in the document, reiterating the importance of comprehensive, effective contingency planning.

This document also includes four appendixes. Appendix A provides a sample IT contingency plan format. Appendix B provides a sample business impact analysis template. Appendixes C and D provide a glossary of terms and a list of references, respectively.

2. BACKGROUND

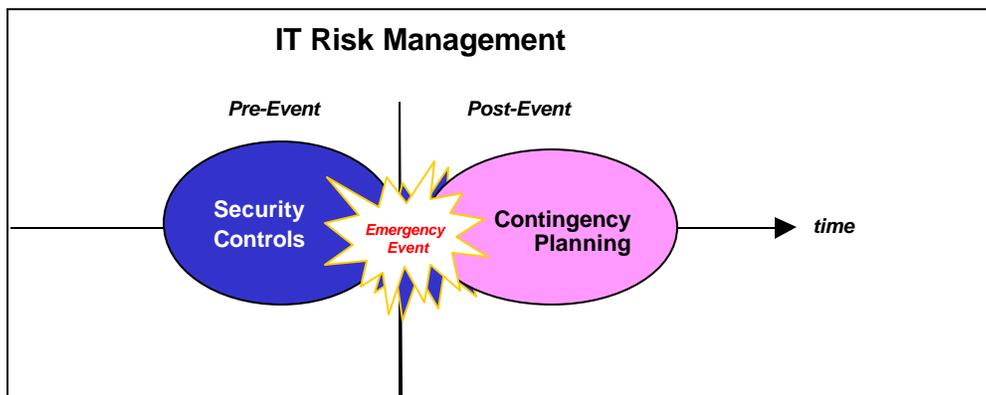
IT systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage, disk drive failure) to severe (e.g., equipment destruction, fire). Many vulnerabilities may be eliminated through procedural or technical solutions as part of the organization's risk management or security controls; however, typically it is impossible to completely eliminate all risks.² Contingency planning is designed to complement these risk management and security activities by focusing recovery solutions on residual risks. As a result, contingency planning can provide a cost-effective means to ensure that essential IT services can be recovered quickly after an emergency.

This section discusses the ways in which contingency planning fits into an organization's larger risk management, security, and emergency preparedness programs. The section describes other types of emergency-related plans and relates them to contingency planning. The section also describes how contingency planning principles may be integrated throughout the system life cycle to increase an organization's ability to respond quickly and effectively to a disruptive event.

2.1 Contingency Planning and the Risk Management Program

Risk management encompasses a broad range of activities to identify, control, and mitigate IT-related risks. Risk management activities may be considered to have two primary functions. First, risk management should prevent or reduce the likelihood of damaging incidents by reducing or eliminating risks. These preventive measures typically form the security controls that protect a system against natural, human, and technological threats. Second, risk management also should encompass actions to reduce or limit the consequences of threats that successfully disrupt a system. These "post-event" measures form the basis for contingency planning. Figure 2-1 illustrates the relationship between preemptive security controls and post-event contingency planning.

Figure 2-1: Contingency Planning an Element of Risk Management



² For example, in many cases, critical resources may reside outside the organization's control (such as electric power or telecommunications), and the organization may be unable to ensure their availability.

Risks result from a variety of factors, although typically they are classified in three types:

- **Natural**—e.g., hurricane, tornado, flood, fire
- **Human**³—e.g., operator error, sabotage, malicious code
- **Technological**—e.g., equipment failure, software error, telecommunications network outage, electric power failure.

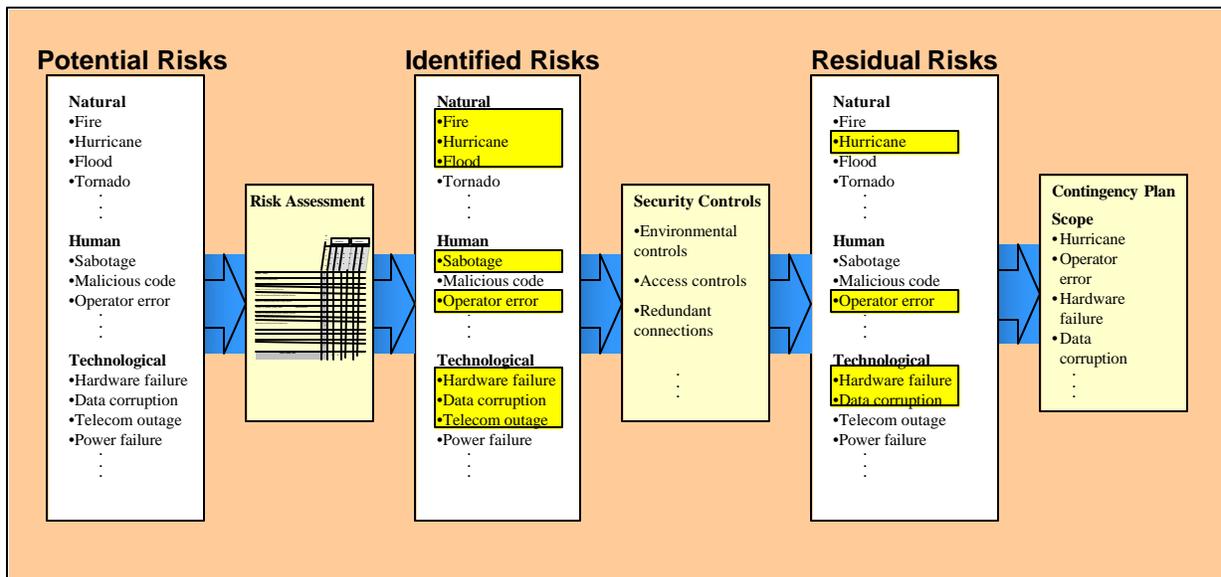
Not all risks are present with respect to a given IT system. For example, depending on its location, a system may have no risk of damage by hurricane, but reasonably high risk of effects from a tornado. To determine effectively the specific risks to a system, a risk assessment is required. A thorough risk assessment should identify all system risks and attempt to determine the likelihood of the risk actually occurring. The risk assessment is critical because it enables the system manager to focus risk management efforts and resources in a prioritized manner only on identified risks.⁴

Ideally, the system manager would be able to eliminate identified risks completely. However, rarely is this possible or cost effective. Rather, the manager will attempt to reduce risks to an acceptable level and remain aware of residual risks. Because these residual risks represent the complete set of situations that could affect system performance, the system manager may reduce the scope of contingency plan to address only this reduced risk set. As a result, the contingency plan can be more narrowly focused, conserving agency resources while ensuring an effective system recovery capability. Figure 2-2 shows this critical risk assessment-contingency plan relationship.

³ Responses to cyber attacks (denial of service, viruses, etc.) are not covered in this document. Responses to these types of incidents involve network security activities outside the scope of contingency planning. Similarly, this document does not address incident response activities associated with preserving evidence for computer forensics analysis following an illegal intrusion, denial of service attack, introduction of malicious logic, or other cyber crime.

⁴ NIST SP-800-30, *Risk Management Guide for Information Technology Systems*, provides information on how to conduct risk assessments.

Figure 2-2: Contingency Planning-Risk Assessment Relationship



Because risks can vary over time, and new risks may replace old ones as a system evolves, the risk management process must be ongoing and dynamic. The IT system manager must be aware of risks to the system and recognize whether the current contingency plan is able to address residual risks completely and effectively. As described in Section 3.6, the shifting risk spectrum necessitates regular contingency plan maintenance and testing.

2.2 Types of Plans

IT contingency planning represents a broad scope of activities designed to sustain or recover critical IT services following an emergency. As such, IT contingency planning fits into a much broader emergency preparedness environment that also includes organizational and business process continuity and recovery planning. In general, universally accepted definitions for contingency planning and these related planning areas have not been available. In some cases, this has led to confusion regarding the actual scope and purpose of various plan types. To provide a common basis of understanding regarding IT contingency planning, this section identifies several other plan types and describes their purpose and scope relative to IT contingency planning. Because of the lack of standard definitions for these plan types, in some cases, actual plans may vary from the descriptions below. However, when these plans are discussed in this document, the following descriptions will apply.

Continuity of Operations Plan (COOP). The COOP⁵ focuses on restoring an *organization's* (usually a headquarters element) essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. The Federal Emergency Management Agency (FEMA), which is the government's executive agent for COOP, provides COOP guidance in FPC 65, *Federal Executive Branch Continuity of Operations*. Standard elements of a COOP include Delegation of Authority statements, Orders of Succession, and Vital

⁵ Some organizations use COOP to indicate Continuity of Operations, rather than Continuity of Operations Plan.

Records and Databases. Because the COOP emphasizes the recovery of an organization's operational capability at an alternate site, the plan does not necessarily include IT operations. In addition, the COOP typically does not address minor disruptions that do not require relocation to an alternate site.

Disaster Recovery Plan (DRP). As suggested by its name, the DRP applies 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 an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation.

Business Continuity Plan (BCP). The BCP focuses on sustaining an organization's *business functions* during and after a disruption. A BCP may be written for a specific business process or may address all key business processes. Information systems are considered in the BCP only in terms of their support to the larger business process(es). In some cases, the BCP may not address long-term recovery of processes and return to normal operations, solely covering interim business continuity requirements.

Business Recovery Plan (BRP), also Business Resumption Plan. The BRP addresses the restoration of business processes after an emergency. The BRP is similar to the BCP, but unlike that plan, the BRP typically lacks procedures to ensure continuity of critical processes throughout an emergency or disruption.

Continuity of Support Plan. OMB Circular A-130, Appendix III requires the development and maintenance of continuity of support plans for general support systems and contingency plans for major applications. This planning guide considers continuity of support planning to be synonymous with IT contingency planning. OMB Circular A-130 does not provide a template or format for continuity of support plans.

Incident Response Plan. The Incident Response Plan establishes procedures to address cyber attacks against an organization's IT system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware or software (e.g., malicious logic such as a virus, worm or Trojan Horse).

Table 2-1 summarizes the plan types discussed above.

Table 2-1: Types of Contingency-Related Plans

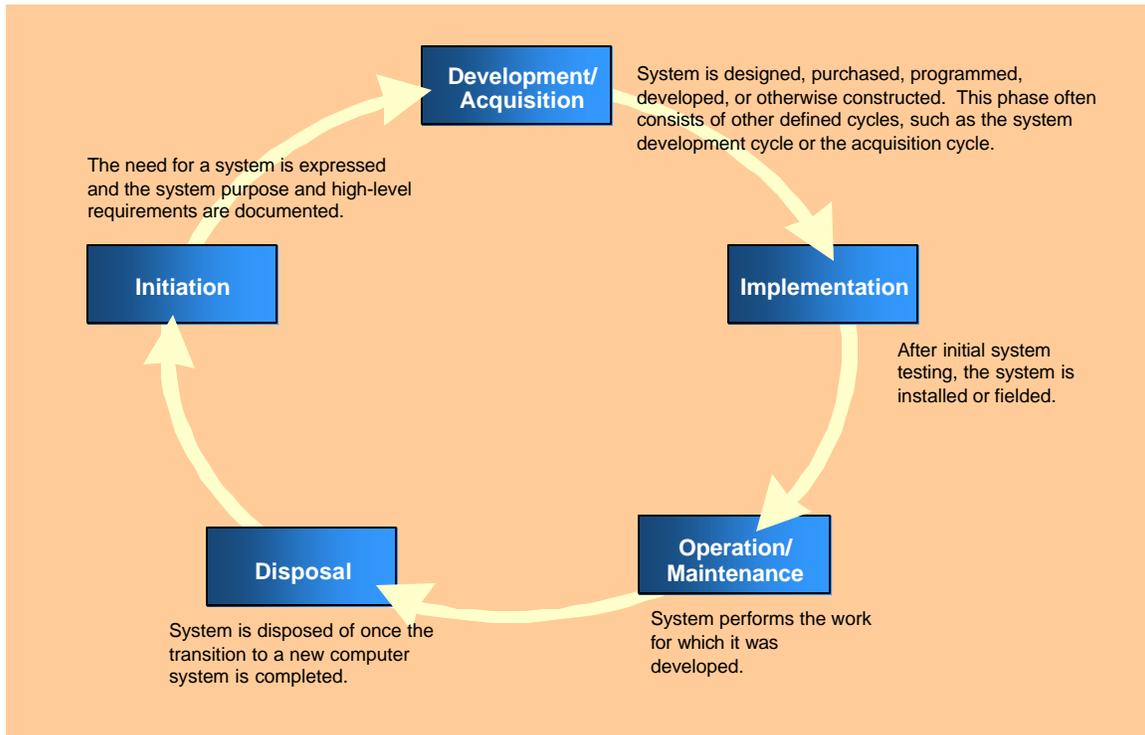
| Plan | Purpose | Scope |
|--|--|---|
| Continuity of Operations (COOP) | Establish procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days | Addresses the subset of an organization's missions that are deemed most critical; usually written at headquarters level; not IT-focused |
| Disaster Recovery Plan (DRP) | Provide detailed procedures to facilitate recovery of capabilities at an alternate site data | Often IT-focused; limited to major disruptions with long-term effects |
| Business Continuity Plan (BCP) | Provide procedures for sustaining essential business operations while recovering from a significant disruption | Addresses business processes; not IT-focused; IT addressed only based on its support for business process |
| Business Recovery (or Resumption) Plan (BRP) | Provide procedures for recovering business operations immediately following a disaster | Addresses business processes; not IT-focused; IT addressed based only on its support for business process |
| Continuity of Support Plan | Establish procedures and capabilities for recovering a general support system | Same as IT contingency plan |
| Incident Response Plan | Define strategies to detect, respond to, and limit consequences of malicious cyber incident | Focuses on information security responses to incidents affecting systems and/or networks |

2.3 Contingency Planning and the Computer System Life Cycle

The computer system life cycle refers to the full scope of activities associated with a system during its life span. The life cycle, depicted in Figure 2-3, begins with project initiation and ends with system disposal.⁶ Although contingency planning is associated with activities occurring in the operation/maintenance phase, contingency measures should be identified and integrated at all phases of the computer system life cycle. This approach reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is implemented. This section discusses common ways in which contingency strategies can be incorporated throughout the computer system life cycle.

⁶ There are several models of the computer system life cycle. The model used for the this document is consistent with NIST Special Publication 800-12, Chapter 8, *An Introduction to Computer Security: The NIST Handbook*.

Figure 2-3: Computer System Life Cycle



Initiation. Contingency planning requirements should be considered when a new IT system is being conceived. In this first phase, Initiation, as system requirements are identified and matched to their related operational processes, initial contingency requirements may become apparent. Very high system availability requirements may indicate that redundant, real-time mirroring and fail-over capabilities should be built into the system design. Similarly, if the system is intended to operate in unusual conditions, such as in a mobile application or an inaccessible location, the design may need to include additional features, such as remote diagnostic or self-healing capabilities.

Development / Acquisition. As initial concepts evolve into system designs, specific contingency solutions may be incorporated. As in the Initiation Phase, contingency measures included in this phase should reflect system and operational requirements. The design should incorporate redundancy and robustness directly into the system architecture to optimize reliability, maintainability, and availability during the Operation/Maintenance Phase. By including them in the initial design, costs are reduced, and problems associated with retrofitting or modifying the system during the Operation/Maintenance Phase are reduced. Examples of contingency measures that should be considered in this phase are, redundant communications paths, lack of single points of failure, enhanced fault tolerance of network components and interfaces, power management systems with appropriately sized backup power sources, load balancing, and data mirroring and replication to ensure a uniformly robust system.

Implementation. While the system is undergoing initial testing, contingency strategies also should be tested to ensure that technical features, and recovery procedures are accurate and

effective. When these contingency measures have been verified, they should be clearly documented in the contingency plan.

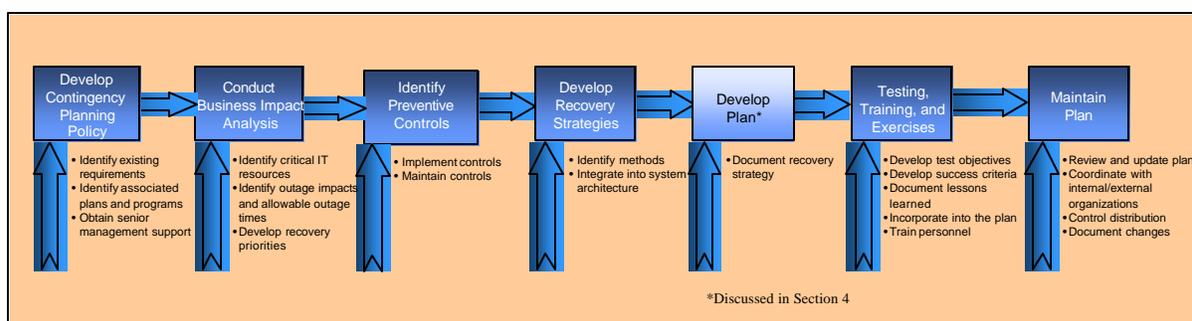
Operation/Maintenance. When the system is operational, users, administrators, and managers should maintain training and awareness of the contingency plan procedures. Exercises and tests should be conducted to continue to ensure the procedures are effective. The plan should be updated to reflect changes to procedures based on lessons learned. When the IT system undergoes upgrades or any other modifications, such as changes to external interfaces, these modifications should be reflected in the contingency plan. Coordinating and documenting changes in the plan should be performed in a timely manner to maintain an effective plan.

Disposal. Contingency considerations should not be neglected because a computer system is retired and another system replaces it. Until the new system is operational and fully tested (including its contingency capabilities), the original system's contingency plan should be ready for implementation. As legacy systems are replaced, they may provide a valuable backup capability if a loss or failure of the new system should occur. Also, in some cases, equipment parts, such as hard drives, power supplies, memory chips, or network cards from hardware that has been replaced by new systems can be used as spare parts for new, operational equipment. In addition legacy systems can be used as test systems for new applications, allowing potentially disruptive system flaws to be identified and corrected on nonoperational systems.

3. IT CONTINGENCY PLANNING PROCESS

This section describes the process to develop and maintain an effective IT contingency plan. The process presented here is common to all IT systems. The 7 process steps include developing the contingency planning policy, conducting the BIA, identifying preventive controls, developing effective recovery strategies, developing the contingency plan, plan testing and training, and plan maintenance. These steps represent key elements in a comprehensive IT contingency planning capability. Six of the 7 process steps are discussed in this section. Because it represents the heart of the contingency planning program, plan development, including the sections that comprise the plan, is addressed in its own section (Section 4). Figure 3-1 illustrates the contingency planning process.

Figure 3-1: Contingency Planning Process



3.1 Develop the Contingency Planning Policy

To be effective and to ensure that personnel understand the agency's contingency planning requirements fully, the contingency plan must be based on a clearly defined policy. The contingency planning policy should define the agency's overall contingency objectives and establish the organizational framework and responsibilities for IT contingency planning. To be successful, a contingency program must be supported by senior personnel, and these personnel should be included in the process to develop the program policy, structure, objectives, and responsibilities. At a minimum, the contingency policy should comply with federal guidance contained in the documents listed in Section 1.1; agencies should evaluate their respective IT systems, operations, and requirements to determine if additional contingency planning requirements are necessary. Key policy elements are as follows:

- Roles and responsibilities
- Plan scope
- Training requirements
- Exercise and testing schedules
- Plan maintenance schedule.

Sample IT Contingency Policy:

The organization shall develop a contingency planning capability to meet the needs of critical IT operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. The plan should assign specific responsibilities to designated staff or positions to facilitate the recovery and/or continuity of essential IT functions. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, the recovery capabilities, and personnel shall be tested at least annually to identify weaknesses of the capability.

As the IT contingency policy and program are developed, they should be coordinated with related agency activities, including IT security, physical security, IT operations, and emergency preparedness functions. IT contingency activities should be compatible with program requirements for these areas, and contingency personnel should coordinate with representatives from each area to remain aware of new or evolving policies, programs, or capabilities. Contingency plans must be written in coordination with other existing plans associated with system. Such plans include the following:

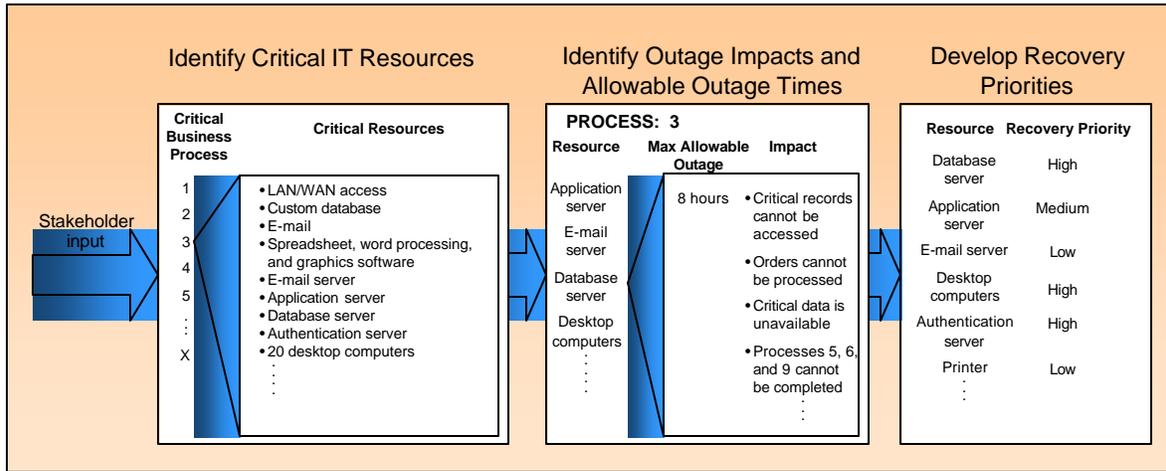
- Security-related plans, such as system security, physical, and personnel security plans
- Facility-level plans, such as the occupant emergency plan and COOP
- Agency-level plans, such as crisis communication, business resumption, and critical infrastructure protection (CIP) plans.

3.2 Conduct Business Impact Analysis

The BIA is a key step in the contingency planning process. The BIA enables the system manager to characterize fully the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities. The sample BIA process outlined in this section, illustrated in Figure 3-2, helps IT system managers streamline and focus their contingency plan development activities to achieve a more effective plan.⁷ An example of the BIA process and a sample BIA template are provided in Appendix B.

⁷ For completeness and to assist system managers who may be new to or unfamiliar with the system, the sample BIA process presented here includes basic steps. The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences if system components were to be disrupted. In many cases, the system manager will be very familiar with specific system components and the ways in which they support business processes. This is especially true with respect to small systems. In these cases, not all BIA steps may be necessary; the system manager may modify the approach to fit the respective system and contingency planning needs.

Figure 3-2: Business Impact Analysis Process



3.2.1 Identify Critical IT Resources

IT systems can be very complex, with numerous components, interfaces, and processes. A system also often has multiple stakeholders with different perspectives on the importance of system services or capabilities.⁸ This first BIA step evaluates the IT system to determine the critical functions performed by the system and then to identify the specific system resources required to perform them. Two activities usually are needed to complete this step:

- The system manager should identify and coordinate with internal and external stakeholders to characterize the ways that these stakeholders depend on or support the IT system. This coordination should enable the system manager to characterize the full range of support provided by the system.
- Next, the system manager evaluates the system to link these critical services to system resources. This analysis usually will identify infrastructure requirements such as electric power, telecommunications connections, and environmental controls. Specific IT equipment, such as routers, application servers, and authentication servers, also are usually considered to be critical. However, the analysis also may determine that certain IT components, such as a printer or print server, are not needed to support critical services.

3.2.2 Identify Outage Impacts and Allowable Outage Times

In this step, the system manager should analyze the critical resources identified in the previous step and determine the impacts on IT operations if a given resource were disrupted or damaged. The analysis should evaluate the impact of the outage in two ways.

- The effects of the outage may be tracked *over time*. This will enable the system manager to identify the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function

⁸ Stakeholders may include customers, business process or application owners, end users, management staff, and other groups.

- The effects of the outage may be tracked *across related or dependent systems*, identifying any cascading effects that may occur as a disrupted system affects other processes that rely on it.

3.2.3 Develop Recovery Priorities.

The outage impacts and allowable outage times characterized in the previous step enable the system manager to develop and prioritize recovery strategies that personnel will implement during contingency plan activation.⁹ For example, if the outage impacts step determines that the system must be recovered within 4 hours, the system manager would need to adopt measures not needed if the system could accept a 72-hour disruption. Similarly, if most system components could tolerate a 24-hour outage but a critical component could only be unavailable for 8 hours, the system manager could prioritize recovery actions and resources to meet that requirement. By prioritizing these recovery strategies, the system manager may make more informed, tailored decisions regarding contingency resource allocations and expenditures, saving time, effort, and costs.

3.3 Identify Preventive Controls

As indicated in the previous section, the BIA can provide the system manager with vital information regarding system availability and recovery requirements. 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, preventive methods should be used rather than measures designed to recover the system after a disruption. A wide variety of preventive controls are available, depending on system type and configuration; however, some common measures are listed below:

- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls)
- Gasoline or diesel powered generators to provide long-term backup power
- Air conditioning systems with adequate excess capacity to permit failure of certain components, such as a compressor
- Fire suppression systems
- Fire and smoke detectors
- Water sensors in the computer room ceiling and floor
- Plastic tarps that may be unrolled over IT equipment to protect it from water damage
- Heat-resistant and waterproof containers for backup media and vital nonelectronic records
- Emergency master system shutdown switch.

⁹ The recovery strategy may include a combination of preventive controls described in the Section 3.3 and recovery techniques and technologies described in Section 3.4.

Preventive controls should be documented in the contingency plan, and personnel associated with the system should be trained on how and when to use the controls. These controls should be maintained in good condition to ensure their effectiveness in an emergency.

3.4 Develop Recovery Strategies

Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address residual risks identified in the BIA. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

The recovery strategy selected should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full-spectrum of identified risks. A wide variety of recovery approaches may be considered; the appropriate choice depends on the type of system and its operational requirements.¹⁰ Specific recovery methods that should be considered may include commercial contracts with hot site vendors, reciprocal agreements with internal or external organizations, warm sites, cold sites, mobile sites, and service level agreements with the equipment vendors. In addition, technologies such as Redundant Arrays of Independent Disks (RAID), automatic failover, UPS, and mirrored systems should be considered when developing a system recovery strategy.

3.4.1 *Backup Methods*

System data should be backed up regularly. Policies should specify the frequency of backups (e.g., daily or weekly, incremental or full), based on data criticality and the frequency that new information is introduced. Data backup policies also should designate the location of stored data, file-naming conventions, tape rotation frequency, and the method for transporting data offsite. Data may be backed up on magnetic disk or tape or optical disks (such as compact disks [CD]). The specific method chosen for conducting backups should be based on system and data availability and integrity requirements. These methods include electronic vaulting, mirrored disks (using direct access storage devices [DASD] or RAID)¹¹, and floppy disks.

It is good business practice to store backed-up data offsite. Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. If using offsite storage, data is backed up at the organization's facility and then labeled, packed, and transported to the storage facility. If the data is required for recovery or testing purposes, the organization contacts the storage facility requesting specific data to be transported to the

¹⁰ Section 5.0, *IT System Specific Contingency Considerations*, provides detailed discussion of recovery methods applicable to specific IT systems.

¹¹ Detailed discussion of DASD and RAID are discussed in Section 5.0.

organization or to an alternate facility.¹² Commercial storage facilities also often offer media transportation and response and recovery services.

When selecting an offsite storage facility and vendor, the following criteria should be considered—

- Geographic area — consider the distance from organization and the probability of the storage site being affected by same disaster event as the organization
- Accessibility — consider the length of time necessary to retrieve the data from storage and the storage facility's operating hours
- Security — security capabilities of the storage facility and employee confidentiality must meet the data's sensitivity and security requirements
- Environment — consider the structural and environmental conditions of the storage facility, (i.e., temperature, humidity, fire prevention, and power management controls)
- Cost — consider the cost of shipping, operational fees, and disaster response/recovery services.

3.4.2 Equipment Replacement

If the IT system is damaged or destroyed or the primary site is not available, necessary hardware and software requirements will need to be procured quickly and delivered to the recovery location. Three basic strategies exist to prepare for equipment replacement.

- **Vendor Agreements.** As the contingency plan is being developed, service level agreements (SLA) with hardware, software, and support vendors may be made for emergency maintenance service. The SLA should specify the vendor's response time after being notified. The agreement also should give the organization priority status for the shipment of replacement equipment. The details of these negotiations should be documented in the SLA, which should be maintained with the contingency plan.
- **Equipment Inventory.** Equipment required may be purchased in advance and stored at a secure offsite location, such as an alternate site where recovery operations will take place (warm or mobile site) or at another location where they will be stored and then shipped to the recovery site. This solution has certain drawbacks however. An organization must commit financial resources to purchase this equipment in advance,¹³ and the equipment could become obsolete or unsuitable for use over time, as system technologies and requirements change.
- **Existing Equipment.** Equipment currently housed and used by the contracted hot site or by another organization may be utilized by the organization. Agreements made with hot sites and reciprocal sites stipulate that similar equipment will be available for contingency use by the organization. It also is possible that another organization within the department may have similar equipment that can be used during an emergency.

¹² Backup tapes should be tested regularly to ensure that data is being stored correctly and that the files may be retrieved without errors or lost data. Also, the system manager should test the backup tapes at the alternate site, if applicable, to ensure that the site supports the same backup configuration that the organization has implemented.

¹³ Retired equipment may be suitable for use as spare or backup hardware; this strategy would reduce capital replacement costs.

When evaluating the choices, the system manager should consider that purchasing equipment when needed is cost-effective, but can add significant overhead time to recovery while waiting for shipment and setup; storing unused equipment is costly, but allows recovery operations to begin more quickly. Regardless of the strategy selected, detailed lists of equipment needs and specifications should be maintained within the contingency plan. Documentation of equipment lists is discussed further in Section 4.1., *Supporting Information*.

3.4.3 *Alternate Sites*

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, the plan must include a strategy to recovery and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

- Dedicated site owned or operated by the agency
- Reciprocal agreement or memorandum of agreement with an internal or external entity
- Commercially leased facility.

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types also may be categorized in terms of their operational readiness. Based on this factor, sites may be classified as cold sites, mobile sites, warm sites, hot sites, and mirrored sites. Progressing from basic to advanced, the sites 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 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.
- ***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 receive 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 the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24/7. Hot site personnel begin to prepare for the system arrival as soon as they are notified that the contingency plan has been activated.
- ***Mobile Sites*** are self-contained, transportable shells custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements. These 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 recovery location. In most cases, to be a viable recovery solution, mobile sites should be designed in advance with the vendor, and a service level agreement should be signed between the two parties. This is necessary because the time required to configure the mobile site can be extensive, and without prior coordination, the time to deliver the mobile site may exceed the system's allowable outage time.

- **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 agency.

There are obvious cost and ready-time differences among the four options. The mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain; however, they require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours. However, installation time can increase this response time. Table 3-1 summarizes the criteria that can be employed to determine which type of alternate site meets the organization's requirements. Sites should be analyzed further by the organization based on the specific requirements defined in the BIA. As sites are evaluated, the system manager also should ensure that the system's security controls, such as firewalls and physical access controls, are compatible with the prospective site.

Table 3-1: Alternate Site Criteria Selection

| Site | Cost | Hardware Equipment | Telecommunications | Setup Time | Location |
|----------------------|-------------|--------------------|--------------------|------------|-----------|
| Cold Site | Low | None | None | Long | Fixed |
| Warm Site | Medium | Partial | Partial/Full | Medium | Fixed |
| Hot Site | Medium/High | Full | Full | Short | Fixed |
| Mobile Site | High | Dependent | Dependent | Dependent | Not Fixed |
| Mirrored Site | High | Full | Full | None | Fixed |

These alternate sites may be owned and operated by the organization (*internal recovery*) or may be contracted for commercially. If contracting for the site with a commercial vendor, adequate testing time, work space, hardware requirements, telecommunications requirements, support services, and recovery days (how long the organization can occupy the space during recovery period) must be negotiated and clearly stated in the contract. Customers should be aware that multiple organizations may contract with a vendor for the same alternate site, and, as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously.

Two organizations with similar or identical IT configurations and backup technologies may enter a formal agreement to serve as alternate sites for one another. This type of site is set up via a *reciprocal agreement* or MOA. A reciprocal agreement should be entered into carefully because each site must be able to support the other in addition to their own workload, in the event of a disaster. Testing should be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and backup configurations, sufficient telecommunications connections, and compatible security measures, in addition to functionality of the recovery strategy.

3.4.4 Roles and Responsibilities

Having selected and implemented the system recovery strategy, the system manager must designate appropriate teams to implement the strategy. Each team should be trained and ready to deploy in the event of a disruptive situation requiring plan activation. Recovery personnel should be assigned to one of several specific teams that will respond to the event, recover capabilities, and return the system to normal operations. To do so, they will need to clearly understand the team's goal in the recovery effort, each step they are to execute, and how their team relates to other teams.

The specific types of teams required are based on the system affected. The size of each team, specific team titles, and hierarchy designs depend on the organization. A capable strategy will require some or all of the following functional groups:

- Management Team
- Damage Assessment Team
- Operating System Administration Team
- Systems Software Team
- Server Recovery Team (e.g., client server, Web server, etc.)
- LAN/WAN Recovery Team
- Database Recovery Team
- Network Operations Recovery Team
- Application Recovery Team(s)
- Telecommunications Team
- Hardware Salvage Team
- Alternate Site Recovery Coordination Team
- Original Site Restoration Coordination Team
- Test Team
- Administrative Support Team
- Transportation and Relocation Team
- Procurement Team

Personnel should be chosen to staff these teams based on their skills and knowledge. Ideally, teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. For example, Server Team members should include the server administrators. Team members must understand the contingency plan purpose, as well as the procedures necessary for executing the recovery strategy. Teams should be sufficient in size to remain viable if some members are unavailable to respond, or alternate team members may be

designated. Similarly, it is useful for team members to be familiar with the goals and procedures of other teams to facilitate inter-team coordination.

Each team is led by a team leader who directs overall team operations and serves as the team’s representative to management and other recovery elements. The team leader disseminates information to team members and approves any decisions that must be made within the team. Team leaders should have a designated alternate to act as the leader if the primary leader is unavailable.

For most systems, a Management Team is necessary for providing overall guidance following a major system disruption or emergency. The team is responsible for activating the contingency plan and supervises the execution of contingency operations. The Management Team also facilitates communications among other teams and supervises plan tests and exercises. All or some of the Management Team also may lead specialized contingency teams.

3.4.5 Cost Considerations

The system manager should ensure that the strategy chosen can be implemented effectively with available personnel and financial resources. The cost of each type of alternate site, equipment replacement, and storage option under consideration should be weighed against budget limitations.¹⁴ The system manager should determine known contingency planning expenses, such as recovery site contract fees, and those that are less obvious, such as the cost of implementing departmentwide awareness programs and contractor support. The budget must be sufficient to encompass software, hardware, travel and shipping, testing, plan training programs, awareness programs, labor-hours, other contracted services, and any other applicable resources. The agency should perform a cost-benefit analysis to identify the optimum recovery strategy. Table 3-2 provides a template for evaluating cost considerations.

Table 3-2: Recovery Strategy Budget Planning Template

| | | Vendor Costs | Hardware Costs | Software Costs | Travel / Shipping Costs | Labor / Contractor Costs | Testing Costs |
|------------------------------|----------------------|--------------|----------------|----------------|-------------------------|--------------------------|---------------|
| Alternate Site | Cold Site | | | | | | |
| | Warm Site | | | | | | |
| | Hot Site | | | | | | |
| | Mobile Site | | | | | | |
| | Mirrored Site | | | | | | |
| Offsite Storage | Commercial | | | | | | |
| | Internal | | | | | | |
| Equipment Replacement | SLAs | | | | | | |
| | Storage | | | | | | |
| | Existing use | | | | | | |

¹⁴ If possible, the costs and benefits of technical recovery methods should be evaluated during system development.

3.5 Testing, Training, and Exercises

Plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps to evaluate the ability of recovery staff to implement the plan quickly and effectively. Each element of the contingency plan should be tested to confirm the accuracy of individual recover procedures and the overall effectiveness of the plan. Areas that should be addressed in a contingency test include:

- System recovery on an alternate platform from backup tapes
- Coordination among recovery teams
- Internal and external connectivity
- Restoration of normal operations.

To derive the most value from the test, explicit test objectives and success criteria should be identified. For example, one test objective might be the recovery of a database, database server, and operating system at an alternate site. Two success criteria may be recovery within 8 hours and database recovery with no errors. The use of test objectives and success criteria enable the effectiveness of each plan element as well as the overall plan to be assessed. Test results and lessons learned should be documented and reviewed by test participants and other personnel as appropriate. Information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the contingency plan.

Training for personnel with contingency plan responsibilities should complement testing. Training should be provided at least annually; new hires that will have plan responsibilities should receive training shortly after they are hired. Recovery personnel should be trained on the following plan elements:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (activation/notification, recovery, and reconstitution phases)
- Individual responsibilities (activation/notification, recovery, and reconstitution phases).

3.6 Plan Maintenance

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, and policies. IT systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly to ensure new information is documented and contingency measures are revised if required. As a general rule, the plan should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the plan. Certain elements will require more frequent reviews, such as contact lists. Based on the system type and criticality, it may be reasonable to evaluate plan

contents and procedures more frequently. At a minimum, plan reviews should focus on the following elements:

- Operational requirements
- Technical procedures
- Hardware, software, and other equipment (types, specifications, and amount)
- Names and contact information of team members
- Names and contact information of vendors, including alternate and offsite POCs
- Alternate and offsite facility requirements
- Vital records (electronic and hard-copy).

Because the contingency plan contains potentially sensitive operational and personnel information, its distribution should be controlled. Typically, copies of the plan are provided to recovery personnel and are stored at the alternate site and also with the backup tapes. Storing a copy of the plan at the alternate site ensures its availability and good condition in the event local plan copies can not be accessed due to the disaster. The system manager should maintain a record of copies of the plan and to whom they were distributed. Other information that should be stored with the plan, include contracts with vendors (SLAs and other contracts), software licenses, system users manuals, and operating procedures.

Changes made to the plan, strategies, and policies should be coordinated through the system manager, who should communicate changes to the representatives of associated plans or programs, as necessary. The system manager should record plan modifications using a Record of Changes, which lists the page number, change comment, and date of change. The Record of Changes, depicted in Table 3-3, should be integrated into the plan as discussed in Section 4.1.

Table 3-3: Sample Record of Changes

| Record of Changes | | | |
|--------------------------|-----------------------|-------------|------------------|
| Page # | Change Entered | Date | Signature |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

The system manager should coordinate with associated internal and external organizations and system POCs frequently to ensure that impacts caused by changes within either organization will be reflected in the contingency plan.

The system manager also should evaluate supporting information to ensure that it is current and continues to meet system requirements adequately. This information includes, but is not limited to—

- Alternate site contract, including testing times
- Offsite storage contract
- Software licenses
- MOUs or vendor SLAs
- Mitigation strategy
- Contingency policies
- Training and awareness materials.

Although some changes may be quite visible, others will require additional analysis. The BIA should be reviewed periodically and updated with new information to identify new contingency requirements or priorities. As new technologies become available, preventive controls may be enhanced and recovery strategies may be modified. In addition, the NIST SP 800-26, *Security Self-Assessment for Information Technology Systems*,¹⁵ provides a checklist to assist in determining the viability of contingency planning elements.

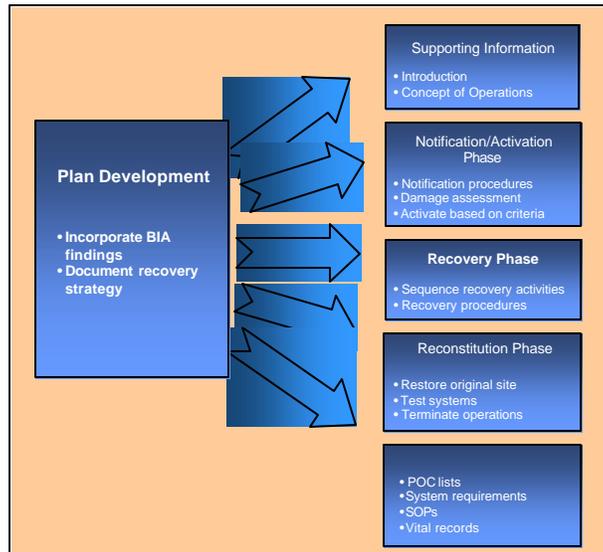
¹⁵ This table is located in SP 800-26, Section 4.2.4, *Contingency Planning*.

4. IT CONTINGENCY PLAN DEVELOPMENT

This section discusses the key elements that comprise the contingency plan. As described in Section 3, contingency plan development is a critical step in the process of establishing a comprehensive contingency planning program. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The contingency plan also should document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the organization and its requirements. Plans need to balance detail with flexibility; usually the more detailed the plan is, the less scalable and versatile the approach. The information presented here is meant to be a guide; however, the plan format in this document may be modified as needed to better meet the user's specific system, operational, and organization requirements. Appendix A provides a template that individuals may use to develop contingency plans for their respective systems.

As shown in Figure 4-1 below, this planning guide identifies five main components of the contingency plan. The Notification / Activation, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency. The Supporting Information and Appendixes components provide other essential data to ensure a comprehensive plan. Each plan component is discussed later in this section.

Figure 4-1: Contingency Plan Structure



Plans should be formatted to provide quick and clear direction in the event personnel unfamiliar with the plan or the systems are performing recovery operations. Plans should be clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures should be used. A concise and well-formatted plan also reduces the likelihood of creating an overly complex or confusing plan.

4.1 Supporting Information

The Supporting Information component includes two main sections that provide essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These sections, Introduction and Concept of Operations, are discussed below.

The *Supporting Information* section helps the reader to understand the premise of the IT contingency plan should be provided as an introduction and/or concept of operations to the plan. These details help the plan user in understanding the applicability of the guidance within, in making decisions on how to use the plan, and guidance on where associated plans and information outside the scope of the plan may be found. The *Introduction* section also orients the reader to the type and location of information contained in the plan. Generally, the section includes the Purpose, Scope, Authorities/References, and Record of Changes.¹⁶ These subsections are described below.

- **Purpose.** This section establishes the reason for developing the contingency plan; it also defines the plan objectives.
- **Scope.** The scope discusses the issues, situations, and conditions addressed and not addressed in the plan. The section identifies the target system and the locations covered by the plan if the system is distributed among multiple locations. For example, the plan may not address short-term disruptions expected to last less than 4 hours, or it may not address catastrophic events that result in the destruction of the IT facility.
- The scope also should address any assumptions made in the plan, such as the assumption that all key personnel would be available in an emergency. However, assumptions should not be used as a substitute for thorough planning. For example, the plan should not assume that disruptions would occur only during business hours; by developing a contingency plan based on such an assumption, the system manager may be unable to recover the system effectively should a disruption occur during nonbusiness hours.
- **Authority/References.** This section identifies the Federal or Agency documents that require or govern the information contained in the contingency plan. The section also documents the organizations subject to the contingency plan.
- **Record of Changes.** The contingency plan should be a living document that is changed as required to reflect system or operational changes. Changes made to the plan should be recorded in the Record of Changes located at the front of the plan.¹⁷

The Concept of Operations section provides additional details about the IT system, the contingency planning framework, and response, recovery, and resumption activities. Sections of *The Concept of Operations* may include the following elements:

¹⁶ As stated previously, this plan format is meant to guide the contingency plan developer. Individuals may choose to add, delete, or modify this format as required, to best fit the system's and organization's contingency planning requirements.

¹⁷ The Record of Changes was discussed in Section 3.6, Plan Maintenance.

- **System Description.** It is necessary to include a general description of the system addressed by the contingency plan. The description should include the system architecture, location(s), and any other important technical considerations.¹⁸ A system architecture diagram, including security devices, such as firewalls, and internal and external connections, are useful.
- **Responsibilities.** The Responsibilities section presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The section also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation. Roles should be assigned to team positions rather than to a specific individual. Listing team members by role rather than by name not only reduces confusion if the member is unavailable to respond but also helps reduce the number of changes that would have to be made to the document because of personnel turnover.

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 assess system damage, implement the plan, and notify recovery personnel. At the completion of the Notification/Activation Phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis.

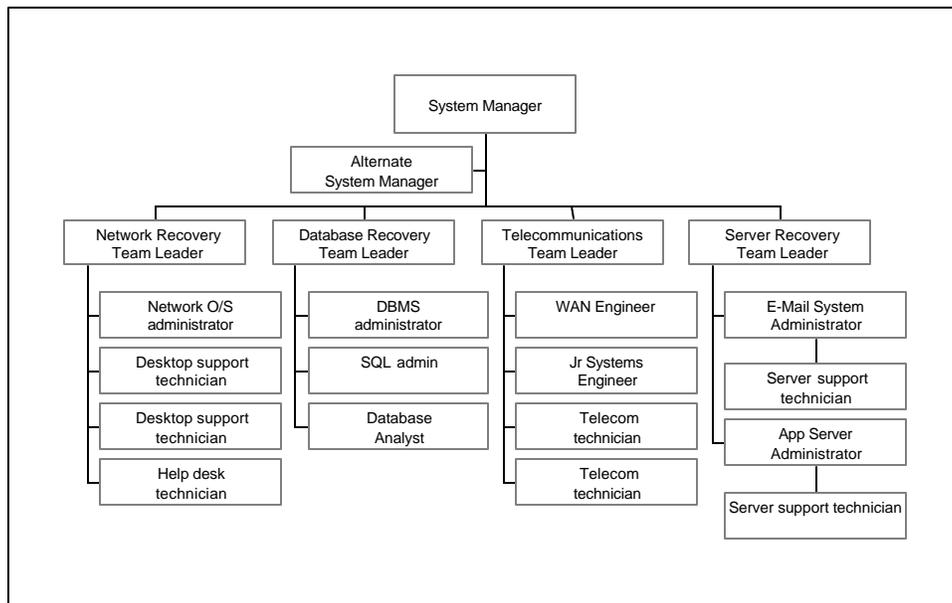
4.2.1 *Notification Procedures*

An event may occur *with* or *without* prior notice. For example, advanced notice is often given that a hurricane will affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act. Notification procedures should be documented in the plan for either type of situation. The procedures also should describe the methods used to notify recovery personnel during business and non-business hours. Prompt notification is important to reduce the impacts on the IT system, and in some cases it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash.

Notifications can be accomplished through a variety of methods, including telephone, pager, e-mail, or cell phone. The notification strategy should define procedures to be followed in the event that certain personnel cannot be contacted. Notification procedures should be documented clearly in the contingency plan. A common notification method is a *call tree*. This technique involves assigning notification duties to specific individuals, who in turn, are responsible for notifying other recovery personnel. The call tree should account for primary and alternate contact methods and should discuss procedures to be followed if an individual cannot be contacted. Figure 4-2 presents a sample call tree.

¹⁸ NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998, provides guidance for formatting the system description.

Figure 4-2: Sample Call Tree



Personnel to be notified should be clearly identified in the contact lists appended to the plan. This list should identify personnel by their team position, name, and contact information including home, work, and pager numbers, electronic mail (e-mail) addresses, and home addresses. An entry may resemble the following format:

Systems Software Team

Team Leader—Primary

Jane Jones

1234 Any Street

Town, State, Zip code

Home: (123) 456-7890

Work: (123) 567-8901

Cell: (123) 678-9012

E-mail: jones@organization.ext

Notification also should be sent to points-of-contact (POC) of external organizations or system partners that may be adversely affected if they are unaware of the situation or if they have recovery responsibilities. These POCs should also be listed in an appendix to the plan.¹⁹

The type of information to be relayed to those being notified should be documented in the plan. The following information may be relayed may—

- The nature of the incident that has occurred or is impending
- Any known damage estimates

¹⁹ The contact lists generally contain sensitive information and should be disseminated only to those requiring access. The lists should be frequently reviewed to ensure names, positions, and contact information is up-to-date.

- Response and recovery details
- Where and when to convene for briefing or further response instructions
- Instructions to prepare for relocation for estimated time period
- Instructions to complete notifications using the call tree (if applicable).

4.2.2 Damage Assessment

To determine how the contingency plan will be implemented following an emergency, it is essential to assess the nature and extent of the damage to the system. This damage assessment should be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. Once the impact to the system has been determined, contingency staff should be notified using the notification procedures described in the section above. Damage assessment procedures must be specific to the particular system; however, the following areas should be addressed:

- Cause of the emergency or disruption
- Potential for additional disruptions or damage
- Area affected by the emergency
- Status of physical infrastructure (e.g., structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning[HVAC])
- Inventory and functional status of IT equipment (e.g., fully functional, partially functional, and nonfunctional)
- Type of damage to IT equipment or data (e.g., water damage, fire and heat, physical impact, and electrical spike)
- Items to be replaced (hardware, software, firmware, and supporting materials)
- Estimated time to restore normal services.

4.2.3 Plan Activation

The contingency plan should be activated only when the damage assessment indicates that one or more of the activation criteria for that system are met. If an activation criterion is met, the system manager should activate the plan.²⁰ Activation criteria for events are unique for each organization and should be stated in the contingency planning policy statement. Criteria may be based on—

- Safety of personnel and/or status of facility
- Extent of damage to system (physical, operational, or cost)
- Anticipated duration of disruption.

²⁰ For this document, the IT system manager is assumed to have the authority to implement the contingency plan. That authority may vary among organizations; however, the individual(s) with this authority should be designated clearly in the plan.

Once the system damage has been characterized, the system manager may select the appropriate recovery strategy,²¹ and the associated recovery teams may be notified. Notification should follow the procedures outlined in Section 4.2.1.²²

4.3 Recovery Phase

Recovery operations begin after the contingency plan has been activated, personnel have been notified, and appropriate teams have been mobilized. Recovery phase activities focus on contingency measures to restore temporary IT processing capabilities, where as other efforts are directed to repair damage to the original system and restore operational capabilities at the original facility. At the completion of the recovery phase, the 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, recovery and operation on an alternate system, or relocation and recovery at an alternate site.

4.3.1 *Sequence of Recovery Activities*

When recovering a complex system, such as a WAN, involving multiple independent components, recovery procedures should reflect system priorities identified in the BIA. The sequence of activities should reflect the system's allowable outage time to avoid significant impacts to related systems and business processes. Procedures should be written in a stepwise, sequential format so system components may be restored in a logical fashion. For example, if a LAN is being recovered after a disruption, the most critical servers should be recovered before other, less critical devices, such as printers. Similarly, to recover an application server, procedures first should address operating system restoration and verification before the application and its data are recovered. The procedures should also include instructions to coordinate with other teams when certain situations occur, such as—

- An action is not completed within the expected time frame
- A key step has been completed
- Item(s) must be procured
- Other system-specific concerns.

If conditions require the system to be recovered at an alternate site, certain materials will need to be transferred there or procured. These items may include shipment of data backup tapes from offsite storage, hardware, copies of the recovery plan, and software programs. Procedures should designate the appropriate team or team members to coordinate shipment of equipment, data, and vital records. References to applicable appendixes, such as equipment lists or vendor contact information, should be made in the plan where necessary. Procedures should clearly

²¹ For example, if the incident is expected to cause only a short-term disruption and physical damage is limited to a particular hardware device, the system manager may choose to recover the system onsite, using another device. However, if the damage assessment reveals extensive damage to the facility, the system manager may need to relocate the system and recovery teams to an alternate site for an extended period.

²² If the event requires IT operations to be relocated temporarily to an alternate site, travel arrangements should be made for recovery team members. Travel information such as preferred travel agency, hotels, and car rental companies may be included as a contingency plan appendix.

describe requirements to package, transport, and purchase materials required to recover the system.

4.3.2 Recovery Procedures

To facilitate recovery phase operations, the contingency plan should provide detailed procedures to restore the system or system components.²³ Procedures should be assigned to the appropriate recovery team and typically address the following actions:

- Installing necessary hardware components
- Loading backup tapes or media
- Restoring operating system and application(s)
- Restoring system data
- Testing system functionality
- Connecting system to network or other external systems
- Operating the system in accordance with contingency plan objectives.

Recovery procedures should be written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted. A checklist format is useful for documenting the sequential recovery procedures. It also is useful for troubleshooting problems if the system cannot be recovered properly. The example below provides an example of a general procedural checklist for a LAN Recovery Team.

| | | | | | | | | |
|---|--|--------------|---|--------------|--|--------------|--|--------------|
| <p>Recovery Process for the LAN Recovery Team: <i>These procedures are for recovering volume files from Backup tapes. The LAN Recovery Team is responsible for reloading all critical files necessary to continue production.</i></p> <table><tr><td>▪ Identify tape number using tape log book</td><td>Time: __: __</td></tr><tr><td>▪ If tape is not in correct location, request from recovery facility; fill out request with appropriate authorizing signature</td><td>Time: __: __</td></tr><tr><td>When tape is received, place into tape drive</td><td>Time: __: __</td></tr><tr><td>▪ When volume files are recovered, notify LAN Recovery Team Leader</td><td>Time: __: __</td></tr></table> | ▪ Identify tape number using tape log book | Time: __: __ | ▪ If tape is not in correct location, request from recovery facility; fill out request with appropriate authorizing signature | Time: __: __ | When tape is received, place into tape drive | Time: __: __ | ▪ When volume files are recovered, notify LAN Recovery Team Leader | Time: __: __ |
| ▪ Identify tape number using tape log book | Time: __: __ | | | | | | | |
| ▪ If tape is not in correct location, request from recovery facility; fill out request with appropriate authorizing signature | Time: __: __ | | | | | | | |
| When tape is received, place into tape drive | Time: __: __ | | | | | | | |
| ▪ When volume files are recovered, notify LAN Recovery Team Leader | Time: __: __ | | | | | | | |

4.4 Reconstitution Phase

In the Reconstitution Phase, recovery activities are terminated and normal operations are transferred back to the original facility.²⁴ During the Recovery Phase, as the contingency activities are performed, reconstitution of the original site should be under way. Once the original site is restored to the level that it can support the IT system and its normal processes, the system may be transitioned back to the original site. Until the primary system is restored and

²³ Given the extensive variety of system types, configurations, and applications, this planning guide does not provide specific recovery procedures. However, recovery considerations are detailed for each IT system type in Section 5.0.

²⁴ Should the original facility be unrecoverable, the activities in this phase also can be applied to preparing a new facility to support system processing requirements.

tested at the original site, the contingency system should continue to be operated. The Reconstitution Phase should specify teams responsible for restoring the original site and the IT system. The following major activities occur in this phase:

- Ensuring adequate infrastructure support, such as electric power, telecommunications, security, and environmental controls
- Installing system hardware, software, and firmware at the original site. This step should include detailed restoration procedures similar to those followed in the Recovery Phase
- 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
- Shutting down the contingency system
- Terminating contingency operations
- Cleaning the office space used, if at another location, of any sensitive materials
- Arranging for recovery personnel to return to the original facility.

4.5 Plan Appendixes

Contingency plan appendixes provide key details not contained in the main body of the plan. The appendixes should reflect the specific technical, operational, and contingency requirements of the given system; however, some appendixes are found frequently in contingency plans. Common contingency plan appendixes include the following:

- Contact information for recovery personnel and teams
- Vendor contact information, including offsite storage and alternate site POCs
- Standard operating procedures (SOPs) and checklists for system recovery or processes
- Equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations. Details should be provided for each entry, including model or version number, specifications, and quantity.
- Vendor SLAs, reciprocal agreements with other organizations, and other vital records
- Description of, and directions to, the alternate site
- The BIA, conducted during the planning phases, contains valuable information about the interrelationships, risks, and impacts to each element of the system. The BIA may be included as an appendix for reference should the plan be activated.

5. TECHNICAL CONTINGENCY PLANNING CONSIDERATIONS

This section complements the process and framework guidelines presented in earlier sections by the discussing technical contingency planning considerations for specific types of IT systems. The information presented in this section is intended to assist the reader in selecting, developing, and implementing specific technical contingency strategies based on the type of IT system. Because each system is unique, information is provided at a level that may be used by the widest audience. All of the information presented may not apply to a specific IT system; therefore, the system manager should draw on the information as appropriate and modify it to be meet the system's particular contingency requirements. The following IT platforms are addressed in this section:

- Desktop computers and portable systems
- Servers
- Web sites
- Local area networks
- Wide area networks
- Distributed systems
- Mainframe systems.

For each IT platform type, technical measures are considered from two perspectives. First, the document discusses technical requirements or factors that the system manager should consider when planning a system recovery strategy. Second, technology-based solutions are provided for each platform. The technical considerations and solutions addressed in this section include preventive measures discussed in Section 3.3 and recovery measures described in Section 3.4. Several of these contingency measures are common to all IT systems. Common considerations include the following:

- Backup and offsite storage of data, applications, and the operating system
- Redundancy of critical system components or capabilities
- Documentation of system configurations and requirements
- Interoperability between system components and between primary and alternate site equipment to expedite system recovery
- Appropriately sized and configured power management systems and environmental controls.

Each of these considerations is discussed throughout Section 5.

5.1 Desktop Computers and Portable Systems

A computer is a device that accepts digital data and manipulates the information based on a program or sequence of instructions for how data is to be processed. *Personal Computers* are those computers that are capable of accepting data and instructions, executing the instructions to process the data, and presenting the results. A personal computer typically consists of a central

processing unit (CPU), memory, disk storage, and various input and output devices. A personal computer is designed for use by one person at a time. Personal computers can be classified as a desktop computer or a portable system (e.g. laptop or handheld device).

Desktop computers are stationary personal computers that fit conveniently on top of an office desk or table. They are not well suited to move or travel. A desktop computer consists of three basic components:

- A micro-tower case or mini-tower case designed to fit under the desk or on top of the desk which contains the CPU, memory, disk storage, a motherboard and ports for cards such as video cards or network interface cards. Depending on the configuration, the case can also contain a floppy drive, CD-ROM drive or other internal devices.
- Input devices connect to the case, such as a keyboard, mouse, external CD-ROM, or portable storage devices, and
- Output devices connect to the case through appropriate cabling such as a printer and display monitor.

Portable systems, such as laptops or handheld computers, are personal computers that can be carried for convenience and travel purposes. Portable systems are compact desktop computers that can have comparable processing, memory and disk storage to desktop computers or limited processing memory and disk storage, such as a handheld computer.

A laptop computer, also called a *notebook computer*, is a battery- or AC-powered personal computer generally smaller than a briefcase, lightweight, easily transportable, and can be used conveniently in temporary spaces. A handheld computer is a personal computer that can conveniently be stored in a pocket and used while being held; thus the handheld computer is considerably smaller than a laptop. Handheld computers are also referred to as *personal digital assistants (PDAs)*. The processing, memory and disk storage capability of handheld computers varies by brand and model. Handheld computers can accept handwriting, or a variation of handwriting, as input in addition to typing through small keyboards.

Personal computers are ubiquitous in most organizations' IT infrastructures. Because the desktop and portable computers are the most common platform for routine automated processes, they are important elements in a contingency plan. Personal computers can be physically connected to an organization's LAN, dial into the organization's network from a remote location, or can be act as a stand-alone system.

5.1.1 Contingency Considerations

Contingency considerations for desktop and portable systems should emphasize data availability and integrity. To address these requirements, the systems manager should consider the following best practices:

- **Store backups offsite.** As mentioned in Section 3.4.1, backup media should be stored offsite in a secure, environmentally controlled facility. If users back up data on a stand-alone system rather than saving data to the network, a means should be provided for storing the media at an alternate site. A copy of the contingency plan, software licenses, vendor SLAs and contracts, and other important documents should be stored with the backup media.
- **Encourage individuals to backup data.** If the personal computer backup process is not automated from the network, users should be encouraged to backup data on a regular basis. This can be conducted through employee security training and awareness.
- **Provide guidance on saving data on personal computers.** Instructing users to save data to a particular folder eases the IT department's desktop support requirements. In the event that a machine must be rebuilt, the technician will know which folders to copy and preserve while the system is being reloaded.
- **Standardize hardware, software, and peripherals.** System recovery is faster if hardware, software, and peripherals are standardized throughout the organization. If standard configurations are not possible throughout the organization, then configurations should be standardized by department or by machine type or model if possible. Additionally, critical hardware components that would need to be recovered immediately in the event of a disaster should be compatible with off-the-shelf computer components. This will avoid delays in ordering custom-built equipment from a vendor.
- **Document system configurations and vendor information.** Well-documented system configurations ease recovery. Similarly, vendor names and emergency contact information should be listed in the contingency plan so that replacement equipment may be purchased quickly.
- **Coordinate with Network Security Policy and System Security Controls.** Desktop and portable computer contingency solutions should be coordinated with network security policies. Network security controls, such as virus protection, can help protect against malicious code or attacks that could compromise the computer's availability. In choosing the appropriate technical contingency solution, data confidentiality, and sensitivity requirements should be considered to ensure that the technical contingency solution does not compromise or disclose sensitive, proprietary, or classified data.

5.1.2 Contingency Solutions

A wide range of technical contingency solutions are available for desktop computers; several best practices are discussed here.

Backups are the most common means to ensure data availability on personal computers. Personal computers should be backed up on a regular basis, which should be determined by data criticality and the frequency of data updates. The user or owner also should identify the files and folders to be backed up. If the backup is completed from the network, users should be instructed to save all files to a specific folder. This will reduce the amount of media required for the backup. Certain factors should be considered when choosing the appropriate backup solution.

- **Equipment Interoperability.** To facilitate recovery, the backup device should be compatible with platform operating system and applications and should be easy to install onto different models or types of personal computers.
- **Storage volume.** To ensure adequate storage, the amount of data to be backed up should determine the appropriate backup solution.
- **Media Life.** Each type of media has a different use and storage life beyond which, the media cannot be relied on for effective data recovery.
- **Backup Software.** When choosing the appropriate backup solution, the software or method used to backup data should be considered. In some cases, the backup application can be as simple as a file copy using the operating system file manager; in cases involving larger data transfers, a third party application may be needed to automate and schedule the file backup.

Personal computer data backups can be accomplished in various ways, including those listed below:²⁵

- **Floppy Diskettes.** Floppy diskette drives come standard with most desktop computers and represent the cheapest backup solution; however, these drives have a low storage capacity and are slow in saving data.
- **Tape Drives.** Tape drives are not common in desktop computers, but are an option for a high capacity backup solution. Tape drives are automated and require a third party backup application or backup capabilities in the operating system. Tape media are relatively low cost.
- **Removable Cartridges.** Removable cartridges are not common in desktop computers and are often offered as a backup solution as a portable or external device. Removable cartridges are more expensive than floppy diskettes and are comparable in cost to tape media depending on the media model and make. However, removable cartridges are fast and their portability allows for flexibility. The portable devices come with special drivers and application to facilitate data backups.
- **Compact Disk.** CD, read-only-memory (CD-ROM) drives come standard in most desktop computers; however, not all computers are equipped with writeable CD drives. CDs are low cost storage media and have a higher storage capacity than floppy diskettes. To read from a CD, the operating system's file manager is sufficient; however, to write to a CD, a re-writable CD (CD-RW) drive and the appropriate software is required.
- **Network Storage.** Data stored on networked personal computers can be backed up to a network storage device or a networked disk:

²⁵ Section 5.2 discusses different backup methods that can be used: full, incremental and differential.

- **Networked disk.** A server with data storage capacity is a networked disk. The amount of data that can be backed up from a personal computer is limited by the network disk storage capacity or disk allocation to the particular user. However, if users are instructed to save files to a networked disk, the networked disk itself should be backed up through the network or server backup program.
- **Networked storage device.** A network backup system can be configured to backup the local drives on networked personal computers. The backup can be started from either the networked backup system or the actual personal computer.
- **Replication or Synchronization.** Data replication or synchronization is a common backup method for portable computers. Handheld computers or laptops may be connected to a personal computer and replicate the desired data from the portable system to the desktop computer.
- **Internet Backup.** Internet Backup, or Online Backup, is a commercial service that allows personal computer users to backup data to a remote location over the Internet for a fee. A utility is installed onto the personal computer that allows the user to schedule backups, select files and folders to be backed up, and establish an “archiving” scheme to prevent files from being over-written. Data can be encrypted for transmission. The disadvantage of this method is that the data transfer speed will be slow over a modem connection. Additionally, this method may not be appropriate for storing sensitive data if high confidentiality is required. The advantage of this method that the user is not required to purchase data backup hardware or media.

DESKTOP COMPUTER CONTINGENCY STRATEGIES:

- DOCUMENT SYSTEM AND APPLICATION CONFIGURATIONS
- ENSURE INTEROPERABILITY AMONG COMPONENTS
- APPROPRIATE SECURITY CONTROLS
- DATA BACKUP AND OFFSITE STORAGE
- APPLICATION BACKUP AND OFFSITE STORAGE
- ENCRYPTION KEY BACKUP
- DISK IMAGING
- REDUNDANT CRITICAL SYSTEM COMPONENTS
- UNINTERRUPTIBLE POWER SUPPLIES

In addition to backing-up data, organizations should **store software and software licenses in a secondary location.** If the software is commercial-off-the-shelf (COTS), it can be purchased through a vendor in the event that the copy or license installed prior to destruction is unavailable. However, at a minimum, custom-built applications installed on desktops should be saved to an alternate location or backed-up through one of the methods described above. Instructions on recovering custom-built applications at an alternate site also should be documented, particularly if the application has hard-coded drive mappings (for the personal computer or network server). Code that prevents the application from running on a different system should be discouraged. If driver mappings are hard-coded, the application should be modified to enable the application to be restored on another system other than the original.

The popularity of encryption as a security tool used on portable computers is growing. With increased use of digital signatures for non-repudiation and the use of encryption for

confidentiality, organizations must **backup encryption key pairs and verification keys**.²⁶ If the encryption key pair and verification key are stored on the personal computer, data can become unrecoverable or unverifiable in the event the personal computer becomes corrupted.

Because portable computers are vulnerable to theft, encryption can be used to protect data from being disclosed on a stolen computer. Portable computer users can also be provided a **second hard drive** to be used while on travel. The second hard drive should contain only the minimum applications and data necessary. By utilizing a second hard drive, if the laptop is stolen, the amount of data loss is minimized.

PORTABLE SYSTEM CONTINGENCY STRATEGIES:

- DOCUMENT SYSTEM AND APPLICATION CONFIGURATIONS
- ENSURE INTEROPERABILITY AMONG COMPONENTS
- APPROPRIATE SECURITY CONTROLS
- DATA REPLICATION AND OFFSITE STORAGE
- APPLICATION BACKUP AND OFFSITE STORAGE
- ENCRYPTION KEY BACKUP
- ALTERNATE HARD DRIVES
- DISK IMAGING
- REDUNDANT CRITICAL SYSTEM COMPONENTS
- UNINTERRUPTIBLE POWER SUPPLIES

Imaging represents another contingency solution. A standard desktop computer image can be stored and the corrupted computer can be reloaded. Imaging will install the applications and setting stored in the image; however, all data currently on the disk will be lost. Therefore, personal computer users should be encouraged to backup their data files. Since disk images can be large, dedicated storage, such as a server or server partition, may need to be allocated for the disk images alone. To decrease the number of images necessary for recovery in the event that multiple personal computers are corrupted,

standardizing personal computer models and configurations across all organizations will save space and ease the process of rebuilding computers. If site relocation is necessary, personal computer configurations and basic applications needed for mission-critical processing should be documented in the contingency plan.

The system and its data can become corrupt due to a power failure. A personal computer can be configured with **dual power supplies** to prevent corruption. The two power supplies should be used at the same time so that if the main power supply becomes overheated or unusable, the second unit will become the main power source, resulting in no system disruption

The second power supply will protect against hardware failure, but not power failure. However, **UPS** can protect the system should power be lost. The UPS usually provide 30 to 60 minutes of backup temporary power. This may be enough to permit a graceful shutdown. A cost benefit analysis should be conducted to compare the dual power supply and UPS combination to other contingency solutions. While dual power supplies and UPS are cost-effective for a server, they might not be so for a personal computer.

²⁶ Non-repudiation cannot be guaranteed if the signing key from the signing key pair is backed up. The signing key should remain in one location and be regenerated if lost. NIST 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides additional information on data encryption.

5.2 Servers

A server is a common network device. Larger networks have multiple servers that perform provide various services to nodes, an end point for data transmissions, connected to the network. Servers support file sharing and storage, data processing, central application hosting (such as e-mail or a central database), printing, access control, user authentication, remote access connectivity, and other shared network services. Local users log into the server through networked personal computer to access resources that the server provides.

A *server* is a computer that runs administrative software to control access to all or part of the network and network resources, such as disk storage, printers, and network applications. A server can be any type of computer running a network operating system. It may be a standard personal computer, or a server can be a large computer containing multiple disk drives and a large amount of memory that will allow the computer to process hundreds of requests at once.

5.2.1 *Contingency Considerations*

Because servers can support a large number of users or host critical applications, server loss could cause significant problems to business processes. To address server vulnerabilities, the following best practices should be considered:

- **Store backup tapes offsite.** As described previously, backup tapes should be stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.
- **Standardize hardware, software, and peripherals.** System recovery may be expedited if hardware, software, and peripherals are standardized throughout the organization or site. Standard configurations should be documented in the contingency plan.
- **Document system configurations and vendors.** Maintaining detailed records of system configurations enhances system recovery capabilities. Additionally, vendors that supply essential hardware, software, and other components should be identified in the contingency plan.
- **Coordinate with Network Security Policy and System Security Controls.** Server contingency solutions should be coordinated with network security policies. Network security controls, such as virus protection and system vulnerability patching, can help protect against malicious code or attacks that could compromise the server's availability.

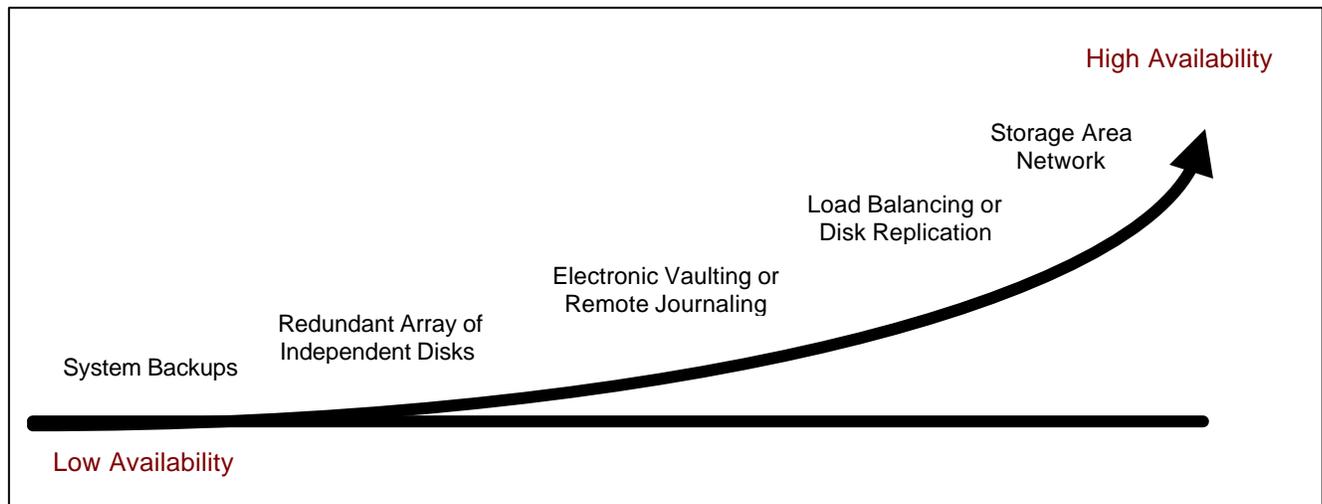
5.2.2 *Contingency Solutions*

Several technical measures are available to enhance server recovery capabilities. Server contingency planning should emphasize reliability and availability of the network services provided by the server. When selecting the appropriate technical contingency solution, data confidentiality and sensitivity requirements should be considered. Additionally, when selecting the appropriate server contingency solution, the availability requirements for the server, its applications, and data should be assessed. As a preventive contingency measure, critical

functions should not be co-located on servers with non-critical functions if possible. For example, a server hosting a critical application should be dedicated to that application and not provide other resources. If the server also supports a networked printer, and a large print job is sent to the printer, the server could be caused to crash due to insufficient resources.

Figure 5-1 presents a scale that maps the relative availability of the server contingency solutions discussed in this section. High availability is measured in terms of minutes of lost data or server downtime; low availability implies that server recovery could require days to be completed.

Figure 5-1: Server Contingency Solutions and Availability



As with personal computers, servers should be backed up regularly. Servers can be backed up through a distributed system, in which each server has its own tape drive, or through a centralized system, where a centralized backup device is attached to one server. There are three types of **system backup** methods available to preserve server data:²⁷

- **Full.** A full backup captures all files on the disk or within the folder selected for backup. Because all backed up files were recorded to a single tape or tape set, locating a particular file or group of files is simple. However, full backups may require a large number of tapes, and the time required to perform a full backup can be lengthy. Also, full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary tape storage requirements.
- **Incremental.** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. Incremental backups afford more efficient use of storage media, and backup times are reduced. However, to recover a system from incremental backup tapes, multiple tapes from different backup operations may be required. For example, consider a case in which a directory needed to be recovered. If the last full backup was performed three days prior, and one file has changed each day, then the tapes for

²⁷ Seagate “Types of Backups, Technical Bulletin #4062” <http://www.seagate.com/support/kb/tape/4062.html>

the full backup as well as for each day's incremental backups would be needed to restore the entire directory.

- **Differential.** A differential backup stores files that were created or modified since the last full backup. Therefore, if a file is changed since the previous full backup, a differential backup will save the file each time a differential is run until the next full backup is completed. The differential backup takes less time to complete than a full backup and may require fewer tapes than an incremental backup, because only the full backup tape and the last differential tape would be needed. As a disadvantage, differential backups take longer to complete than incremental backups. The time to complete a differential backup increases each day, because the amount of data being backed up is compiled since the last full backup.

Depending on system configuration and recovery requirements, the system manager can use a combination of backup operations. For example, a full backup can be conducted on the weekend with differential backups conducted each evening. In developing the server backup schedule, the following questions should be considered:

- Where will media be stored?
- What data should be backed up? How often?
- How frequent are backups conducted?
- How quickly can the backups be retrieved in the event of an emergency?
- Who is authorized to retrieve the media?
- How long will it take to retrieve the media?
- Where will the media be delivered?
- Who will restore the data from the media?
- What is the tape-labeling scheme?
- How long will the backup media be retained?
- When the media is stored onsite, what environmental controls are provided to preserve the media?
- What types of tape readers are used at the alternate site?

Backup media should be stored offsite in a secure, environmentally controlled location. When selecting the offsite location, hours of the location, ease of accessibility to backup media, physical storage limitations, and the contract terms should be taken into account. Periodically, media should be retrieved from offsite storage and tested to ensure that the backups are being performed correctly.

Each backup tape, cartridge, or disk should be uniquely labeled to ensure that the required data can be identified quickly in an emergency. This requires that the agency develop an effective marking and tracking strategy. One method might be to label the media by month, day and the year that the backup was created. Other strategies can be more complex, involving multiple sets of tapes that are rotated as old data is either appended to or overwritten. The marking strategy

should be consistent with the tape retention guidelines that dictate how long the media should be stored before it is destroyed.

Though offsite storage of backup tapes enables the system to be recovered, data added to or modified on the server since the previous backup could be lost during a disruption or disaster. To avoid this potential data loss, a backup strategy may need to be complemented by redundancy solutions, such as disk mirroring, RAID, and load balancing. These solutions are discussed below.

RAID provides disk redundancy and fault tolerance for data storage and decreases mean time between failure (MTBF). RAID is used to mask disk drive and disk controller failures. In addition, RAID increases performance and reliability by spreading data storage across multiple disk drives, rather than a single disk. RAID can be implemented through hardware or software, and in either case, the solution appears to the operating system as a single logical hard drive. With a RAID system, hot swappable drives can be used, that is, disk drives can be swapped without shutting down the system when a disk drive fails. RAID technology uses three data redundancy techniques: mirroring, parity, and striping.

- **Mirroring.** With this technique, the system writes the data simultaneously to separate hard drives or drive arrays. The advantages of mirroring are minimal downtime, simple data recovery, and increased performance in reading from the disk. If one hard drive or disk array fails, the system can operate from the working hard drive or disk array, or the system can use one disk to process a read request and use the second disk for a different processing request. The disadvantage of mirroring is that both drives or disk arrays are processing in the writing to disks function, which can hinder system performance. Mirroring has a high fault tolerance and can be implemented through a hardware RAID controller or through the operating system.
- **Parity.** Parity refers to a technique of determining whether data has been lost or overwritten. Parity has a lower fault tolerance than mirroring. The advantage of parity is that data can be protected without having to store a copy of the data, as is required with mirroring. A disadvantage of parity is that the hardware array controller must perform automatic rebuilding. As a result, the parity technique can not be implemented through a software solution.
- **Striping.** Striping improves the performance of the hardware array controller by distributing data across all the drives. In striping, a data element is broken into multiple pieces and a piece is distributed to each hard drive. Data transfer performance is increased using striping because the drives may access each data piece simultaneously. Striping can be implemented in bytes or blocks. Byte-level striping breaks the data into bytes and stores the bytes sequentially across the hard drives. Block-level striping breaks the data into a given size block and each block is distributed to a disk.

RAID solutions rely on mirroring, parity and striping techniques. Currently, five RAID levels are available, with each level providing a different configuration. RAID-1 and RAID-5 are the most popular levels for data redundancy.

- **RAID-0** is the simplest RAID level, relying solely on striping. RAID-0 has a higher performance in read/write speeds than the other levels, but it does not provide data redundancy. Thus, RAID-0 is not recommended as a data recovery solution.
- **RAID-1** uses mirroring, creating and storing identical copies on two drives. RAID-1 is simple and inexpensive to implement; however, 50% of storage space is lost because of data duplication.
- **RAID-2** uses bit-level striping; however, the solution is not often employed because the RAID controller is expensive and difficult to implement.
- **RAID-3** uses byte-level striping with dedicated parity. RAID-3 is an effective solution for applications handling large files; however, fault tolerance for the parity information is not provided because that parity data is stored on one drive.
- **RAID-4** is similar to RAID-3, but it uses block-level rather than byte-level striping. The advantage of this technique is that the block size can be changed to meet the application's needs. With RAID-4, the storage space of one disk drive is lost.
- **RAID-5** uses block-level striping and distributed parity. This solution removes the bottleneck caused by saving parity data to a single disk in RAID-3 and RAID-4. In RAID-5, parity is written across all drives along with the data. Separating the parity information block from the actual data block provides fault tolerance. If one drive fails, the data from the failed drive can be rebuilt from the data stored on the other drives in the array. Additionally, the stripe set can be changed to fit the application's needs. With RAID-5, the storage space of one disk drive is lost.

If a particular RAID level does not meet the system manager's contingency requirements, RAID levels may be combined to derive the benefits of both RAID levels. The most common combination is RAID-0+1 and RAID-1+0. For example, in RAID-0+1, eight hard drives could be split into two separate arrays of four hard drives each. Then, RAID-1 could be applied and the two arrays would be mirrored to provide data redundancy. Thus, the high fault tolerance of RAID-1 is combined with the improved performance speeds of RAID-0. For RAID-1+0, the eight drives would be mirrored to make four sets of two drives a piece, or four mirrored sets. Then, RAID-0 could be applied across all four sets to make a striped array across mirrored sets. However, in both cases, 50% of the possible drive storage space is lost.

RAID is an effective strategy for disk redundancy. However, **redundancy for other critical server parts**, such as the power supply, should be provided as well. The server may be equipped with two power supplies so that the second power supply may continue to support the server if the main power supply becomes overheated or unusable.

While a second power supply can protect against hardware failure, it is not an effective preventive measure against power failure. To ensure short-term power and to protect against power fluctuations, a **UPS** should be installed. The UPS often provides enough backup power to enable the system to shut down gracefully. If high availability is required, a gas- or diesel-powered generator may be needed. The generator can be wired directly into the site's power system and can be configured to start automatically when a power interruption is detected.

Remote journaling and electronic vaulting provide additional data backup capabilities, with backups made to remote tape drives over communication links.²⁸ Remote journaling and electronic vaulting enable shorter recovery times and reduced data loss should the server be damaged between backups. With electronic vaulting, the system is connected to an electronic vaulting provider to allow backups to be created offsite automatically. The electronic vault could use optical disks, magnetic disks, mass storage devices, or an automated tape library as the storage devices. With this technology, data is transmitted to the electronic vault as changes occur on the servers between regular backups. These transmissions between backups are sometimes referred to as electronic journaling.

With remote journaling, transaction logs or journals are transmitted to a remote location. If the server needed to be recovered, the logs or journals may be used to recover transactions, applications, or database changes that occurred after the last server backup. Remote journaling can either be conducted through batches or be communicated continuously using buffering software. Remote journaling and electronic vaulting require a dedicated offsite location to receive the transmissions. The site can be the system's hot site, offsite storage site, or another suitable location. Depending on the volume and frequency of the data transmissions, remote journaling or electronic vaulting could be conducted over a connection with limited bandwidth.

SERVER CONTINGENCY STRATEGIES:

- DOCUMENT SYSTEM AND APPLICATION CONFIGURATIONS
- ENSURE INTEROPERABILITY AMONG COMPONENTS
- APPROPRIATE SECURITY CONTROLS
- SYSTEM BACKUP AND OFFSITE STORAGE
- REDUNDANT ARRAY OF INDEPENDENT DISKS
- REDUNDANCY FOR CRITICAL SERVER PARTS
- UNINTERRUPTIBLE POWER SUPPLY
- REMOTE JOURNALING AND ELECTRONIC VAULTING
- SERVER LOAD BALANCING
- DISK REPLICATION
- STORAGE AREA NETWORKS

Server load balancing increases server and application availability. Through load balancing, traffic can be distributed dynamically across groups of servers running a common application so that no one server is overwhelmed. With this technique, a group of servers appears as a single server to the network. Load balancing systems monitor each server to determine the best path to route traffic to increase performance and availability so that one server is not overwhelmed with traffic. Load balancing can be implemented among servers within a site or among servers in different sites. Using load balancing among different sites can enable the application to continue to operate as long as one or more sites remain operational. Thus, load balancing could be a viable contingency measure depending on system availability requirements.

With **disk replication**, recovery windows are minimized because data is written to two different disks to ensure that two valid copies of the data are always available. The two disks are called the protected server (the main server) and the replicating server (the backup server). Disk replication can be implemented locally or between different locations. Two different data replication techniques are available, and each provides different recovery time objectives (RTOs) and recovery point objectives (RPOs). The RTO is the maximum acceptable length of time that

²⁸ Tom Flesher "Remote Journaling: A New Trend in Data Recovery and Restoration" Contingency Planning & Management. Page 14 – 19, March, 2000.

elapses before the unavailability of the system severely impacts the organization. The RPO is the point in time in which data must be restored in order to resume processing. Disk replication techniques are described below.²⁹

- **Synchronous or Mirroring.** This method uses a disk-to-disk copy and maintains a replica of the database or file system by applying changes to the replicating server at the same time changes are applied to the protected server. The synchronous mode can degrade performance on the protected server and should only be implemented over short physical distances where bandwidth will not restrict data transfers between servers. With synchronous mirroring, the RTO can be minutes to several hours, and the RPO may be reduced to the loss of uncommitted work. Mirroring should be used for critical applications that can accept little or no data loss.
- **Asynchronous or Shadowing.** This technique maintains a replica of the database or file system by continuously capturing changes to a log and applying the changes in the log to the replicating server. With asynchronous shadowing, the RTO can range from hours to a day, depending on the time that is required to implement the changes in the unapplied logs. An acceptable RPO is the last data transfer the mirroring server received. Asynchronous replication is useful over smaller bandwidth connections and longer distances where network latency could occur. As a result, shadowing helps to preserve the protected server's performance.

Replication solutions also can be operating system dependent, called host-based replication, and can use both synchronous and asynchronous replication. To choose the appropriate disk replication technique and product, the system manager should evaluate platform support, integration with other complementary products, cost, speed of deployment, performance impact, and product completeness and manageability.

Disk replication also can act as a load balancer, where traffic is directed to the server with the most resources available. With disk replication, the protected server sends status messages to the replicating server. If the protected server stops replicating, or sends a "distress" call, the replicating machine automatically assumes the protected server's functions. If the replication ceases, a resynchronization will have to be conducted between the protected server and mirroring server before beginning the replication.

If the system manager is considering implementing replication between two sites, the supporting infrastructure for the protected and replicating server also should be considered. Redundant communications paths should be provided if adequate resources are available. The system manager also should be aware of potential disadvantages of disk replication, including the possibility that a corrupted disk or data could be replicated, which could destroy the replicated copy.

A **storage area network (SAN)** is a high-speed, high-performance network that enables computers with different operating systems to communicate with one storage device. With a

²⁹ D. Scott, J. Krischer, J. Rubin. "Research Note: Disaster Recovery: Weighing Data Replication Alternatives" Gartner Group. June 15, 2001

central storage disk, the server is freed from data storage requirements, and its resources may be allocated to other processing needs, such as application processing. As a result, storage capacity can be increased without having to replace or upgrade the server. A SAN can be local or remote (within a limited distance) and usually communicates with the server over a fiber channel. The SAN solution moves away from the server/client architecture and towards a data-centric architecture. Using a SAN enables backup data to be streamed to high-speed tape drives, which does not affect network resources as distributed and centralized back-up architecture does. With the fiber channel connection, backups and mirroring are conducted at over 100 megabits per second (Mbps), allowing for faster recovery times.

5.3 Web Sites

Web sites present information to the public or authorized personnel via the World Wide Web or a private Intranet. An external Web site also may be an electronic commerce (e-commerce) portal, through which the organization may sell products or services over the Internet. A Web site may be used internally within an organization to provide information, such as corporate policies, human resources forms, or a phone directory to its employees.

A *Web site* is used for information dissemination on the Internet or an Intranet. The Web site is created in hypertext mark-up language (HTML) code that may be read by a Web browser on a client machine. A Web site is hosted on a computer (Web server) that serves Web pages to the requesting client browser. The Web server hosts the components of a Web site (e.g. pages, scripts, programs, and multimedia files) and serves them using the hypertext transfer protocol (HTTP). Web sites can present static or dynamic content. A Web site can be either internal to an organization (an Intranet) or be published to the public over the Internet.

5.3.1 *Contingency Considerations*

In addition to the information presented in the server section (Section 5.2), several factors should be considered when determining the Web site recovery strategy. Best practices for Web site contingency planning include the following measures:

- **Document Web site.** Document the hardware, software, and their configurations used to host and create the Web site.
- **Web site programming.** As with other applications, Web sites should undergo thorough testing on test servers prior to production. A configuration management program should be maintained, and changes should be documented appropriately. Approved versions should be recorded on CDs for easy storage.
- **Web site coding.** A Web site is hosted on a server that is assigned an Internet protocol (IP) address. That IP address maps to a domain name, or Uniform Resource Locator (URL) by a Domain Name Server (DNS). Since the IP address and domain name can be assigned randomly, the Web site should not have IP addresses or domain names programmed into the code. If the Web site were recovered at an alternate site, the server could be assigned a different IP address. If the Web site contained hard-coded IP addresses, domain names, or drive letters, system recovery could be delayed.

- **Coordinate Contingency Solutions with Appropriate Network Policy and Security Controls.** A Web site often is the entry point for a hacker into an organization’s network. Thus, the Web server and supporting infrastructure must be protected through strong security controls. Contingency planning measures should be coordinated with these controls to ensure that security is not compromised during system recovery.
- **Coordinate Contingency Solutions with Incident Response Procedures.** Because an external Web site provides an image of the organization to the public, the organization’s public image could be damaged if the Web site were defaced or taken down by a cyber attack. To reduce the consequences of such an attack, contingency solutions should be coordinated closely with incident response procedures designed to limit the impacts of a cyber incident.

5.3.2 Contingency Solutions

Web site contingency solutions should ensure the reliability and availability of the Web site and its resources. Web pages that do not change in content are considered static, while Web pages that change in content are called dynamic pages. Dynamic pages are a result of multiple transactions initiated from either or both the client and the server. The content presented in dynamic pages may be stored on a server other than the Web site, such as a protected server behind a firewall. Thus, when choosing contingency solutions for a Web site, the Web site’s supporting infrastructure must be considered carefully. In addition to servers, the supporting infrastructure also could include the LAN and WAN hosting the Web site.

Due to the amount of requests Web sites could receive and process, load balancing is a popular contingency solution. **Load balancing** uses the cluster approach, in which Web traffic is balanced across at least two servers. Web clustering is not apparent to the user, because it appears as if one server is answering the request. Therefore, if one server were to fail, traffic would be directed to the operational server. Load balancing can be accomplished through two approaches:

WEB SITE CONTINGENCY STRATEGIES:

- DOCUMENT WEB SITE
- CODE/PROGRAM WEB SITE
- PROPERLY
- APPROPRIATE SECURITY CONTROLS
- CONSIDER CONTINGENCIES OF SUPPORTING INFRASTRUCTURE
- LOAD BALANCING
- INCIDENT RESPONSE PROCEDURES

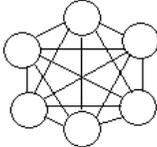
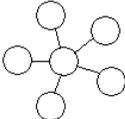
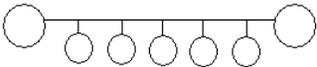
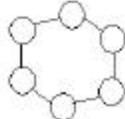
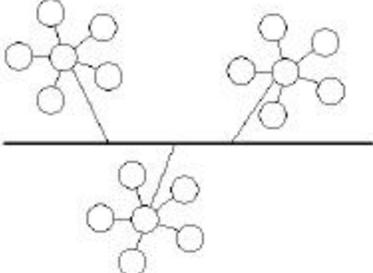
- **DNS.** When a user enters a URL using the Web browser, the request is directed to a DNS server that maps the URL to an IP address. The IP address is assigned to the Web server. The DNS server then directs the request to one of the clustered servers. One common DNS approach is the “round robin” method used by the Berkeley Internet Name Server (BIND).
- **Reverse Proxy.** The reverse proxy approach bundles the requests of the browsers and reduces bandwidth by performing data caching. The proxy server is logically located between the client and the Web server, where it receives client requests and forwards them on to the Web server. The server returns the response to the proxy and the proxy forwards the response to the requesting client. With this method, one IP addresses is needed. To further segment traffic, the servers can be placed on different subnets to prevent a single subnet from being overloaded. In addition, logs can be collected and monitored in one location, which is the reverse proxy. Also, the administrator can determine the delegation

configuration so that if one machine crashes, the delegation configuration of the reverse proxy can be reconfigured so that the crashed server will not return errors to the requesting browser.

5.4 Local Area Networks

A LAN is owned by a single organization; it can be as small as two personal computers attached to a single hub, or it may support hundreds of users and multiple servers. As shown in Table 5-1, several topologies are possible when designing a LAN.

Table 5-1: LAN Topologies³⁰

| Topology | Diagram |
|--|---|
| <p style="text-align: center;">Mesh</p> <p>Networked components are connected with many redundant interconnections between network nodes. In a true mesh topology every node has a connection to every other node in the network.</p> |  |
| <p style="text-align: center;">Star</p> <p>All nodes are connected to a central hub.</p> |  |
| <p style="text-align: center;">Bus</p> <p>All nodes are connected to a central cable, called the bus or backbone.</p> |  |
| <p style="text-align: center;">Ring</p> <p>All nodes are connected to one another in the shape of a closed loop, so that each node is connected directly to two other nodes, one on either side of it.</p> |  |
| <p style="text-align: center;">Tree</p> <p>A hybrid topology where a linear bus backbone connects of star-configured networks.</p> |  |

³⁰ http://www.Webopedia.com/quick_ref/topologies.html

A protocol, an agreed-upon format for transmitting data, facilitates communication between nodes.³¹ The protocol determines how the sending and receiving nodes format the data packet. Two main network standards may be implemented on a LAN:

- **Ethernet.** Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps, 100 Mbps, or at gigabit speeds. It is one of the most widely implemented LAN standards.
- **Token Ring.** Token ring is a type of network in which all the computers are arranged (schematically) in a circle. A token, which is a special bit pattern, travels around the circle. To send a message, a computer catches the token, attaches a message to it, and then lets it continue to travel around the network to the destination host.

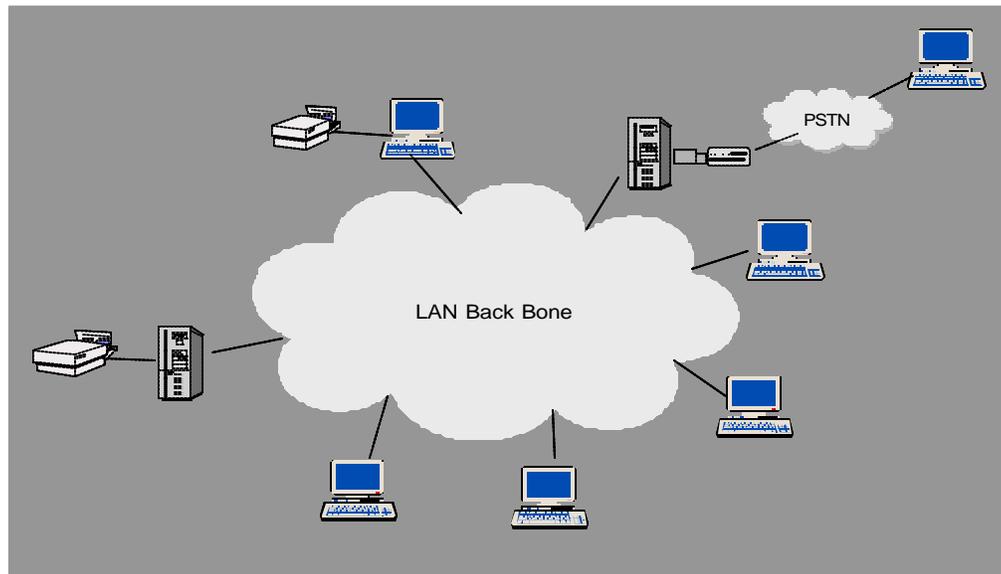
LANs can also be implemented in two main architectures:

- **Peer-to-Peer.** In a peer-to-peer network, each node has equivalent capabilities and responsibilities. For example, five personal computers can be networked through a hub to share data.
- **Client/Server.** In a client/server network, each node on the network is either a client or a server. A client can be a personal computer or a printer where a client relies on a server for resources.

A LAN's topology, protocol, architecture, and nodes will vary depending on the organization. Thus, contingency solutions for each organization will be different. The example LAN presented in Figure 5-2 depicts a network with a client/server architecture and a star topology running the Ethernet protocol. The LAN consists of five desktop computers, one server, one networked printer, one local desktop printer, and dial-in access over the public switched telephone network to the server.

³¹ <http://www.Webopedia.com/TERM/p/protocol.html>

Figure 5-2: Local Area Network



5.4.1 Contingency Considerations

When developing the LAN recovery strategy, the system manager should follow the information presented earlier in Section 5, regarding desktops, servers, and Web sites. In addition, the following best practices should be considered:

- **Document LAN.** A LAN diagram should be up-to-date. Cable jack numbers should be documented, and all nodes should be included on the diagram. The physical diagram depicting and cable drops complements the logical diagram of the LAN and its nodes. Both diagrams help recovery personnel to restore LAM services more quickly.
- **Document Systems Configurations and Vendors.** Document configurations network connective devices that facilitate LAN communication (e.g. switches, bridges, hubs) to ease recovery. Vendors and their contact information should be documented in the contingency plan to provide for prompt hardware and software resupply.
- **Coordinate with Network Security Policy and System Security Controls.** LAN contingency solutions should be coordinated with network security policies to protect against threats that could disrupt the network.

5.4.2 Contingency Solutions

When developing the LAN contingency plan, the system manager should identify **single points of failure** that affect critical systems or processes. This analysis could include threats to the **cabling system**, such as cable cuts, electromagnetic and radio frequency interference, and damage caused by fire, water, and other hazards. As a solution, redundant cables may be installed when appropriate. For example, it might not be cost effective to install duplicate cables

to desktops. However, it may be cost effective to install a 100 megabit cable between floors so that hosts on both floors may be reconnected if the primary cable is cut.

Often, it is not cost-effective to run duplicate cables to each jack. However, each desktop jack usually is equipped with at least one phone jack and computer jack. When cables are installed, an organization may choose to install an extra data or phone jack every few drops, so that if a problem does occur in a cable run, an extra jack within a short distance would be available as backup. In this case, temporary cable can be run from the desktop to the extra jack to provide connectivity for the desktop until a new cable can be run to the problem jack. Also, if the phone system's connectivity block is located in the same location as the backbone hubs, a phone jack can be converted easily into a data jack, if the phone jack provides the appropriate bandwidth.

Contingency planning also should consider **network connecting devices**, such as hubs, switches, routers and bridges. The BIA should characterize the roles that each device serves in the network, and a contingency solution should be developed for each device based on its BIA criticality. As an example of a contingency strategy for network connecting devices, redundant intelligent network routers may be installed in a network, enabling a router to assume the full traffic workload if the other router were to fail. As another example, spare network hubs could replace a failed switch until the switch could be replaced.

Remote access is a service provided by servers and devices on the LAN. Remote access provides a convenience for users working offsite or allows for a means for servers and devices to communicate between sites. Remote access can be conducted through various methods, including dial-up access and virtual private network (VPN). In the event of an emergency or serious system disruption, remote access may serve as an important contingency capability by providing access to organization-wide data for recovery teams or users from another location. If remote access is established as a contingency strategy, data bandwidth requirements should be identified and used to scale the remote access solution.

- LAN CONTINGENCY STRATEGIES:
- DOCUMENT LAN
 - COORDINATE WITH VENDORS
 - APPROPRIATE SECURITY CONTROLS
 - IDENTIFY SINGLE POINTS OF FAILURE
 - CABLING SYSTEM
 - NETWORK CONNECTING DEVICES
 - REMOTE ACCESS
 - WIRELESS LOCAL AREA NETWORK
 - MONITORING SOFTWARE

Wireless local area networks also can serve as an effective contingency solution to restore network services following a wired LAN disruption. Wireless networks do not require the cabling infrastructure of conventional LANs; therefore, they may be installed quickly as an interim or permanent solution. However, wireless networks broadcast the data over a radio signal, enabling the data to be intercepted. When implementing a wireless network, security controls, such as data encryption, should be implemented if the communications traffic contains sensitive information.

To reduce the effects of a LAN disruption through prompt detection, **monitoring software** can be installed. The monitoring software issues an alert if a node begins to fail or is not responding. The monitoring software can facilitate troubleshooting and often provides the administrator with a warning before users and other nodes notice problems. Many types of monitoring software

may be configured to send an electronic page to a designated individual automatically when a system parameter falls out of its specification range.

5.5 Wide Area Networks

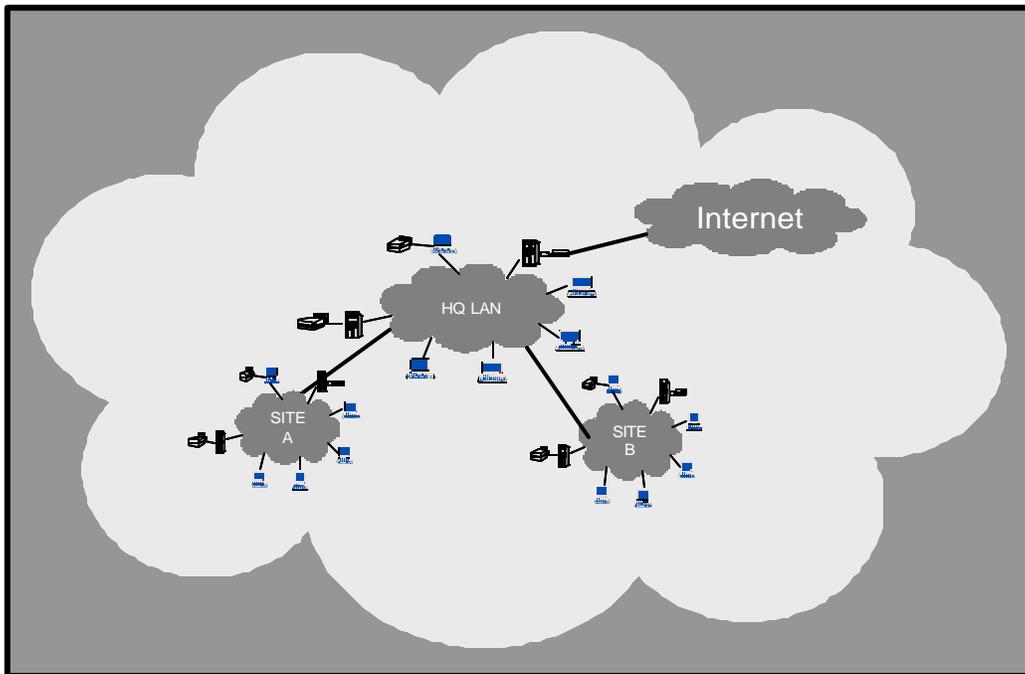
A *Wide Area Network (WAN)* is a data communications network that consists of two or more local area networks that are dispersed over a wide geographical area. Communications links, usually provided by a public carrier, enable a one local area network to interact with other local area networks.

In addition to connecting LANs, a WAN also can connect to another WAN, or it can connect a LAN to the Internet. Types of WAN communication links include the following methods:

- **Dial-up.** Dial-up connections over modems can provide minimal data transfer over a non-permanent connection. The speed will depend on the modems used, up to 56 kilobits per second (Kbps).
- **ISDN.** Integrated services digital network (ISDN) is an international communications standard for sending voice, video, and data over digital or standard telephone wires. ISDN supports data transfer rates of 64 or 128 Kbps.
- **T-1.** T-1 is a dedicated phone connection supporting data rates of 1.544 Mbps. A T-1 line consists of 24 individual 64 Kbps channels, and each channel can be configured to carry voice or data signals. Fractional T-1 access also can be provided when multiples of 64Kbps lines are required.
- **T-3.** T-3 is a dedicated phone connection supporting data rates of about 43 Mbps. A T-3 line consists of 672 individual channels, each of which supports 64 Kbps. T-3 is also referred to as DS3.
- **Frame Relay.** Frame relay is a packet-switching protocol for connecting devices on a WAN. In frame relay, data is routed over virtual circuits. Frame relay networks support data transfer rates at T-1 and T-3 speeds.
- **ATM.** Asynchronous Transfer Mode (ATM) is a network technology that transfers data at high speeds using packets of fixed size. Implementations of ATM support data transfer rates of from 25 to 622 Mbps.
- **SONET.** Synchronous Optical Network (SONET) is that standard for synchronous data transmission on optical media. SONET supports gigabit transmission rates.
- **Wireless.** A wireless LAN bridge can connect multiple LANs to form a WAN. Wireless supports distances of 20 to 30 miles with a direct line of sight.
- **VPN.** The VPN uses public telephone wires to send encrypted data between nodes via the Internet.

Figure 5-3 depicts a corporate WAN, linking the Headquarters LAN to two satellite LANs. The WAN also maintains a link to the Internet.

Figure 5-3:WAN Diagram



5.5.1 Contingency Considerations

WAN contingency considerations should enhance the ability of recovery personnel to restore WAN services after a disruption. The best practices listed below complement the WAN recovery strategies in Section 5.5.2 to create a more comprehensive WAN contingency capability.

- **Document WAN.** The WAN architecture diagram should be kept up-to-date and should identify network connecting devices, unit addresses (IP addresses), and types of communication links and vendors.
- **Document Systems Configurations and Vendors.** Document configurations media access unit devices that facilitate WAN communication to ease recovery. The contingency plan should include a vendor list to enable rapid replacement of hardware, software, and other WAN components following a disruption. The plan also should document the communications providers, including POC and contract information.
- **Coordinate with Network Security Policy and System Security Controls.** WAN contingency solutions should be coordinated with network security policies to protect against threats that could compromise network availability.

WAN CONTINGENCY STRATEGIES:

- DOCUMENT WAN
- COORDINATE WITH VENDORS
- APPROPRIATE SECURITY CONTROLS
- SINGLE POINTS OF FAILURE
- REDUNDANT COMMUNICATION LINKS
- REDUNDANT NETWORK CONNECTING DEVICES
- REDUNDANT NSPs AND ISPs
- SERVICE LEVEL AGREEMENTS
- INTERNET CONNECTION

5.5.2 Contingency Solutions

WAN contingency solutions include all of the measures discussed for personal computers, servers, Web sites, and LANs. Additionally, WAN contingency planning must consider the communications links that connect the disparate LANs. Also, WAN contingency strategies are influenced by the type of data routed on the network. A WAN that hosts a mission-critical distributed system (see Section 5.6) may require more robust recovery strategy than a WAN that connects multiple LANs for simple resource sharing purposes. Organizations should consider the following contingency solutions for ensuring WAN availability:

- **Redundant Communications Links.** Redundant communications links usually are necessary when the network processes critical data. The redundant links could be the same type, such as two T-1s connections, or the backup link could provide reduced bandwidth to accommodate only critical transmissions in a contingency situation. For example, an ISDN line could be used as a contingency communications link for a primary T-1 connection. If redundant links are used, the system manager should ensure that the links have physical separation and do not follow the same path; otherwise, a single incident, such as a cable cut, could disrupt both links.
- **Redundant Network Service Providers.** If 100 percent data availability is required, redundant communications links can be provided through multiple Network Service Providers (NSP). If this solution is chosen, the manager should ensure the NSPs do not share common facilities at any point, including building entries or demarcations.
- **Redundant Network Connecting Devices.** Duplicate network connecting devices can provide redundancy and load balancing in routing traffic, creating high availability at the LAN interfaces.
- **Redundancy from NSP or Internet Service Provider.** The system manager should consult with the selected NSP or Internet Service Provider (ISP) to assess the robustness and reliability within their core networks (e.g., redundant network connecting devices and power protection).
- **Institute SLAs.** SLAs can facilitate prompt recovery following software or hardware problems associated with the network. A SLA also may be developed with the NSP or ISP to guarantee the desired network availability and establish tariffs should the vendor's network be unavailable. If the NSP or ISP is contracted to provide network connecting devices, such as routers, the availability of these devices should be included in the SLA.

To provide further redundancy, independent Internet connections may be established from two geographically separated LANs. If one connection were to fail, Internet traffic could be routed through the remaining connection. However, this strategy highlights the balance that must be maintained between security and availability. Multiple Internet connections increase a network's vulnerability to hackers. Therefore, as emphasized previously, contingency strategies must be weighed against security considerations at all times.

5.6 Distributed System

Distributed systems are implemented in environments in which clients and users are widely dispersed. These systems rely on LAN and WAN resources to facilitate user access, and the elements comprising the distributed system require synchronization and coordination to prevent disruptions and processing errors. A common form of distributed systems is a large database management system (DBMS) that supports agency-wide business functions in multiple geographic locations. In this type of application, data is replicated among servers at each of the locations, and users access the system from their local server.

A *distributed system* is an interconnected set of multiple autonomous processing elements, configured to exchange and process data to complete a single business function. To the user, a distributed system appears to be a single source. Distributed systems use the client-server relationship model to make the application more widely accessible to users in different locations.

5.6.1 *Contingency Considerations*

Contingency considerations for the distributed system draw on the concepts discussed for the previous platforms. Because the distributed system relies extensively on local and wide area network connectivity, distributed system contingency measures are similar to those discussed for LANs and WANs.

- **Standardize Hardware, Software, and Peripherals.** System recovery may be expedited if hardware, software, and peripherals are standardized throughout the distributed system. Recovery costs may be reduced, because standard configurations may be designated and resources may be shared. Standardized components also reduce system maintenance across the organization.
- **Document Systems Configurations and Vendors.** Document the distributed system's architecture and the configurations of its various components. Also, the contingency plan should identify vendors and model specifications to facilitate rapid equipment replacement after a disruption.
- **Coordinate with Network Security Policy and System Security Controls.** Distributed system contingency solutions should be coordinated with network security policies to protect against threats that could compromise its availability.

DISTRIBUTED SYSTEM CONTINGENCY STRATEGIES:

- STANDARDIZE COMPONENTS
- DOCUMENT SYSTEM
- COORDINATE WITH VENDORS
- APPROPRIATE SECURITY CONTROLS
- SERVER CONTINGENCIES
- LAN CONTINGENCIES
- WAN CONTINGENCIES

5.6.2 *Contingency Solutions*

Because a distributed system spans multiple locations, risks to the system and its supporting infrastructure should be analyzed thoroughly in the BIA process. As discussed above, distributed system contingency strategies typically reflect the system's reliance on LAN and WAN availability. Based on this fact, when developing a distributed system contingency

strategy, the following technologies should be considered, as they were addressed for LANs and WANs:

- System backups
- RAID
- Redundancy of critical system components
- Electronic vaulting and remote journaling
- Disk replication
- SAN
- Remote access
- Wireless networks
- LAN cabling system redundancy
- WAN communication link redundancy.

Contingency solutions may be built into the distributed system during design and implementation. A distributed system may be constructed so that all data resides in one location (such as the organization's headquarters) and is replicated to the local sites. Changes at local sites could be replicated back to headquarters. If data is replicated to the local sites as read-only, the data in the distributed system is backed up at each local site. This means that if the headquarters server were to fail, data could still be accessed at the local sites over the WAN. Conversely, if data were uploaded from local sites to the headquarters' site hourly, then the headquarters' server would act as a backup for the local servers.

As the example above illustrates, the distributed system typically provides some inherent level of redundancy that can be incorporated in the contingency strategy. For example, consider a critical system that is distributed between an agency headquarters and a small office. Assuming data is replicated at both sites, a cost-effective recovery strategy may be to establish a reciprocal agreement between the two sites. Under this agreement, in the event of a disruption at one office, essential personnel would relocate to the other office to continue to process system functions. This strategy could save significant contingency costs by avoiding the need to procure and equip alternate sites.

5.7 Mainframe Systems

Unlike the client/server architecture, the mainframe architecture is centralized. The clients that access the mainframe are “dumb” terminals with no processing capabilities. The dumb terminals accept output only from the CPU or mainframe. However, personal computers also can access a mainframe by using terminal emulation software.

A *mainframe* is a multi-user computer designed to meet the computing needs of a large organization. The term was created to describe the large central computers developed in the late 1950s and 1960s to process bulk accounting and information management functions. Mainframe systems store all data in a central location rather than dispersing data among multiple machines, as with distributed systems.

5.7.1 *Contingency Considerations*

Although the mainframe computer is large and more powerful than the platforms discussed previously, it shares many of the same contingency requirements. Because a mainframe uses a centralized architecture, the mainframe does not have the inherent redundancy that a distributed system or network provides. As a result, mainframe availability and data backups are critical. The following measures should be considered when determining mainframe contingency requirements:

- **Store backup tapes offsite.** Backup tapes should be stored offsite in a secure, environmentally controlled facility. The storage facility should be located far enough away from the original site to reduce the likelihood that both sites would be affected by the same event.
- **Document system configurations and vendors.** Maintaining detailed records of system configurations enhances system recovery capabilities. Additionally, vendors that supply essential hardware, software, and other components should be identified in the contingency plan.
- **Coordinate with Network Security Policy and System Security Controls.** Mainframe contingency solutions should be coordinated with network security policies, such as stringent access controls. Network security controls can help protect against attacks that could compromise the mainframe’s availability.

5.7.2 *Contingency Solutions*

Mainframes require different contingency strategies than distributed systems because data is stored in a single location. Contingency strategies should emphasize the mainframe’s data storage capabilities and underlying architecture. **Redundant system components** are critical to ensure that a failure of a system component, such as a power supply, does not cause a system failure. Also, UPS and power monitoring and management systems should be used to ensure power fluctuation will not affect the mainframe. Because mainframes typically process large, critical applications, a **long-term backup power** solution may be needed. A gas- or diesel-generator can ensure that mainframe processing is not interrupted by a power outage.

Disk redundancy can be provided for the disk access storage devices (DASD) by implementing a RAID solution.³²

Because each mainframe architecture is unique and centralized, the common contingency strategy is to have a replacement system available at an alternate warm or hot site. However, backup mainframe platforms are very costly to purchase and maintain. Agencies also typically maintain vendor support contracts to repair the damaged unit. However, vendor support alone may not restore system functions within the allowable outage time.

MAINFRAME CONTINGENCY STRATEGIES:

- BACKUPS AND OFFSITE STORAGE
- DOCUMENT SYSTEM
- COORDINATE WITH VENDORS
- APPROPRIATE SECURITY CONTROLS
- REDUNDANT SYSTEM COMPONENTS
- HOT SITE/RECIPROCAL AGREEMENT
- VENDOR SERVICE LEVEL AGREEMENTS
- BACKUPS
- DISK REPLICATION
- ELECTRONIC VAULTING/REMOTE JOURNALING

For some agencies a possible alternative may be a **reciprocal agreement** with an alternate site that operates an identical mainframe system. In all cases, **vendor service level agreements** should be kept up to date and reviewed to ensure that the vendor provides adequate support to meet system availability requirements.

Mainframes should be **backed up** on a regular basis and backup media should be stored offsite. Backup schedules should be based on the criticality of the data being processed, as well as the frequency that the data is modified. (See Section 5.2.2 for backup solutions.) As with servers, **remote journaling or electronic vaulting** to the alternate site could be an effective technical contingency solution. Additionally, **disk replication** or **SAN** technologies that replicate various platforms to one replicating server could be used in some cases.

³² RAID levels are discussed in detail in Section 5.3.3.

6. SUMMARY

The IT Contingency Planning Guide provides instructions, recommendations, and considerations for government IT contingency planning. Contingency planning refers to interim measures to recover IT services after an emergency or system disruption. Interim measures may include relocation of IT systems and operations to an alternate site, recovery of IT functions using alternate equipment, or performance of IT functions using manual methods. The information presented in this document addresses 8 IT platform types:

- Desktops and portable systems
- Servers
- Web sites
- Servers
- Local area networks
- Wide area networks
- Distributed systems
- Mainframe systems.

The document defines the following 7-step contingency process that an agency may apply to develop and maintain a viable contingency planning program for their IT systems. These 7 steps are designed to be integrated into each stage of the computer system life cycle.

- **Develop contingency planning policy.** A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan
- **Conduct the business impact analysis.** The BIA helps to identify and prioritize critical IT systems and components
- **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs
- **Develop recovery strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption
- **Develop contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system
- **Test, train, and exercise the plan.** Testing the plan identifies planning gaps, while training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness
- **Maintain the plan.** The plan should be a living document that is updated regularly to remain current with system enhancements.

The document presents a sample format for developing an IT contingency plan. The format defines three phases that govern actions taken following a system disruption. The

Notification/Activation Phase describes the process to notify recovery personnel and perform a damage assessment. The **Recovery** Phase discusses actions taken by recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities. The final phase, **Reconstitution**, outlines actions taken to return the system to normal operating conditions.

If a system cannot be recovered at the original site, in most cases it must be relocated to an alternate site for temporary processing. The planning guide discusses various types of alternate sites and their respective capabilities. These sites include:

- Cold sites
- Mobile sites
- Warm sites
- Hot sites
- Mirrored sites.

This document provides specific contingency planning recommendations and best practices for the 8 IT platforms. However, several strategies or techniques discussed in this guide are common to all IT systems. Some common contingency strategies include:

- **Offsite storage.** System information should be backed up regularly and stored offsite in a protected environment. The document describes several techniques for performing backup operations. Operating system, application, and application data should be backed up based on system and data criticality. Software licenses, system configurations, and other vital records should be stored offsite with the backup data
- **Interoperability.** Providing standard platforms and configurations assist system recovery and reduce expenses associated with procuring replacement equipment
- **Redundancy.** Redundant data storage, communications paths, power sources, and system components reduce the likelihood of system failure. The costs of implementing redundant capabilities should be weighed against the risks of system outage
- **Coordination with security controls.** Contingency planning cannot be conducted in a vacuum. Contingency strategies must be coordinated closely with existing and proposed security controls to reduce system risks and ensure viable contingency capabilities.

LIST OF APPENDIXES

Appendix A: Sample IT Contingency Plan Format

Appendix B: Sample Business Impact Analysis Template

Appendix C: Glossary

Appendix D: References

APPENDIX A: SAMPLE IT CONTINGENCY PLAN FORMAT

This sample format provides a template for preparing an actual IT contingency plan. The template is intended to be used as a guide, and the system manager should modify the format as necessary to meet the system's contingency requirements and comply with internal policies. Where practical, the guide provides instructions for completing specific sections. Text is added in certain sections; however, this information is intended only to suggest the type of information that may be found in that section. The text is not comprehensive and should be modified to meet specific agency and system considerations.

1. Introduction

1.1. Purpose

This *{system name}* Contingency Plan establishes procedures to recover the *{system name}* following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
 - *Notification/Activation phase* to detect and assess damage and to activate the plan
 - *Recovery phase* to restore temporary IT operations and recover damage to the original system
 - *Reconstitution phase* to restore IT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out *{system name}* processing requirements during prolonged interruptions to normal operations
- Assign responsibilities to designated the *{Organization name}* personnel and provide guidance for recovering *{system name}* during prolonged periods of interruption to normal operations
- Ensure coordination with other *{Organization name}* staff who will participate in the contingency planning strategies. Ensure coordination with external points-of-contact and vendors who will participate in the contingency planning strategies.

1.2. Scope

1.2.1. Applicability

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles—

- *The {Organization name}'s facility in City, State is inaccessible; therefore, {Organization name} is unable to perform {system name} processing for the Department.*
- *A valid contract exists with the Alternate site that designates that site in City, State, as the {Organization name}'s alternate operating facility.*

- *{Organization name}* will use the *Alternate site* building and information technology resources to *recover {system name} functionality* during an emergency situation that prevents access to the *original facility*.
- The designated computer system at the *Alternate site* has been configured to begin processing *{system name} information*.
- The *Alternate site* will be used to continue *{system name}* recovery and processing throughout the period of disruption, until the return to normal operations.

1.2.2. Assumptions

Based on these principles, the following assumptions were used when developing the IT Contingency Plan—

- The *{system name}* is inoperable at the *{Organization name}* computer center and cannot be recovered within *48 hours*
- Key *{system name}* personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the *{system name}* Contingency Plan
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster
- Computer center equipment, including components supporting *{system name}*, are connected to an uninterruptible power supply (UPS) that provides *45 minutes to 1 hour* of electricity during a power failure
- *{system name}* hardware and software at the *{Organization name}* *original site* are unavailable for at least *48 hours*
- Current backups of the application software and data are intact and available at the *Offsite storage facility*
- The equipment, connections, and capabilities required to operate *{system name}* are available at the *Alternate site* in *City, State*
- Service agreements are maintained with *{system name}* hardware, software, and communications providers to support the emergency *system* recovery.

The *{system name}* Contingency Plan does not apply to the following situations:

- Overall recovery and continuity of business operations. The Business Resumption Plan and Continuity of Operations Plan (COOP) are appended to the plan
- Emergency evacuation of personnel. The Occupant Evacuation Plan is appended to the plan
- *Any additional constraints should be to this list.*

1.3. Authority/References

This *{system name}* Contingency Plan complies with the *{Organization name}*'s IT contingency planning policy as follows:

“The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, the recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.”

The *{system name}* Contingency Plan also complies with the following Federal and departmental policies:

- The Computer Security Act of 1987
- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, November 2000.
- Federal Information Processing Standards Publication (FIPS PUB) 87, *Guidelines for ADP Contingency Planning*, March 1981
- Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations*, July 1999
- Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government Operations*, October 1998
- PDD 63, *Critical Infrastructure Protection*, May 1998
- The Federal Response Plan (FRP), April 1999
- *Any other applicable Federal policies should be added*
- *Any other applicable departmental policies should be added.*

2.2. Responsibilities

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Contingency Plan establishes several teams assigned to participate in recovering *{system name}* operations. The *{team name}* is responsible for recovery of the *{system name}* computer environment and all applications. Members of the *team name* include personnel who are also responsible for the daily operations and maintenance of *{system name}*. The *team leader title* directs the *{team name}*.

Continue to describe each team, their responsibilities, leadership and coordination with other applicable teams during a recovery operation.

The relationships of the team leaders involved in *system* recovery and their member teams are depicted in the figure below.

(Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel.)

Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.

3. Notification and Activation Phase

This phase addresses the initial actions taken to detect, and assess damage inflicted by a disruption to *{system name}*. Based on the assessment of the event, the plan may be activated by the *system manager*.

In an emergency, the *{Organization name}*'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in Appendix A. The notification sequence is listed below:

- The first responder is to notify the *system manager*. All known information must be relayed to the *system manager*
- The *systems manager* is to contact the *Damage Assessment Team Leader* and inform him/her of the event. The *system manager* is to instruct the *Team Leader* to begin assessment procedures
- The *Damage Assessment Team Leader* is to notify team member and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment can not be performed locally because of unsafe conditions, the *Damage Assessment Team* is to follow the also outlined below

Damage Assessment Procedures:

(Detailed procedures should be outlined to include activities to determine the cause of the disruption, potential for additional disruption or damage, affected physical area and status of physical infrastructure, status of IT equipment functionality and inventory, including items that will need to be replaced, and estimated time to repair services to normal operations.)

- Upon notification from the *system manager* the *Damage Assessment Team Leader* is to ...
- *Damage Assessment Team* is to

Alternate Assessment Procedures

- Upon notification from the *system manager* the *Damage Assessment Team Leader* is to ...
- *Damage Assessment Team* is to
 - When damage assessment has been completed, the *Damage Assessment Team Leader* is to notify the *system manager* of the results
 - The *system manager* is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required

The Contingency Plan is to be activated if one or more of the following criteria are met:

1. *{system name}* will be unavailable for more than 48 hours
 2. *facility is damaged and will be unavailable for more than 24 hours*
 3. *other criteria, as appropriate*
- If the plan is to be activated, the *system manager* is to notify all necessary Team Leaders and inform them of the details of the event and if relocation is required
 - Upon notification from the *system manager*, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary
 - The *system manager* is to notify the *Offsite storage facility* that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the *Alternate site*
 - The *system manager* is to notify the *Alternate site* that a contingency event has been declared and to prepare the facility for the *Organization's* arrival.

4. Recovery Operations

This section provides procedures for recovering the application at the alternate site while other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the *{system name}* at the *Alternate Site*. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal. *State the first recovery objective as determined by the BIA. For each team responsible to execute a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
 - *Team Recovery Procedures*
- *{team name}*
 - *Team Recovery Procedures*
- *{team name}*
 - *Team Recovery Procedures*

Recovery Goal. *State the second recovery objective as determined by the BIA. For each team responsible to execute a function to meet this objective, state the team names and list their respective procedures.*

- *{team name}*
 - *Team Recovery Procedures*
- *{team name}*
 - *Team Recovery Procedures*
- *{team name}*
 - *Team Recovery Procedures*

Recovery Goal. *State remaining recovery objectives (as determined by the BIA). For each team responsible to execute a function to meet this objective, state the team names and list their respective procedures.*

5. Return to Normal Operations

This section discusses activities necessary for restoring *{system name}* operations at the *{Organization name}*'s original site. When the computer center at the original sites has been restored, *{system name}* operations at the *Alternate site* must be transitioned back to the original site. The goal is to provide a seamless transition of operations from the *Alternate site* to the computer center.

Original Site Restoration

Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred back. IT equipment and telecommunications connections should be tested.

- {team name}
 - *Team Resumption Procedures*
- {team name}
 - *Team Resumption Procedures*

5.1. Concurrent Processing

Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original site. These procedures should include testing the original system until it is functioning properly and the contingency system is shut down gracefully.

- {team name}
 - *Team Resumption Procedures*
- {team name}
 - *Team Resumption Procedures*

5.2. Plan Deactivation

Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organization, with special attention paid to handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate locations. Team members should be instructed to return to the original site.

- {team name}
 - *Team Testing Procedures*
- {team name}
 - *Team Testing Procedures*

6. Plan Appendices *The appendices included should be based on system and plan requirements.*

- *Personnel Contact List*
- *Vendor Contact List*
- *Equipment & Specifications*
- *Service Level Agreements & Memorandums of Understanding*

- *IT Standard Operating Procedures*
- *Business Impact Analysis*
- *Related Contingency Plans*
- *Emergency Management Plan*
- *Occupant Evacuation Plan*
- *Continuity of Operations Plan*

APPENDIX B: SAMPLE BUSINESS IMPACT ANALYSIS AND BIA TEMPLATE

In this example, an agency maintains a small field office with a local area network that supports approximately 50 users. The office relies on the LAN and its components for standard automated processes, such as developing and using spreadsheets, word processing, and e-mail. The office also maintains a customized database application that supports Inventory, a key resource management process. The network manager is responsible for developing a LAN contingency plan and begins with the BIA.³³ The LAN includes the following components:

- Authentication/network operating system server
- Database server (supports customized Inventory database application)
- File server (stores general, non-Inventory files)
- Application server (supports office automation software)
- Networked printer
- E-mail server and application
- 50 desktop computers
- 5 hubs.

The system manager begins the BIA process by identifying the network stakeholders. In this case, the manager identifies and consults with the following individuals:

- Field office manager
- Inventory process manager
- Sampling of network users
- System administrators for each network server.

Based on subsequent discussions, the network manager learns the following information:

- The Inventory system is critical to the parent agency's master resource management operations; the system provides updated data to the larger system at the end of each business day. If the system were unavailable for more than one working day (8 hours), significant business impacts would result at the parent agency. Inventory requires a minimum of 5 personnel with desktop computers and access to the system database to process data
- Other non-Inventory processes may be considered non-critical and could be allowed to lapse for up to 10 days
- The field office manager and Inventory manager indicate that e-mail is an essential service; however, staff can operate effectively without e-mail access for up to 3 days

³³ Although the LAN connects to the agency WAN, because the plan scope is limited to the local network, WAN components are not addressed here.

- Staff could function without access to the spreadsheet application for up to 15 working days without impacting business processes significantly
- Word processing access would need to be restored within working 5 days; however, individuals could use manual processes for up to 10 days if the required forms were available in hard-copy format
- Outputs from the day's Inventory system records normally are printed daily; the data to be printed may be stored on any desktop computer used by the Inventory system staff. In an emergency, the Inventory system output could be transmitted electronically via e-mail, for up to 4 days before significantly impacting business operations. Other printing functions would not be considered essential and could be unavailable for up to 10 days with no impact on business functions.

Based on the information gathered in discussions with stakeholders, the system manager follows the 3-step BIA process to identify critical IT resources, identify outage impacts and allowable outage times, and develop recovery priorities.

Identify critical IT resources

The manager identifies the following resources as critical, meaning that they support critical business processes:

- Authentication/network operating system server (required for users to have LAN access)
- Database server (required to process the Inventory system)
- E-mail server and application
- Five desktop computers (to support 5 Inventory users)
- One hub (to support 5 Inventory users)
- Network cabling
- Electric power.

Identify Outage Impacts and Allowable Outage Times

Next, the manager determines outage impacts and allowable outage times for the critical resources:

| Resource | Outage Impact | Allowable Outage Time |
|-----------------------|---|------------------------------|
| Authentication server | Users could not access Inventory system | 8 hours |
| Database server | Users could not access Inventory system | 8 hours |
| E-mail server | Users could not send e-mail | 2 days |
| 5 desktop computers | Users could not access Inventory system | 8 hours |
| Hub | Users could not access Inventory system | 8 hours |
| Network cabling | Users could not access Inventory system | 8 hours |
| Electric power | Users could not access Inventory system | 8 hours |
| Printer | Users could not produce Inventory reports | 4 days |

Develop Recovery Priorities

Using the table completed in the previous step, the system manager develops recovery priorities for the system resources. The manager uses a simple high, medium, low scale to prioritize the resources. High priorities are based on the need to restore critical resources within their allowable outage times; medium and low priorities reflect the requirement to restore full operational capabilities over a longer recovery period.

| Resource | Recovery Priority |
|----------------------------------|--------------------------|
| Authentication server | High |
| Database server | High |
| 5 desktop computers | High |
| 1 hub | High |
| Network cabling | High |
| Electric power | High |
| E-mail server | Medium |
| Printer | Medium |
| Remaining desktop computers (45) | Low |
| Remaining hubs (4) | Low |

Having completed the BIA, the system manager may use the recovery priority information above, the system manager to develop recovery strategies that enable the network to be recovered in a prioritized manner, with all system resources being recovered within their respective allowable outage times.

A template for completing the BIA is provided on the following page.

Business Impact Analysis (BIA) Template

This sample template is designed to assist the user in performing a BIA on an IT system. The BIA is an essential step in developing the IT contingency plan. The template is meant only as a basic guide and may not apply to all systems. The user may modify this template or the general BIA approach as required to best accommodate the specific system.

Preliminary System Information

| | |
|--|--|
| Organization: | Date BIA completed: |
| System Name: | BIA POC: |
| System Manager or POC: | |
| System Description: <i>{Discussion of the system purpose, architecture, including system diagrams}</i> | |
| A. System Stakeholders | Role |
| Internal {Identify the individuals, positions, or offices <i>within</i> your organization that depend on or support the system; also specify their relationship to the system} | |
| <ul style="list-style-type: none"> ▪ ▪ | <ul style="list-style-type: none"> ▪ ▪ |
| External {Identify the individuals, positions, or offices <i>outside</i> of your organization that depend on or support the system; also specify their relationship to the system} | |
| <ul style="list-style-type: none"> ▪ ▪ | <ul style="list-style-type: none"> ▪ ▪ |
| B. System Resources <i>{Identify the specific hardware, software, and other resources that comprise the system; include quantity and type}</i> | |
| Hardware | |
| <ul style="list-style-type: none"> ▪ ▪ | |
| Software | |
| <ul style="list-style-type: none"> ▪ ▪ | |
| Other resources | |
| <ul style="list-style-type: none"> ▪ ▪ | |

C. Identify critical roles {List the roles identified in Section A that are deemed critical}

| |
|--|
| <ul style="list-style-type: none"> ▪ ▪ ▪ ▪ |
|--|

D. Link critical resources to critical roles {Identify the IT resources needed to accomplish the roles listed in Section C}

| Critical Role | Resources |
|---------------|--|
| | <ul style="list-style-type: none"> ▪ ▪ |
| | <ul style="list-style-type: none"> ▪ ▪ |
| | <ul style="list-style-type: none"> ▪ ▪ |

E. Identify Outage Impacts and Allowable Outage Times {Characterize the impact on critical roles if a critical resource is unavailable; also, identify the maximum acceptable period that the resource could be unavailable before unacceptable impacts resulted}

| Resource | Outage Impact | Allowable Outage Time |
|----------|--|--|
| | <ul style="list-style-type: none"> ▪ ▪ | <ul style="list-style-type: none"> ▪ ▪ |
| | <ul style="list-style-type: none"> ▪ ▪ | <ul style="list-style-type: none"> ▪ ▪ |
| | <ul style="list-style-type: none"> ▪ ▪ | <ul style="list-style-type: none"> ▪ ▪ |

D. Prioritize resource recovery {List the priority associated with recovering a specific resource, based on the outage impacts and allowable outage times provided in Section E. Use quantitative or qualitative scale (e.g. high/medium/low, 1-5, A/B/C)}

| Resource | Recovery Priority |
|----------|-------------------|
| | |
| | |
| | |

APPENDIX C: GLOSSARY

Backup: A duplicate of hardware, software or data intended to replace the original in the event of a malfunction or disaster.

Business Continuity Plan (BCP): Documentation of a predetermined set of instructions or procedures that describe how an organization's *business functions* will be sustained during and after a significant disruption.

Business Impact Analysis (BIA): An analysis of an IT system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Business Recovery/Resumption Plan (BRP): Documentation of a predetermined set of instructions or procedures that describe how *business processes* will be restored after a significant disruption has occurred.

Cold Site: An environmentally conditioned facility of adequate workspace and infrastructure to support relocated IT operations in the event of a significant disruption. The facility does not, however, permanently contain the equipment necessary to continue operations.

Computer System Life Cycle: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal – which instigates another system initiation.

Computer: A device that accepts digital data and manipulates the information based on a program or sequence of instructions for how data is to be processed.

Contingency Plan: A documented set of instructions or procedures that describe how to recover and restore to normal operations a specific IT system due to a significant disruption.

Contingency Planning: A coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption

Continuity of Operations Plan (COOP): A predetermined set of instructions or procedures that describe how an organization's *essential functions* will be sustained for up to 30 days due to a disaster event before returning to normal operations.

Continuity of Support Plan: Documentation of a predetermined set of instructions or procedures mandated by OMB A-130, that describe how to sustain general support systems and major applications in the event of a significant disruption.

Desktop computers: Stationary personal computers that fit conveniently on top of an office desk or table. They are not suited to move or travel. Desktop computers usually consist of a micro-case or mini-tower that contains the central processing unit, memory, disk drives, a motherboard, and communication ports, input devices and output devices.

Disaster Recovery Plan (DRP): A predetermined set of instructions or procedures that describe how an *IT system* will be recovered after a **catastrophic** event that denying access to the normal facility has occurred.

Disk Replication: Process of making a copy of the disk.

Distributed System: A system of multiple autonomous processing elements, cooperating in a common purpose or to achieve a common goal, and appears to the users as being a single source.

Electronic Vaulting: Ability to store and retrieve backups electronically at a remote site.

Fault Tolerance: Ability of a system to continue to perform after the occurrence of faults.

Hot Site: An environmentally conditioned facility of adequate workspace fully configured with the necessary system hardware, supporting infrastructure, and support personnel for contingency use during a significant disruption to system operations.

Imaging: The capture and storage of a disk for disk replication purposes.

Incident Response Plan: Documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT systems(s).

IT System: A combination of IT components whose boundaries are identified by a set of processes, communications, storage and related resources (an architecture).

Load balancing: Traffic is dynamically distributed across groups of servers running a common application so that no one server is overwhelmed

Local Area Network: A data communications system that facilitates information sharing and transmission from one node to another in a small geographical area

Local Area Network: A data communications system that is composed of a group of computers and/or other devices that are dispersed over a limited area. Communications links enable a device to interact with any other on the network. The Local Area Network is owned by a single organization.

Mainframe: A multiuser computer designed to meet the computing needs of a large organization. The term came to be used generally to refer to the large central computers developed in the late 1950s and 1960s to meet the accounting and information management needs of large organizations

Mirrored Site: A fully redundant facility with complete, real-time information mirroring, technically identical to the primary IT operations site which can be used for contingency purposes in the event of a significant disruption to normal IT system operations.

Mobile Site: A self-contained, transportable shell custom-fitted with the specific IT equipment and telecommunications necessary to provide full recovery capabilities upon notice of a significant disruption.

Personal Computer: A computer is capable of accepting data and instructions, executing the instructions to process the data, and presenting the results. A computer typically consists of a central processing unit, memory, disk storage, and various input and output devices. A personal computer designed for use by one person at a time

Personal Computers: Computers that are capable of accepting data and instructions, executing the instructions to process the data, and presenting the results.

Portable Computer: A personal computer that can be carried for convenience or travel purposes.

Portable System: A personal computer that can be carried for convenience and travel purposes.

Redundancy: Use of duplicate components to prevent failure of an entire system.

Redundant Array of Independent Disks (RAID): a technology that provides disk redundancy and fault tolerance for data storage by spreading data storage across multiple disk drives, rather than a single disk.

Remote Access: Ability to get access to a computer or a network from a remote distance

Remote Journaling: Transaction-level logging is conducted over communications links where transaction logs or journals are stored at a remote location

Risk Management: A program of activities implemented to identify, control, and mitigate IT-related risks as part of an effort to protect the whole organization.

Server: A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources and services available to network servers and devices.

Storage area network: A high-speed, high-performance network that allows different computers with different operating systems to communicate with one storage device.

Warm Site: An environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption.

Web Server: A computer that serves Web pages to the requesting client browser over the Internet or an Intranet. The Web server hosts the pages, scripts, programs, and multimedia files and serves them using the hypertext transfer protocol.

Wide Area Network: A data communications network that consists of two or more local area networks that is dispersed over a wide geographical area. Communications links, usually provided by a public carrier, enable a one local area network to interact with other local area networks.

Wireless: telecommunications in which electromagnetic waves in replace of cabling or wire carry the signal over part or all of the communication path.

APPENDIX D: REFERENCES

Academic Press, <http://www.academicpress.com/insight/05051997/compute6.htm>.

Amerivault, *Vaulting Provides Disaster Relief*,
www.amerivault.com/publications/Vaulting_provides_disaster_relief.htm

Charles T. Clark, *State-of-the-Art Storage*, 01/05/01, Network Magazine
<http://www.networkmagazine.com/article/NMG20010104S0002/3>.

CNT, *Electronic Vaulting Service Description*
<http://www.cnt.com/literature/documents/pl468.pdf> 2000.

CNT, *Outsourced Electronic Vaulting: Cost-effective Disaster Recovery and Business Continuation* <http://www.cnt.com/literature/documents/pl486.pdf>.

Comdisco© *Ensuring High Availability for Your Web Environment*
http://www.availability.com/resource/pdfs/comdisco_ha_for_Web.pdf

Contingency Planning and Management Online, <http://www.contingencyplanning.com>,
September 2001.

Contingency Planning and Management, *Master Source 2001, Buyer's Guide Issue*, Volume 6,
2001.

D. Scott, J. Krischer, J. Rubin. *Research Note: Disaster Recovery: Weighing Data Replication Alternatives*, Gartner Group. June 15, 2001

Dave Fetters *Building a Storage Area Network* www.networkcomputing.com
<http://www.networkcomputing.com/1109/1109ws1.html> May 15, 2000

David Risely, May 11, 2001. *RAID: Your Guide* PCMechanic www.pcmach.com
<http://www.pcmach.com/showdoc/296/3/>, October 4, 2001.

Disaster Recovery Institute International, www.dr.org

Disaster Recovery Journal, www.drj.com, September 2001

Enterasys Networks. *The Role of Switch Routers with Server Load Balancing in Enterprise Networks*, 2001.

Federal Information Processing Standards Publication (FIPS PUB) 87, *Guidelines for ADP Contingency Planning*, March 1981.

Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations (COOP)*, July 1999.

GAO Executive Guide, *Information Security Management: Learning From Leading Organizations*, May 1998.

GAO Federal Information System Controls Audit Manual (FISCAM), June 2001.

Information Assurance Technical Framework Forum, *IATF Document and Framework Archive*, Version 3.0, October 2000 www.iatf.net/login/framework_docs/

Jane Wright, Ann Katan. *Technology Overview: High Availability: A Perspective* Gartner. June 15, 2001

Jon William Toigo, *Last Words: Client/Server Computing: Our Achilles' Heel?* http://www.contingencyplanning.com/article_index.cfm?article=229 January, 2000

Loraine Lawson ICN - *DRP increases in importance* Gartner/TechRepublic, Inc., 5/3/2001 http://www.infowar.com/iwftp/icn/03May2001_DRP_increases_in_importance.shtml

Mark F. Leary, CPP, *A Rescue Plan for Your LAN*, Security Management Online, <http://www.securitymanagement.com/library/000496.html>

Michael Hurwicz, *When Disaster Strikes* 01/01/00 Network Magazine <http://www.networkmagazine.com/article/NMG20000510S0027>.

NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, Chapter 11, *Preparing for Contingencies and Disasters*, Chapter 12, *Computer Security Incident Handling*, October 1995.

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

NIST Special Publication 800-26, *Security Self-Assessment for Information Technology Systems*, August 2001.

Omar Barazza, Ted Uhler. *Storage Area Networks: The Superior Storage Solution*. October 2000. Dot Hill

OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, November 2000.

PCWorld.com, *HassleFree Backups*, Retrieved on October 10, 2001: <http://www.pcworld.com/howto/article/0,aid,18040,00.asp>

Presidential Decision Directive (PDD) 62, *Protection Against Unconventional Threats to the Homeland and Americans Overseas*, May 1998

Presidential Decision Directive (PDD) 63, *Critical Infrastructure Protection*, May 1998

Presidential Decision Directive (PDD) 67, *Enduring Constitutional Government and Continuity of Government*, October 1998

Ralf Engelschall, *Load Balancing Your Web Site*, www.Webtechniques.com, May 1998.

Remote Mirroring, Technical White Paper, <http://www.sun.com/storage/white-papers/remote-mirroring.wp.html>

TechTarget http://searchWin2000.techtarget.com/sDefinition/0,,sid1_gci211829,00.html.

The Computer Security Act of 1987.

The Federal Response Plan (FRP), April 1999.

Tom Solinap, "RAID: An In-Depth Guide To RAID Technology" Date Posted: January 24th, 2001, SystemLogic.net Web site: <http://www.systemlogic.net/articles/01/1/raid/> retrieved on October 4, 2001.

University of Bradford School of Informatics, Department of Computing
<http://www.comp.brad.ac.uk>.

University of London, Imperial College of Science, Technology, and Medicine, Department of Computing <http://www.doc.ic.ac.uk>.

Webopedia