NIST Special Publication 800-34 Rev. 1

Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

NIST National Institute of Standards and Technology • U.S. Department of Commerce

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

NIST Special Publication 800-34 Rev. 1

Contingency Planning Guide for Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

May 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST.

All NIST documents mentioned in this publication, other than the ones noted above, are available at http://csrc.nist.gov/publications.

National Institute of Standards and Technology Special Publication 800-34
Natl. Inst. Stand. Technol. Spec. Publ. 800-34, 150 pages (May 2010)
CODEN: NSPUE2

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. Attribution would be appreciated by NIST.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on 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, Director of the OMB, or any other federal official.

NIST Special Publication 800-34, Revision 1, 150 pages

(May 2010)

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.

- Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.

- Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that, for other than national security programs and systems, agencies must follow NIST guidance.[1]

- Other security-related publications, including NIST interagency and internal reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

[1] While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some latitude in the application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of adequate security for federal information systems. When assessing federal agency compliance with NIST guidance, auditors, evaluators, and assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

Acknowledgements

The authors, Marianne Swanson and Pauline Bowen of the National Institute of Standards and Technology (NIST), Amy Wohl Phillips, Dean Gallup, and David Lynes of Booz Allen Hamilton, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge Kelley Dempsey, Esther Katzman, Peter Mell, Murugiah Souppaya, Lee Badger, and Elizabeth Lennon of NIST, and David Linthicum of Booz Allen Hamilton for their keen and insightful assistance with technical issues throughout the development of the document.

Table of Contents

Executive Summary **1**

Chapter 1. Introduction **1**

1.1 Purpose 1
1.2 Scope 2
1.3 Audience 3
1.4 Document Structure 4

Chapter 2. Background **5**

2.1 Contingency Planning and Resilience 5
2.2 Types of Plans 7
2.2.1 Business Continuity Plan (BCP) 8
2.2.2 Continuity of Operations (COOP) Plan 8
2.2.3 Crisis Communications Plan 9
2.2.4 Critical Infrastructure Protection (CIP) Plan 9
2.2.5 Cyber Incident Response Plan 10
2.2.6 Disaster Recovery Plan (DRP) 10
2.2.7 Information System Contingency Plan (ISCP) 10
2.2.8 Occupant Emergency Plan (OEP) 10

Chapter 3. Information System Contingency Planning Process **13**

3.1 Develop the Contingency Planning Policy Statement 14
3.2 Conduct the Business Impact Analysis (BIA) 15
3.2.1 Determine Business Processes and Recovery Criticality 16
3.2.2 Identify Resource Requirements 19
3.2.3 Identify System Resource Recovery Priorities 19
3.3 Identify Preventive Controls 19
3.4 Create Contingency Strategies 20
3.4.1 Backup and Recovery 20
3.4.2 Backup Methods and Offsite Storage 21
3.4.3 Alternate Sites 21
3.4.4 Equipment Replacement 24
3.4.5 Cost Considerations 25
3.4.6 Roles and Responsibilities 26
3.5 Plan Testing, Training, and Exercises (TT&E) 27
3.5.1 Testing 27
3.5.2 Training 28
3.5.3 Exercises 29
3.5.4 TT&E Program Summary 29
3.6 Plan Maintenance 31

Chapter 4. Information System Contingency Plan Development **34**

4.1 Supporting Information 35
4.2 Activation and Notification Phase 36
4.2.1 Activation Criteria and Procedure 36
4.2.2 Notification Procedures 36
4.2.3 Outage Assessment 38
4.3 Recovery Phase 39
4.3.1 Sequence of Recovery Activities 39

4.3.2 Recovery Procedures 39
4.3.3 Recovery Escalation and Notification 40
4.4 Reconstitution Phase 41
4.5 Plan Appendices 42

Chapter 5. Technical Contingency Planning Considerations 43

5.1 Common Considerations 43
5.1.1 Use of the BIA 44
5.1.2 Maintenance of Data Security, Integrity, and Backup 44
5.1.3 Protection of Resources 46
5.1.4 Adherence to Security Controls 46
5.1.5 Identification of Alternate Storage and Processing Facilities 46
5.1.6 Use of High Availability (HA) Processes 48
5.2 Client/Server Systems 48
5.2.1 Client/Server Systems Contingency Considerations 49
5.2.2 Client/Server Systems Contingency Solutions 51
5.3 Telecommunications Systems 52
5.3.1 Telecommunications Contingency Considerations 53
5.3.2 Telecommunications Contingency Solutions 54
5.4 Mainframe Systems 56
5.4.1 Mainframe Contingency Considerations 56
5.4.2 Mainframe Contingency Solutions 56
5.5 System Contingency Planning Considerations Summary 57

Appendix A— Sample Information System Contingency Plan Templates A.1-1

A.1 Sample Template for Low-Impact Systems A.1-1
A.2 Sample Template for Moderate-Impact Systems A.2-1
A.3 Sample Template for High-Impact Systems A.3-1

Appendix B— Sample Business Impact Analysis (BIA) and BIA Template B-1

Appendix C— Frequently Asked Questions C-1

Appendix D— Personnel Considerations in Continuity and Contingency Planning D-1

Appendix E— Contingency Planning Controls E-1

Appendix F— Contingency Planning and the System Development Life Cycle (SDLC) .. F-1

Appendix G— Glossary G-1

Appendix H— Acronyms H-1

Appendix I— Resources I-1

List of Figures

Figure 2-1: Contingency-Related Plan Relationships 12
Figure 3-1: Contingency Planning Process 13
Figure 3-2: Business Impact Analysis Process for the Information System 16
Figure 3-3: Cost Balancing 18
Figure 4-1: Contingency Plan Structure 34

Figure 4-2: Sample Call Tree 37
Figure 4-3: Sample Recovery Process 40
Figure F-1: System Development Life Cycle F-1

List of Tables

Table 2-1: Summary of NIST SP 800-53 Contingency Planning Controls for Low-, Moderate-, and High-Impact Systems of Contingency-Related Plans 7
Table 2-2: Type of Plans 11
Table 3-1: Information System Resource/Component Table 19
Table 3-2: FIPS 199 Category Backup & Strategy Examples 20
Table 3-3: Sample Alternate Site Criteria 23
Table 3-4: Contingency Strategy Budget Planning Template 25
Table 3-5: ISCP TT&E Activities 30
Table 3-6: Sample Record of Changes 32
Table 5-1: Summary 58
Table E-1: Summary of NIST SP 800-53 Contingency Planning Controls for Low-, Moderate- and High- Impact Systems of Contingency-Related Plans E-1
Table F-1: CP Control Implementation in the SDLC F-4

Errata

The following changes have been incorporated into Special Publication 800-34, Revision 1, as of the date indicated in the table.

DATE	TYPE	CHANGE	PAGE NUMBER
5/21/2010	Editorial	Remove hyphenation from "Wohl Phillips"	v
5/21/2010	Editorial	Change "mission/business functions" to "mission/business processes"	ES-1, 1, 2, 3, 7, 8, 10, 11, 13, 15, 16, 18, 19, 20, 21, 40, 44, 47, 48, 56 A.1-4, A.2-4, A.3-4, B-1, B-2, B-3, B-4, C-1, C-2, C-3, C-4, E-2, F-2, G-1, G-2
5/21/2010	Editorial	Remove hyphenation from "mission essential"	2, 5, 8, C-1, G-1, H-2
5/21/2010	Editorial	Correct number of Contingency Planning security controls to 9	6
5/21/2010	Editorial	Change "information system contingency plan" to "ISCP"	10
5/21/2010	Editorial	Change caption from "Plan Types" to "Types of Plans"	11
5/21/2010	Editorial	Change "mission essential functions" to "MEFs"	11, C-1, C-2
5/21/2010	Substantive	Clarify the relationship between Mean Tolerable Downtime and Recovery Point Objective	17
5/21/2010	Editorial	Change "continuity planners" to "contingency planners"	17
5/21/2010	Editorial	Change "missions" to "mission"	20
5/21/2010	Substantive	Add "and scope" to the description of system backup policies specifications	21
5/21/2010	Editorial	Change "Information Systems Planning" to "ISCP" in footnote	21
5/21/2010	Editorial	Change "applications" to "systems"	23, B-4
5/21/2010	Editorial	Change "information technology systems" to "information systems"	24, C-1
5/21/2010	Editorial	Change "Special Publication" to "SP"	30
5/21/2010	Substantive	Clarify the Contingency Plan Test/Exercise requirement for Contingency Plan Control-4 (CP-4). Change "All" to "Low Impact = Yes Mod. Impact = Yes High Impact = Yes"	30
5/21/2010	Substantive	Add Contingency Plan Control-4 (CP-4) to the Alternate Processing Site Recovery event; Change Moderate Impact requirement from "Yes" to "N/A"	30
5/21/2010	Editorial	Add commas around "as part of the organization's change management process" in the plan maintenance description of reviewing and updating the ISCP	31
5/21/2010	Editorial	Figure 4-2, Sample Call Tree, align and remove shadow	37
5/21/2010	Editorial	Remove "and applications" from the Sequence of Recovery Activities	39

DATE	TYPE	CHANGE	PAGE NUMBER
5/21/2010	Editorial	Change “backup application” to “backup solution” in the description of Backup Software	45
5/21/2010	Editorial	Change “discloser” to “disclosure”	46
5/21/2010	Editorial	Remove “major applications and general support” from system description	54
5/21/2010	Editorial	Change “Mission, National, or Primary Essential Functions” to “Mission, Primary, or National Essential Functions”	54
5/21/2010	Substantive	Spell out “ISDN” as “Integrated Services Digital Network (ISDN)”; add “with a bandwith of 128Kbps” for clarification	55
5/21/2010	Editorial	Change “Information System Contingency Plan (ISCP)” to “ISCP”	A.1-4, A.2-4, A.3-4, B-1, D-1
5/21/2010	Editorial	Change “Contingency Plan” to “ISCP”	A.1-5, A.3-5
5/21/2010	Editorial	Change “contingency plan coordinator” to “ISCP Coordinator”	A.1-7, A.2-7, A.3-7
5/21/2010	Editorial	Change “be needed” to “need”	A.1-7, A.2-7, A.3-7
5/21/2010	Editorial	Change “Section 4.1 of the plan” to “Section 4.2.1 of this plan”, in reference to location of system functions	A.1-7, A.2-7, A.3-7
5/21/2010	Substantive	Add to directions for Recovery Procedures “If an alternate location is part of the recovery strategy, include procedures for recovery to that site.”	A.1-8
5/21/2010	Editorial	Correct section numbering starting at 5.6	A.1-9
5/21/2010	Editorial	Change “System Validation Test Plan” to “system validation test plan” in Appendix E	A.1-12, A.2-12, A.3-12
5/21/2010	Substantial	Clarify “at least yearly” to “at the organization defined frequency (e.g., yearly)”	A.1-13, A.2-14, A.3-15
5/21/2010	Editorial	Change “and exercise and questions” to “and an exercise and questions”	A.1-13, A.2-14, A.3-15
5/21/2010	Editorial	Correct reference number to Offsite Data Storage	A.2-9, A.3-10
5/21/2010	Substantive	Remove “For moderate impact systems, a yearly functional test is required.” This is not a requirement.	A.2-14
5/21/2010	Substantive	Remove “For high impact systems, a yearly functional test is required.” This is not a requirement.	A.3-15
5/21/2010	Substantive	Change “Incident Response Plan (IRP)” to “Cyber Incident Response Plan”	B-1
5/21/2010	Editorial	Add “Information System Contingency Plan”	B-1
5/21/2010	Editorial	Change “operation/maintenance” to “Operation/Maintenance”	C-2
5/21/2010	Editorial	Change “Business Impact Analysis (BIA)” to “BIA”	C-2
5/21/2010	Editorial	Change “Primary Mission Essential Functions” to “primary mission essential functions”	C-3
5/21/2010	Editorial	Add “(MTD)” after “mean tolerable downtime”	C-3
5/21/2010	Editorial	Add “and Contingency” to the Appendix title	D-1
5/21/2010	Editorial	Add “(BCP) after “business continuity plan”	D-1
11/11/2010	Substantive	Replaced Section 5.2 with Data Functionality Testing template text and direction. Previous text was a repeat of Section 5.3.	A.3-8

Executive Summary

NIST Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems,* provides instructions, recommendations, and considerations for federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. This guide addresses specific contingency planning recommendations for three platform types and provides strategies and techniques common to all systems.

- Client/server systems;
- Telecommunications systems; and
- Mainframe systems.

This guide defines the following seven-step contingency planning process that an organization may apply to develop and maintain a viable contingency planning program for their information systems. These seven progressive steps are designed to be integrated into each stage of the system development life cycle.

1. **Develop the contingency planning policy statement.** A formal policy provides the authority and guidance necessary to develop an effective contingency plan.

2. **Conduct the business impact analysis (BIA).** The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes. A template for developing the BIA is provided to assist the user.

3. **Identify preventive controls.** Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.

4. **Create contingency strategies.** Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.

5. **Develop an information system contingency plan.** The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.

6. **Ensure plan testing, training, and exercises.** Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

7. **Ensure plan maintenance.** The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

This guide presents three sample formats for developing an information system contingency plan based on low-, moderate-, or high-impact level, as defined by Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. Each format defines three phases that govern actions to be taken following a system disruption. The **Activation/Notification** Phase describes the process of activating the plan based on outage impacts and notifying recovery personnel. The **Recovery** Phase details a suggested course of action for recovery teams to restore system operations at an alternate site or using contingency capabilities. The final phase,

Reconstitution, includes activities to test and validate system capability and functionality and outlines actions that can be taken to return the system to normal operating condition and prepare the system against future outages.

Chapter 1. Introduction

Information systems are vital elements in most mission/business processes. Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption. Contingency planning is unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level.

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

- Restoring information systems using alternate equipment;
- Performing some or all of the affected business processes using alternate processing (manual) means (typically acceptable for only short-term disruptions);
- Recovering information systems operations at an alternate location (typically acceptable for only long–term disruptions or those physically impacting the facility); and
- Implementing of appropriate contingency planning controls based on the information system's security impact level.

This document provides guidelines to individuals responsible for preparing and maintaining information system contingency plans (ISCPs). The document discusses essential contingency plan elements and processes, highlights specific considerations and concerns associated with contingency planning for various types of information system platforms, and provides examples to assist readers in developing their own ISCPs.

1.1 Purpose

This publication assists organizations in understanding the purpose, process, and format of ISCP development through practical, real-world guidelines. While the principles establish a baseline to meet most organizational needs, it is recognized that each organization may have additional requirements specific to its own operating environment. This guidance document provides background information on interrelationships between information system contingency planning and other types of security and emergency management-related contingency plans, organizational resiliency, and the system development life cycle (SDLC). The document provides guidance to help personnel evaluate information systems and operations to determine contingency planning requirements and priorities. Requirements from FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, security impact levels, and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* contingency planning controls are integrated throughout the guideline. Considerations for impact levels and associated security controls for contingency planning are presented to assist planners in developing the appropriate contingency planning strategy. Although the information presented in this document is largely independent of particular hardware platforms, operating systems, and applications, technical considerations specific to common information system platforms are addressed.

1.2 Scope

This document is published by NIST as recommended guidelines for federal organizations. To assist personnel responsible for developing contingency plans, this document discusses common technologies that may be used to support contingency capabilities. Given the broad range of information system designs and configurations, as well as the rapid development and obsolescence of products and capabilities, the scope of the discussion is not intended to be comprehensive. Rather, the document describes technology practices to enhance an organization's information system contingency planning capabilities. These guidelines present contingency planning principles for the following common platform types:

- Client/server systems;
- Telecommunications systems; and
- Mainframe systems.

The document outlines planning principles for a wide variety of incidents that can affect information system operations. These range from minor incidents causing short-term disruptions to disasters that affect normal operations for an extended period. Because information systems vary in design and purpose, specific incident types and associated contingency measures are not addressed in this guide. Instead, a defined process is provided for identifying planning requirements needed to develop an effective contingency plan for any information system.

This document does not address facility-level information system planning (commonly referred to as a disaster recovery plan) or organizational mission continuity (commonly referred to as a continuity of operations [COOP] plan) except where it is required to restore information systems and their processing capabilities. Nor does this document address continuity of mission/business processes. Although information systems typically support mission/business processes, the processes also depend on a variety of other resources and capabilities not associated with information systems. Recovery of mission essential functions is addressed by COOP plans or business continuity plans. These plans are part of a suite of security and emergency management-related plans further described in Section 2.2. The ISCP may be prepared in coordination with disaster recovery planning, COOP planning, or business continuity planning to the degree that a particular system is necessary to provide a capability that is required during any of these events/efforts.

Information in this guide is consistent with guidelines provided in other NIST documents, including NIST SP 800-53 and FIPS 199. The guidelines proposed are also consistent with federal mandates affecting contingency, continuity of operations, and disaster recovery planning, including:

- Federal Information Security Management Act (FISMA) of 2002;
- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, November 2000;
- Federal Continuity Directive (FCD)-1, *Federal Executive Branch National Continuity Program and Requirements*, February 2008;
- National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20, *National Continuity Policy*, May 2007;
- National Continuity Policy Implementation Plan, August 2007; and
- *National Response Framework*, March 22, 2008.

Federal organizations are required to comply with the above federal policies in addition to internal departmental or agency policies.

Information System:

An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.*

Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include, for example, such devices as firewalls, sensors (local or remote), switches, guards, routers, gateways, wireless access points, and network appliances. Servers can include, for example, database servers, authentication servers, electronic mail and Web servers, proxy servers, domain name servers, and network time servers. Information system components are either purchased commercially off-the-shelf or are custom-developed and can be deployed in land-based, sea-based, airborne, and/or space-based information systems.**

** As defined by 44 U.S.C., Sec 3502.*
*** As defined in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations.*

1.3 Audience

This document has been created for managers within federal organizations and those individuals responsible for information systems or security at system and operational levels. It is also written to assist emergency management personnel who coordinate facility-level contingencies with supporting information system contingency planning activities. The concepts presented in this document are specific to government systems, but may be used by private and commercial organizations, including contractor systems. The audience includes the following types of personnel:

- **Managers** responsible for overseeing information system operations or mission/business processes that rely on information systems;[2]
- **Chief Information Officers (CIOs)** with overall responsibility for the organization's information systems;[3]
- **Senior Agency Information Security Officers (SAISOs)** responsible for developing and maintaining the security of information systems at the organizational level;[4]
- **Information System Security Officers (ISSOs)/Information System Security Managers (ISSMs)** and other staff responsible for developing, implementing, and maintaining an information system's security activities;
- **System engineers and architects** responsible for designing, implementing, or modifying information systems;
- **System administrators** responsible for maintaining daily information system operations;

[2] Managers include Authorizing Officials, information system owners, and information owners.
[3] For organizations without a CIO position, FISMA requires a comparable executive to have authority over the information systems.
[4] SAISOs are also called Chief Information Security Officers (CISOs).

- **Users** who employ desktop and portable systems to perform their assigned job functions; and
- **Other personnel** responsible for designing, managing, operating, maintaining, or using information systems.

1.4 Document Structure

This document is designed to logically lead the reader through the contingency plan development process. The process includes designing a contingency planning program, evaluating the organization's needs against contingency strategy options based on the system impact levels, security controls, and technical considerations, and documenting the contingency strategy into a contingency plan, testing the plan, and maintaining it. The resulting contingency plan serves 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 chapters of this document address the following areas of contingency planning:

- Chapter 2, Background, provides background information about contingency planning, including the purpose of various security and emergency management-related plans, their relationships to ISCPs, and how the plans are integrated into an organization's overall resilience strategy by implementing the six steps of the Risk Management Framework (RMF).[5] In addition, the way in which the FIPS 199 impact levels and NIST SP 800-53 contingency planning controls must be considered during the contingency planning process is also explained.
- Chapter 3, Information System Contingency Planning Process, details the fundamental planning principles necessary for developing an effective contingency capability. The principles outlined in this section are applicable to all information systems. The section presents contingency planning guidelines for all elements of the planning cycle, including business impact analysis, alternate site selection, and recovery strategies. The section also discusses the development of contingency plan teams and the roles and responsibilities commonly assigned to personnel during plan activation.
- Chapter 4, Information System Contingency Plan Development, breaks down the activities necessary to document the contingency strategy and develop the ISCP. Maintaining, testing, training, and exercising the contingency plan are also discussed in this section.
- Chapter 5, Technical Contingency Planning Considerations, describes contingency planning concerns specific to the three common platform types listed in Section 1.3, Scope. This section helps contingency planners identify, select, and implement the appropriate technical contingency measures for their given systems.

This document includes nine appendices. Appendix A provides three sample ISCP templates, based on the FIPS 199 impact levels. Appendix B presents a sample BIA template. Appendix C contains a list of Frequently Asked Questions about information system contingency planning. Problems relevant to planning for personnel considerations are discussed in Appendix D. Appendix E provides a summary of NIST SP 800-53 contingency planning controls and control enhancements. Appendix F explains the integration of contingency planning into an organization's SDLC. Appendices G and H contain a glossary of terms and acronyms, respectively. Appendix I provides suggested resources and references.

[5] The Risk Management Framework is described in draft NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective.*

Chapter 2. Background

Information 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). Much vulnerability may be minimized or eliminated through management, operational, or technical controls as part of the organization's resiliency effort; however, it is virtually impossible to completely eliminate all risks.[6] Contingency planning is designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability.

This chapter discusses the ways in which federal information system contingency planning fits into an organization's larger risk management, security, and emergency preparedness programs (each of which is a key component in developing a resiliency program). Other types of emergency preparedness-related plans and their relationships to information system contingency planning are also described. Finally, the section discusses how integrating contingency planning principles throughout the SDLC promotes system compatibility and a cost-effective means to increase an organization's ability to respond quickly and effectively to a disruptive event.

2.1 Contingency Planning and Resilience

An organization must have the ability to withstand all hazards and sustain its mission through environmental changes. These changes can be gradual, such as economic or mission changes, or sudden, as in a disaster event. Rather than just working to identify and mitigate threats, vulnerabilities, and risks, organizations can work toward building a resilient infrastructure, minimizing the impact of any disruption on mission essential functions.

Resilience[7] is the ability to quickly adapt and recover from any known or unknown changes to the environment. Resiliency is not a process, but rather an end-state for organizations. The goal of a resilient organization is to continue mission essential functions at all times during any type of disruption. Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical functions. Risk management, contingency, and continuity planning are individual security and emergency management activities that can also be implemented in a holistic manner across an organization as components of a resiliency program.

Effective contingency planning begins with the development of an organization contingency planning policy and subjection of each information system to a business impact analysis (BIA). This facilitates prioritizing the systems and processes based on the FIPS 199 impact level and develops priority recovery strategies for minimizing loss. FIPS 199 provides guidelines on determining information and information system impact to organizational operations and assets, individuals, other organizations and the nation through a formula that examines three security objectives: confidentiality, integrity, and availability.[8]

- **Confidentiality** preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

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

[7] The Department of Homeland Security (DHS) Risk Lexicon (September 2008) defines resilience as the "ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions." The DHS Risk Lexicon can be found at www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf.

[8] As defined in 44 U.S. Code 35 Section 3542 (January 8, 2008).

- **Availability** ensures timely and reliable access to and use of information.

The impact for each security objective is determined to be high, moderate, or low, based on definitions provided in FIPS 199. The highest of the individual security objective impact levels are used to determine the overall information system security impact level.

Contingency planning considerations and strategies address the impact level of the availability security objective of information systems. Strategies for high-impact information systems should consider high-availability and redundancy options in their design. Options may include fully redundant load balanced systems at alternate sites, data mirroring, and offsite database replication. High-availability options are normally expensive to set up, operate, and maintain and should be considered only for those high-impact information systems categorized with a high-availability security objective. Lower-impact information systems may be able to use less expensive contingency options and tolerate longer downtimes for recovery or restoration of data.

Effective contingency planning includes incorporating security controls early in the development of an information system, and maintaining these controls on an ongoing basis. NIST SP 800-53, Rev. 3, identifies nine Contingency Planning (CP) security controls for information systems. Not all controls are applicable to all systems. The FIPS 199 security categorization determines which controls apply to a particular system. For example, information systems that have availability as a security objective categorized as low-impact do not require alternate processing or storage sites, and information systems that have an availability security objective categorized as moderate-impact require compliance with only the first system backup control enhancements. Using the FIPS 199 security categorization allows for tailoring of the CP security controls in NIST SP 800-53 to those applicable to the appropriate security control baselines. Table 2-1 provides a summary of the CP controls from NIST SP 800-53 and their applicability to the security control baselines. Further details and descriptions of the contingency planning controls are provided in Appendix E.

Several CP controls reference environmental controls, which are part of the NIST SP 800-53 Physical and Environmental Protection (PE) control family. Environmental controls considerations are only for the location or building that houses the information system. The environment includes the hardware and technology assets that support the information system. Section 3.3 of NIST SP 800-53 provides more information on environmental controls and their relationship to information systems.

There are options available to organizations to facilitate compliance with the CP controls. NIST SP 800-53 allows for compensating security controls to provide comparable protection for an information system to comply with the intent of a CP control. An organization may use a compensating security control in lieu of a CP control as long as there is justification for the use of the compensating control and willingness to accept the risk of the compensating control implementation. Further explanation of compensating security controls is available in Section 3.3 of NIST SP 800-53.

Table 2-1: Summary of NIST SP 800-53 Contingency Planning Controls for Low-, Moderate-, and High-Impact Systems of Contingency-Related Plans[9]

Control No.	Control Name	Security Control Baselines		
		Low	Moderate	High
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2) (3)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercise	CP-4	CP-4 (1)	CP-4 (1) (2) (4)
CP-5	Contingency Plan Update (Withdrawn)	------	-----	------
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3) (4) (5)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2) (3)	CP-10 (2) (3) (4)

2.2 Types of Plans

Information system contingency planning represents a broad scope of activities designed to sustain and recover critical system services following an emergency event. Information system contingency planning fits into a much broader security and emergency management effort that includes organizational and business process continuity, disaster recovery planning, and incident management. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's information systems, mission/business processes, personnel, and the facility. Because there is an inherent relationship between an information system and the mission/business process it supports, there must be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.

Continuity and contingency planning are critical components of emergency management and organizational resilience but are often confused in their use. *Continuity planning* normally applies to the mission/business itself; it concerns the ability to continue critical functions and processes during and after an emergency event. *Contingency planning* normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency. *Cyber Incident Response Planning* is a type of plan that normally focuses on detection, response, and recovery to a computer security incident or event.

In general, universally accepted definitions for information system contingency planning and the related planning areas have not been available. Occasionally, this leads to confusion regarding the actual scope and purpose of various types of plans. To provide a common basis of understanding regarding information system contingency planning, this section identifies several other types of plans and describes their purpose and scope relative to information system contingency planning. Because of the lack of standard definitions for these types of plans, the scope of actual plans developed by organizations may

[9] Numbers in parentheses in this table refer to control enhancements defined for that control in NIST SP 800-53. A control enhancement either adds related functionality or strengthens a basic control.

vary from the descriptions below. This guide applies the descriptions and references in sections below to security and emergency management-related plans. The plans listed are in alphabetical order, and do not imply any order of importance.

2.2.1 Business Continuity Plan (BCP)

The BCP focuses on sustaining an organization's *mission/business processes* during and after a disruption. An example of a mission/business process may be an organization's payroll process or customer service process. A BCP may be written for mission/business processes within a single business unit or may address the entire organization's processes. The BCP may also be scoped to address only the functions deemed to be priorities. A BCP may be used for long-term recovery in conjunction with the COOP plan, allowing for additional functions to come online as resources or time allow. Because mission/business processes use information systems (ISs), the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and IS capabilities are matched.

2.2.2 Continuity of Operations (COOP) Plan

COOP focuses on restoring an organization's *mission essential functions* (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. Additional functions, or those at a field office level, may be addressed by a BCP. Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP plan.

Standard elements of a COOP plan include:

- Program plans and procedures
- Risk management
- Budgeting and acquisition of resources
- Essential functions
- Order of succession
- Delegation of authority
- Continuity facilities
- Continuity communications
- Vital records management
- Human capital
- Test, training, and exercise
- Devolution
- Reconstitution

COOP plans are mandated for organizations by HSPD-20/NSPD-51, *National Continuity Policy* and FCD 1, *Federal Executive Branch National Continuity Program and Requirements*. Federal directives distinguish COOP plans as a specific type of plan that should not be confused with Information System Contingency Plans, Disaster Recovery Plans or BCPs. Nongovernment organizations typically use BCPs rather than COOP plans to address mission/business processes.

COOP vs. ISCP – The Basic Facts

FUNCTIONS

- COOP plans address national, primary, or mission essential functions; ISCPs address federal information systems.
  - COOP functions have specific criteria; not all government mission/business processes meet COOP criteria.
  - COOP functions may be supported by information systems.
  - Information systems support government mission/business processes, but not all government mission/business processes fall within the scope of COOP.

SCOPE

- COOP planning applies to mission essential functions of federal government departments and agencies.
- ISCPs apply to all information systems in federal organizations.

AUTHORITIES

- COOP is mandated for federal organizations by HSPD-20/NSPD-51, FCDs 1 and 2, and the National Continuity Policy Implementation Plan (NCPIP); ISCPs are mandated for federal organizations by FISMA.

2.2.3 Crisis Communications Plan

Organizations should document standard procedures for internal and external communications in the event of a disruption using a crisis communications plan. A crisis communications plan is often developed by the organization responsible for public outreach. The plan provides various formats for communications appropriate to the incident. The crisis communications plan typically designates specific individuals as the *only* authority for answering questions from or providing information to the public regarding emergency response. It may also include procedures for disseminating reports to personnel on the status of the incident and templates for public press releases. The crisis communication plan procedures should be communicated to the organization's COOP and BCP planners to ensure that the plans include clear direction that only approved statements are released to the public by authorized officials. Appendix D provides further discussion of topics addressed by the crisis communications plan and informational resources.

2.2.4 Critical Infrastructure Protection (CIP) Plan

Critical infrastructure and key resources (CIKR) are those components of the national infrastructure that are deemed so vital that their loss would have a debilitating effect of the safety, security, economy, and/or health of the United States.[10] A CIP plan is a set of policies and procedures that serve to protect and recover these national assets and mitigate risks and vulnerabilities. CIP plans define the roles and responsibilities for protection, develop partnerships and information sharing relationships, implement the risk management framework defined in the National Infrastructure Protection Plan (NIPP) and Homeland Security Presidential Directive (HSPD) - 7 for CIKR assets, and integrate federal, state and local emergency preparedness, protection, and resiliency of critical infrastructure.

[10] For more information on Critical Infrastructure and Key Resources (CIKR), refer to the Department of Homeland Security's *National Infrastructure Protection Plan 2009*, available at www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

2.2.5 Cyber Incident Response Plan

The cyber incident response plan[11] establishes procedures to address cyber attacks against an organization's information system(s).[12] 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, software, or data (e.g., malicious logic, such as a virus, worm, or Trojan horse). This plan may be included as an appendix of the BCP.

2.2.6 Disaster Recovery Plan (DRP)

The DRP applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. The DRP may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. A DRP may support a BCP or COOP plan by recovering supporting systems for mission/business processes or mission essential functions at an alternate location. The DRP only addresses information system disruptions that require relocation.

2.2.7 Information System Contingency Plan (ISCP)

An ISCP provides established procedures for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system.

The ISCP differs from a DRP primarily in that the information system contingency plan procedures are developed for recovery of the system regardless of site or location. An ISCP can be activated at the system's current location or at an alternate site. In contrast, a DRP is primarily a site-specific plan developed with procedures to move operations of one or more information systems from a damaged or uninhabitable location to a temporary alternate location. Once the DRP has successfully transferred an information system site to an alternate site, each affected system would then use its respective ISCP to restore, recover, and test systems, and put them into operation.

2.2.8 Occupant Emergency Plan (OEP)

The OEP outlines first-response procedures for occupants of a facility in the event of a threat or incident to the health and safety of personnel, the environment, or property. Such events include a fire, bomb threat, chemical release, domestic violence in the workplace, or a medical emergency. Shelter-in-place procedures for events requiring personnel to stay inside the building rather than evacuate are also addressed in an OEP. OEPs are developed at the facility level, specific to the geographic location and structural design of the building. General Services Administration (GSA)-owned facilities maintain plans based on the GSA OEP template. The facility OEP may be appended to the COOP or BCP, but is executed separately and as a first response to the incident. Aspects of planning for personnel safety and evacuation are discussed in Appendix D.

---

[11] A cyber incident response plan is different from the Cyber Incident Annex of the National Response Framework (NRF). The Cyber Incident Annex is for incidents "capable of causing extensive damage to critical infrastructure or key assets" and is more applicable to CIP plans.

[12] NIST SP 800-61 Rev. 1, *Computer Security Incident Handling Guide*, provides guidance on establishing a cyber incident response capability and plan.

Error! Reference source not found. summarizes the types of plans. The plan types identified are implemented individually or in coordination with one another as appropriate to respond to a disruptive event.

Table 2-2: Type of Plans

Plan	Purpose	Scope	Plan Relationship
Business Continuity Plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Addresses mission/business processes at a lower or expanded level from COOP MEFs.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs.
Continuity of Operations (COOP) Plan	Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives.	Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions.	MEF focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.
Crisis Communica-tions Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system-focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyber Incident Response Plan	Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP, depending on the extent of the attack.
Disaster Recovery Plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant Emergency Plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

Figure 2-1 shows the interrelationship of each plan as they are implemented to respond to the event as applicable to their respective scopes.

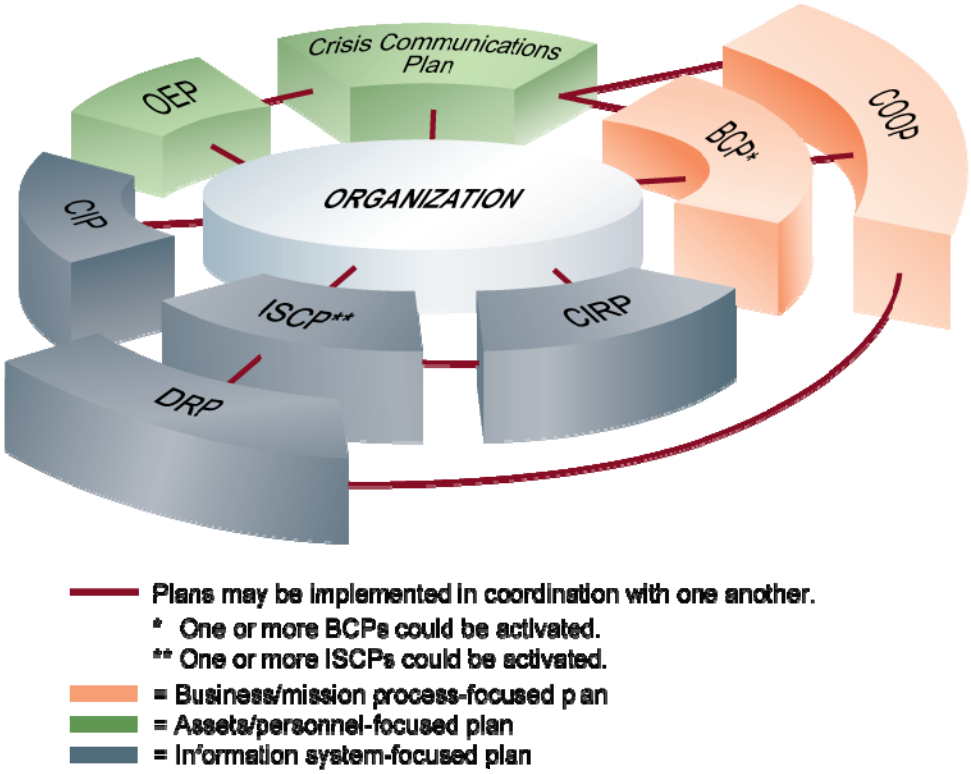

Figure 2-1: Contingency-Related Plan Relationships

Chapter 3. Information System Contingency Planning Process

This section describes the process to develop and maintain an effective information system contingency plan. The process presented is common to all information systems. The seven steps in the process are:

1. Develop the contingency planning policy;
2. Conduct the business impact analysis (BIA);
3. Identify preventive controls;
4. Create contingency strategies;
5. Develop an information system contingency plan;
6. Ensure plan testing, training, and exercises; and
7. Ensure plan maintenance.

These steps represent key elements in a comprehensive information system contingency planning capability. Developing contingency planning policy and performing system BIA(s) are accomplished early in the SDLC (see Appendix F) and before the systems are categorized in accordance with the RMF. Six of the seven planning process steps are discussed in this section. Because plan development represents the core of information system contingency planning, including the individual sections that compose the plan, plan development is addressed in Chapter 4. Responsibility for the planning process generally falls under the auspice of the Information System Contingency Plan Coordinator, or ISCP Coordinator, who is typically a functional or resource manager within the organization. The ISCP Coordinator develops the strategy in cooperation with other functional and resource managers associated with the system or the mission/business processes supported by the system. The ISCP Coordinator also typically manages development and execution of the contingency plan. All federal information systems must have a contingency plan. Figure 3-1 illustrates the contingency planning process.

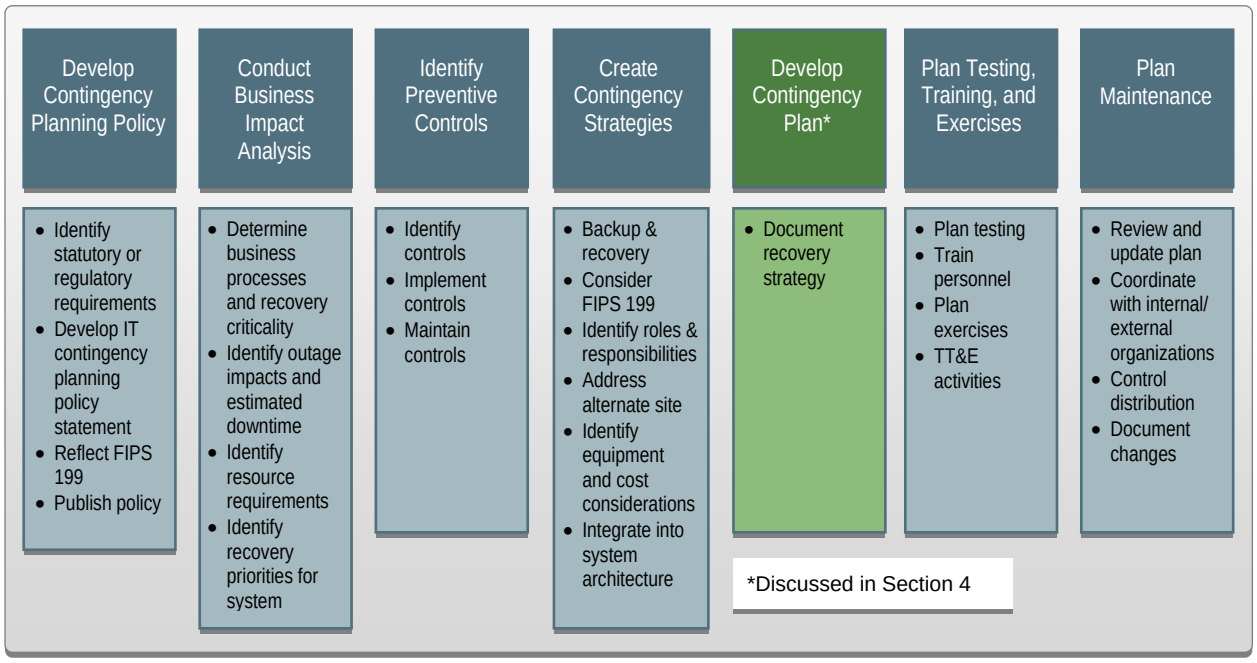

Figure 3-1: Contingency Planning Process

3.1 Develop the Contingency Planning Policy Statement

To be effective and to ensure that personnel fully understand the organization's contingency planning requirements, the contingency plan must be based on a clearly defined policy. The contingency planning policy statement should define the organization's overall contingency objectives and establish the organizational framework and responsibilities for system contingency planning. To be successful, senior management, most likely the CIO, must support a contingency program and be included in the process to develop the program policy. The policy must reflect the FIPS 199 impact levels and the contingency controls that each impact level establishes. Key policy elements are as follows:

- Roles and responsibilities;
- Scope as applies to common platform types and organization functions (i.e., telecommunications, legal, media relations) subject to contingency planning;
- Resource requirements;
- Training requirements;
- Exercise and testing schedules;
- Plan maintenance schedule; and
- Minimum frequency of backups and storage of backup media.

Sample information system contingency policy statement

All organizations must develop contingency plans for each information system to meet the needs of critical system operations in the event of a disruption. The procedures for execution of such a capability shall be documented in a formal contingency plan by the Information Systems Contingency Plan (ISCP) Coordinator and must be reviewed annually and updated as necessary by the ISCP Coordinator. The plan must account for the FIPS 199 security categorization (low, moderate, high) and comply with the appropriate security controls. The plan must assign specific responsibilities to designated staff or positions to facilitate the recovery and/or continuity of essential system functions. Resources necessary to ensure viability of the procedures must be acquired and maintained. Personnel responsible for target systems must be trained to execute contingency procedures. The plan recovery capabilities and personnel shall be tested annually to identify weaknesses of the capability.

As information system contingency plans are developed during the Initiation phase of the SDLC,[13] they should be coordinated with related organization-wide policies and programs, including information system security, physical security, human resources, system operations, and emergency preparedness functions. Information system contingency activities should be compatible with program requirements for these areas, and recovery personnel should coordinate with representatives from each area to remain aware of new or evolving policies, programs, or capabilities. The ISCPs must be written in coordination with other plans associated with each target system as part of organization-wide resilience strategy. Such plans include the following:

[13] The SDLC refers to the scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal that instigates another system initiation. The SDLC approach is discussed in depth in NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*. An overview of contingency planning and the SDLC is provided in Appendix F.

- Information system security plans;
- Facility-level plans, such as the OEP and DRP;
- MEF support such as the COOP plan; and
- Organization-level plans, such as CIP plans.

Similarly, the six-step RMF[14] brings together the supporting security standards and guidelines necessary for managing risk related to information systems. Implementing the RMF on an information system encompasses a broad range of activities to identify, control, and mitigate risks. From the information system contingency planning perspective, the six steps in the RMF actively support the development, implementation, testing, and maintenance of an information system's contingency plan as it supports the mission of the organization.

3.2 Conduct the Business Impact Analysis (BIA)

The BIA is a key step in implementing the CP controls in NIST SP 800-53 and in the contingency planning process overall. The BIA enables the ISCP Coordinator to characterize the system components, supported mission/business processes, and interdependencies. The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. The ISCP Coordinator can use the BIA results to determine contingency planning requirements and priorities. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's COOP, BCPs, and DRP. The BIA should be performed during the Initiation phase of the SDLC. As the system design evolves and components change, the BIA may need to be conducted again during the Development/Acquisition phase of the SDLC. Incorporating the RMF Step 1 (FIPS 199 categorization) and Step 2 (select security controls) helps to ensure that the BIA accounts appropriately for the level of risk to the organization.

COOP vs. ISCP – The Basic Facts

BUSINESS IMPACT ANALYSIS (BIA)

- COOP functions are subject to a process-focused BIA; federal information systems are subject to a system-focused BIA.
  - Information systems that support COOP functions will be identified in the process-based BIA.
  - FCD-2 provides a *required* template for a process-based BIA; NIST 800-34 provides a *recommended* template for a system-based BIA.

Three steps are typically involved in accomplishing the BIA:

1. **Determine mission/business processes and recovery criticality.** Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined **along with outage impacts and estimated downtime.** The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as

[14] NIST SP 800-37 further describes the RMF and provides guidance on organization-wide risk management including the development of risk management strategies, risk-related governance issues, defining protection requirements and associated risks for organizational mission/business processes, integration of security and privacy requirements into enterprise architectures, and managing risk within the system development life cycle.

quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

The sample BIA process and data collection activities, outlined in this section and illustrated in Figure 3-2, consisting of a representative information system with multiple components (servers), are designed to help the ISCP Coordinator streamline and focus contingency plan development activities to achieve a more effective plan.[15] An example of the BIA process and a BIA template are provided in Appendix B.

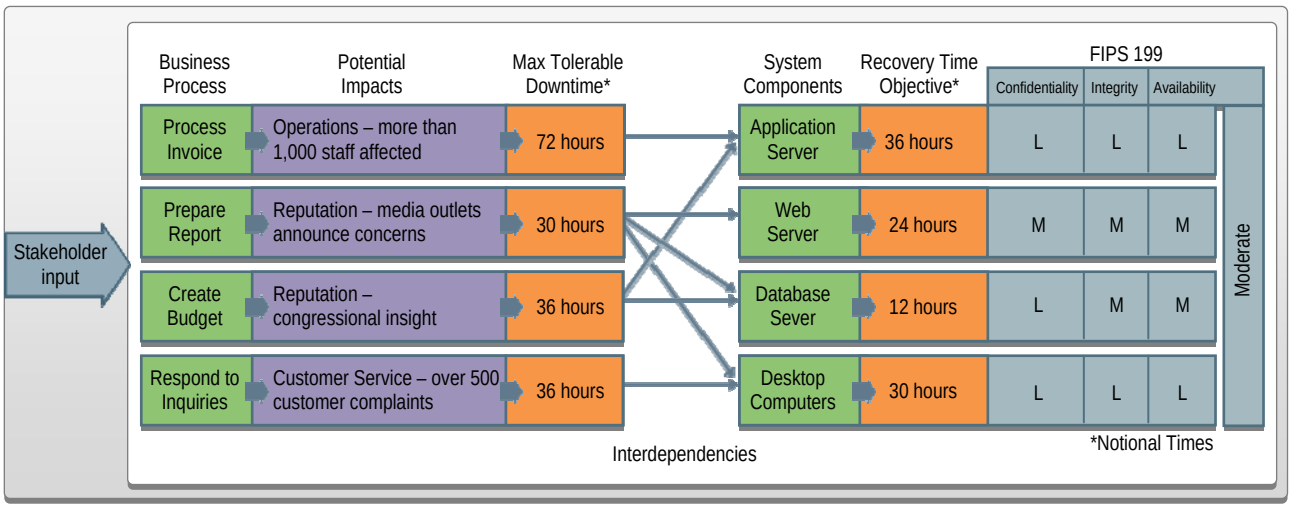

Figure 3-2: Business Impact Analysis Process for the Information System

3.2.1 Determine Business Processes and Recovery Criticality

An information system can be very complex and often supports multiple mission/business processes, resulting in different perspectives on the importance of system services or capabilities. To accomplish the BIA and better understand the impacts a system outage or disruption can have on the organization, the ISCP Coordinator should work with management and internal and external points of contact (POC)[16] to identify and validate mission/business processes and processes that depend on or support the information system. The identified processes' impacts are then further analyzed in terms of availability, integrity, confidentiality, and the established FIPS 199 impact level for the information system.

FIPS 199 requires organizations to categorize their information systems as low impact, moderate impact, or high impact for the security objectives of confidentiality, integrity, and availability (RMF Step 1). The FIPS 199 category for the availability security objective serves as a basis of the BIA. Further identification of additional mission/business processes and impacts captures the unique purpose of the

[15] For completeness and to assist ISCP Coordinators who may be new to or unfamiliar with the information system, the sample BIA process presented includes basic steps. In many cases, the ISCP Coordinator will be very familiar with specific system components and the ways in which they support business processes and may modify the approach to fit the respective system and contingency needs.

[16] When identifying POCs, it is important to include organizations that provide or receive data from the system as well as POCs of any interconnected systems. Coordination should enable the system manager to characterize the full range of support provided by the system, including security, managerial, technical, and operational requirements.

system. Organizational and system uniqueness are important considerations for contingency planning and business impact. Adding information types to address this uniqueness will enhance the prioritization of system component impacts.

Unique processes and impacts can be expressed in values or units of measurement that are meaningful to the organization. Values can be identified using a scale and should be characterized as an indication of impact severity to the organization if the process could not be performed.[17] For example, an impact category such as "Costs" can be created with impact values expressed in terms of staffing, overtime, or fee-related costs.

The ISCP Coordinator should next analyze the supported mission/business processes and with the process owners, leadership and business managers determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable. Downtime can be identified in several ways.[18]

- **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave contingency planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.[19]

- **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.[20] When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and Milestone should be initiated to document the situation and plan for its mitigation.

- **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage. Unlike RTO, RPO is not considered as part of MTD. Rather, it is a factor of how much data loss the mission/business process can tolerate during the recovery process.

Because the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.

---

[17] NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides additional guidance on security categories and information types that could influence criticality.

[18] The first version of NIST SP 800-34 used the term Maximum Allowable Outage (MAO) to describe the downtime threshold. To further delineate business process and information system downtime, Maximum Tolerable Downtime (MTD) and Recovery Time Objective (RTO) terms are used.

[19] Any information system that supports continuity of operations Mission Essential Functions (MEF), Primary Mission Essential Functions (PMEF), or National Essential Functions (NEF) must be able to meet the function's MTD of 12 hours or less per FCD-1.

[20] RTOs for telecommunications systems that support continuity of operation MEFs, PMEFs, or NEFs must support the function's COOP requirements including those put forth by National Communications Systems (NCS) Directive 3-10.

COOP vs. ISCP – The Basic Facts

RECOVERY TIMES

- COOP functions must be sustained within 12 hours and for up to 30 days from an alternate site; ISCP recovery time objectives are determined by the system-based BIA.
  - Information systems that support COOP functions must have an RTO that meets COOP requirements.
  - Information systems that do not support COOP functions do not *require* alternate sites as part of the ISCP recovery strategy, but may have an alternate site security control requirement.

The ISCP Coordinator, working with management, should determine the optimum point to recover the information system by addressing the factors mentioned above while balancing the cost of system inoperability against the cost of resources required for restoring the system and its overall support for critical mission/business processes. This can be depicted using a simple chart, such as the example in Figure 3-3.

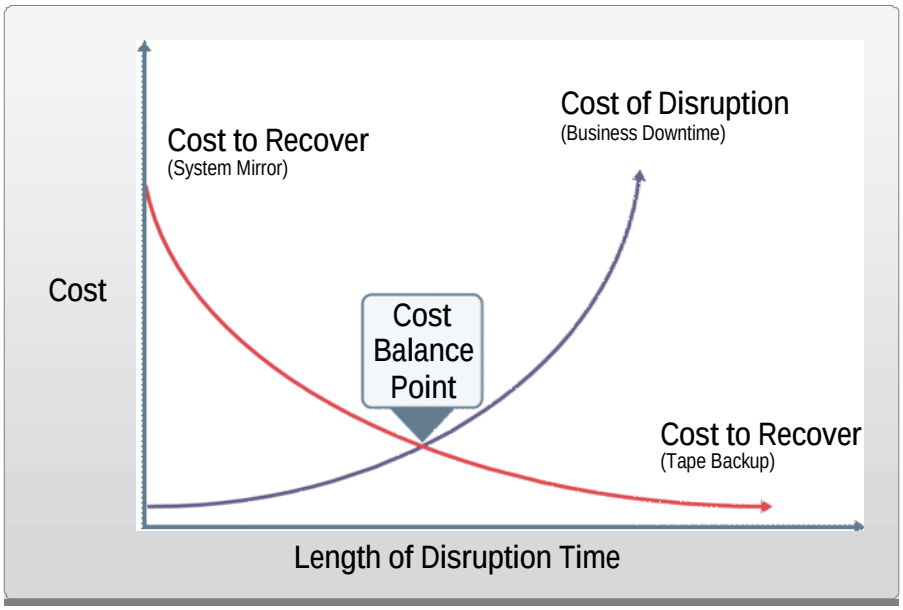

Figure 3-3: Cost Balancing

The longer a disruption is allowed to continue, the more costly it can become to the organization and its operations. Conversely, the shorter the RTO, the more expensive the recovery solutions cost to implement. For example, if the system must be recovered immediately, zero downtime solutions and alternate processing site costs will be much higher, whereas a low-impact system with a longer RTO would be able to implement a less costly simple tape backup system. Plotting the cost balance points will show an optimal point between disruption and recovery costs. The intersecting point (Cost Balance Point in Figure 3-3: Cost Balancing) will be different for every organization and system based on the financial constraints and operating requirements.

3.2.2 Identify Resource Requirements

Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes as quickly as possible. Working with management and internal and external POCs associated with the system, the ISCP Coordinator should ensure that the complete information system resources are identified.[21] A simple table such as the one shown in Table 3-1 can be used to capture relevant information system resources.

Table 3-1: Information System Resource/Component Table

System Resource/Component	Platform/OS/Version (as applicable)	Description
Application Server	*Sun V245/ Solaris / v10.0*	*Serves as the main application server*

3.2.3 Identify System Resource Recovery Priorities

Developing recovery priorities is the last step of the BIA process. Recovery priorities can be effectively established taking into consideration mission/business process criticality, outage impacts, tolerable downtime, and system resources. The result is an information system recovery priority hierarchy. The ISCP Coordinator should consider system recovery measures and technologies to meet the recovery priorities.

3.3 Identify Preventive Controls

In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. Step 2 of the RMF includes the identification of effective contingency planning preventive controls and maintaining these controls on an ongoing basis. A variety of preventive controls are identified in NIST SP 800-53, depending on system type and configuration; 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 prevent failure of certain components, such as a compressor;
- Fire suppression systems;
- Fire and smoke detectors;
- Water sensors in the computer room ceiling and floor;

[21] To avoid duplication of effort, this information may be obtained from the system component inventory and the system software inventory.

- Heat-resistant and waterproof containers for backup media and vital non electronic records;
- Emergency master system shutdown switch;
- Offsite storage of backup media, non electronic records, and system documentation;
- Technical security controls, such as cryptographic key management; and
- Frequent scheduled backups including where the backups are stored (onsite or offsite) and how often they are recirculated and moved to storage.

3.4 Create Contingency Strategies

Organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of mission/business processes. The challenge for organizations is in implementing the right set of security controls. Guided by the RMF and in accordance with FIPS 199 and NIST SP 800-53, security controls are selected and implemented. Contingency strategies are created to mitigate the risks for the contingency planning family of controls and cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance.

3.4.1 Backup and Recovery

Backup and recovery methods and strategies are a means to restore system operations quickly and effectively following a service disruption. The methods and strategies should address disruption impacts and allowable downtimes identified in the BIA and should be integrated into the system architecture during the Development/Acquisition phase of the SDLC. A wide variety of recovery approaches may be considered, with the appropriate choice being highly dependent upon the incident, type of system, BIA/FIPS 199 impact level, and the system's operational requirements.[22] Specific recovery methods further described in Section 3.4.2 should be considered and may include commercial contracts with alternate site vendors, reciprocal agreements with internal or external organizations, and service-level agreements (SLAs) with equipment vendors. In addition, technologies such as redundant arrays of independent disks (RAID), automatic failover, UPS, server clustering, and mirrored systems should be considered when developing a system recovery strategy.

Several alternative approaches should be considered when developing and comparing strategies, including cost, maximum downtimes, security, recovery priorities, and integration with larger, organization-level contingency plans. Table is an example that can assist in identifying the linkage of FIPS 199 impact level for the availability security objective, recovery priority, backup, and recovery strategy.

Table 3-2: FIPS 199 Category Backup & Strategy Examples

FIPS 199 Availability Impact Level	Information System Target Priority and Recovery	Backup / Recovery Strategy[23]
Low	Low priority - any outage with little impact, damage, or disruption to the organization.	Backup: Tape backup Strategy: Relocate or Cold site
Moderate	Important or moderate priority - any system that, if disrupted, would cause a moderate problem to the organization and possibly other networks or systems.	Backup: Optical backup, WAN/VLAN replication Strategy: Cold or Warm site

[22] Chapter 5, Technical Contingency Planning Considerations, provides detailed discussion of recovery methods applicable to specific types of information systems.
[23] Additional recovery strategy technical details and descriptions can be found in Sections 3.4.2 through 3.4.6.

FIPS 199 Availability Impact Level	Information System Target Priority and Recovery	Backup / Recovery Strategy[23]
High	Mission-critical or high priority - the damage or disruption to these systems would cause the most impact on the organization, mission, and other networks and systems.	Backup: Mirrored systems and disc replication Strategy: Hot site

3.4.2 Backup Methods and Offsite Storage

System data should be backed up regularly. Policies should specify the minimum frequency and scope 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 should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. Data may be backed up on magnetic disk, tape, or optical disks, such as compact disks (CDs). The specific method chosen for conducting backups should be based on system and data availability and integrity requirements. These methods may include electronic vaulting, network storage, and tape library systems.[24]

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 organization or to an alternate facility.[25] Commercial storage facilities 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:** distance from the organization and the probability of the storage site being affected by the same disaster as the organization's primary site;
- **Accessibility:** length of time necessary to retrieve the data from storage and the storage facility's operating hours;
- **Security:** security capabilities of the shipping method, storage facility, and personnel; all must meet the data's security requirements;
- **Environment:** structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls); and
- **Cost:** cost of shipping, operational fees, and disaster response/recovery services.

3.4.3 Alternate Sites

As stated in Section 2.1, NIST SP 800-53 identifies the CP controls for information systems. The FIPS 199 security categorization for the availability security objective determines which controls apply to a particular system. For example, an information system categorized with a low-availability security objective does not require alternate storage or a processing site (CP-6 and CP-7, respectively), and an information system with a moderate-availability security objective requires the system backup and testing

[24] Additional technical considerations are discussed in Chapter 5.

[25] Backup tapes should be tested regularly to ensure that data are being stored correctly and that the files may be retrieved without errors or lost data. Also, the ISCP Coordinator 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.

the backup (CP-9 [1]). Further details and descriptions of the contingency planning controls are provided in Appendix E.

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, for all FIPS 199 moderate- or high-impact systems, the plan should include a strategy to recover and perform system operations at an alternate facility for an extended period. Organizations may consider FIPS 199 low-impact systems for alternate site processing, but that is an organizational decision and not required. In general, three types of alternate sites are available:

- Dedicated site owned or operated by the organization;
- Reciprocal agreement or memorandum of agreement with an internal or external entity; and
- 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 commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites.[26] Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types. Progressing from basic to advanced, the sites are described below.

- **Cold Sites** are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.
- **Warm Sites** are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.
- **Hot Sites** are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.

As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution. Two examples of variations to the site types are:

- **Mobile Sites** are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.
- **Mirrored Sites** are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain, although they may 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, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site.

[26] For more complete technical details and descriptions, refer to Chapter 5.

Table 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, including considerations given to business impacts and downtime defined in the BIA. As sites are evaluated, the ISCP Coordinator should ensure that the system's security, management, operational, and technical controls are compatible with the prospective site. Such controls may include firewalls, physical access controls, and personnel security requirements of the staff supporting the site.

Table 3-34: Sample Alternate Site Criteria

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

Alternate sites may be owned and operated by the organization (internal recovery), or commercial sites may be available under contract. If contracting for the site with a commercial vendor, adequate testing time, work space, security requirements, hardware requirements, telecommunications requirements, support services, and recovery days (how long the organization can occupy the space during the 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; as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor's policy on how this situation should be addressed and how priority status is determined should be negotiated.

Two or more organizations with similar or identical system configurations and backup technologies may enter into a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. This type of site is set up via a reciprocal agreement or memorandum of understanding (MOU). A reciprocal agreement should be entered into carefully because each site must be able to support the other, in addition to its own workload, in the event of a disaster. This type of agreement requires the recovery sequence for the systems from both organizations to be prioritized from a joint perspective, favorable to both parties. Testing should be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and backup configurations, sufficient telecommunications connections, compatible security measures, and the sensitivity of data that might be accessible by other privileged users, in addition to functionality of the recovery strategy. Consideration should also be given to system interconnections and possible interconnection security agreements (ISAs). NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, provides guidance for planning, establishing, maintaining, and terminating interconnections between information systems that are owned and operated by different organizations.

An MOU or an SLA for an alternate site should be developed specific to the organization's needs and the partner organization's capabilities. The legal department of each party must review and approve the agreement. In general, the agreement should address at a minimum, each of the following elements:

- Contract/agreement duration;
- Cost/fee structure for disaster declaration and occupancy (daily usage), administration, maintenance, testing, annual cost/fee increases, transportation support cost (receipt and return of offsite data/supplies, as applicable), cost/expense allocation (as applicable), and billing and payment schedules;
- Disaster declaration (i.e., circumstances constituting a disaster, notification procedures);

- Site/facility priority access and/or use;
- Site availability;
- Site guarantee;
- Other clients subscribing to same resources and site, and the total number of site subscribers, as applicable;
- Contract/agreement change or modification process;
- Contract/agreement termination conditions;
- Process to negotiate extension of service;
- Guarantee of compatibility;
- Information system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software);
- Change management and notification requirements, including hardware, software, and infrastructure;
- Security requirements, including special security needs;
- Staff support provided/not provided;
- Facility services provided/not provided (use of onsite office equipment, cafeteria, etc.);
- Testing, including scheduling, availability, test time duration, and additional testing, if required;
- Records management (onsite and offsite), including electronic media and hardcopy;
- Service-level management (performance measures and management of quality of information system services provided);
- Work space requirements (e.g., chairs, desks, telephones, personal computers);
- Supplies provided/not provided (e.g., office supplies);
- Additional costs not covered elsewhere;
- Other contractual issues, as applicable; and
- Other technical requirements, as applicable.

3.4.4 Equipment Replacement

If the information system is damaged or destroyed or the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. Three basic strategies exist to prepare for equipment replacement.

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

often receive the highest priority for shipment. The details of these negotiations should be documented in the SLA, which should be maintained with the contingency plan.

- **Equipment Inventory**. Required equipment 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 alternate site. This solution has certain drawbacks. An organization must commit financial resources to purchase this equipment in advance, and the equipment could become obsolete or unsuitable for use over time because system technologies and requirements change.
- **Existing Compatible Equipment**. Equipment currently housed and used by the contracted hot site or by another organization within the organization may be used. Agreements made with hot sites and reciprocal internal sites stipulate that similar and compatible equipment will be available for contingency use by the organization.

When evaluating the choices, the ISCP Coordinator should consider that purchasing equipment when needed is cost-effective but can add significant overhead time to recovery while waiting for shipment and setup; conversely, storing unused equipment is costly, but allows recovery operations to begin more quickly. When selecting the most appropriate strategy, note that the availability of transportation may be limited or temporarily halted in the event of a catastrophic disaster. Based on impacts discovered through the BIA, consideration should be given to the possibility of a widespread disaster entailing mass equipment replacement and transportation delays that would extend the recovery period. 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.

3.4.5 Cost Considerations

The ISCP Coordinator 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. The coordinator should determine known contingency planning expenses, such as alternate site contract fees, and those that are less obvious, such as the cost of implementing an agency-wide contingency awareness program 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 (e.g., desks, telephones, fax machines, pens, and paper). The organization should perform a cost-benefit analysis to identify the optimum contingency strategy. Table provides a template for evaluating cost considerations.

Table 3-5: Contingency Strategy Budget Planning Template

Contingency Resources	Strategies	Vendor Costs	Hardware Costs	Software Costs	Travel / Shipping Costs	Labor / Contractor Costs	Testing Costs	Supply Costs
Alternate Site	Cold Site							
	Warm Site							
	Hot Site							
Offsite Storage	Commercial							
	Internal							
Equipment Replace-ment	SLA							
	Storage							
	Existing Use							

3.4.6 Roles and Responsibilities

Having selected and implemented the backup and system recovery strategies, the ISCP Coordinator must designate appropriate teams to implement the strategy. Each team should be trained and ready to respond 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, recovery team members need to clearly understand the team's recovery effort goal, individual procedures the team will execute, and how interdependencies between recovery teams may affect overall strategies.

The types of teams required are based on the information system affected and could be tailored according to FIPS 199 impact levels to reflect specific differences in requirements and backup procedures. The size of each team, team titles, and hierarchy designs depend on the organization. In addition to a single authoritative role for overall decision-making responsibility, including plan activation, a capable strategy will require some or all of the following groups:

- Management team (including the ISCP Coordinator);
- Outage assessment team;
- Operating system administration team;
- Server recovery team (e.g., client server, Web server);
- Local Area Network/Wide Area Network (LAN/WAN) recovery team;
- Database recovery team;
- Network operations recovery team;
- Application recovery team(s);
- Telecommunications team;
- Test team;
- Transportation and relocation team;
- Media relations team;
- Legal affairs team;
- Physical/personnel security team; and
- Procurement team (equipment and supplies).

Personnel should be chosen to staff these teams based on their skills and knowledge. Ideally, teams are staffed with personnel responsible for the same or similar functions under normal conditions. For example, server recovery team members should include the server administrators. Team members must understand not only the contingency plan purpose, but also 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, team members should be familiar with the goals and procedures of other teams to facilitate cross-team coordination. The ISCP Coordinator should also consider that a disruption could render some personnel unavailable to respond. In this situation, executing the plan may be possible only by using personnel from another geographic area of the organization or by hiring contractors or vendors. Such personnel may be coordinated and trained as an alternate team.

Each team is led by a team leader who directs overall team operations, acts as the team's representative to management, and liaises with other team leaders. 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 supervising the execution of contingency operations. The management team also facilitates

communications among other teams and supervises information system contingency plan tests and exercises. Some or all of the management team may lead specialized recovery teams. A senior management official, such as the CIO, has the ultimate authority to activate the plan and to make decisions regarding spending levels, acceptable risk, and interagency coordination. The senior management official typically leads the management team.

3.5 Plan Testing, Training, and Exercises (TT&E)

An ISCP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the ISCP. In addition, as indicated in Step 4 (Assess Security Controls) of the RMF, the effectiveness of the information system controls should be assessed by using the procedures documented in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. NIST SP 800-84, *Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities*, provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events. While the majority of TT&E activities occur during the Operations/Maintenance phase, initial TT&E events should be conducted during the Implementation/Assessment phase of the SDLC to validate ISCP recovery procedures.

Organizations should conduct TT&E events periodically, following organizational or system changes, or the issuance of new TT&E guidance, or as otherwise needed. Execution of TT&E events assists organizations in determining the plan's effectiveness, and that all personnel know what their roles are in the conduct of each information system plan. TT&E event schedules are often dictated in part by organizational requirements. For example, NIST SP 800-53 includes a control (CP-4) for federal organizations to conduct exercises or tests for their systems' contingency plans around an organization-defined frequency. Section 3.5.4 provides guidance on the type of TT&E identified for each FIPS 199 impact level.

For each TT&E activity conducted, results are documented in an after-action report, and Lessons Learned corrective actions are captured for updating information in the ISCP. While NIST SP 800-84 provides detailed information on how to plan and conduct TT&E activities for information systems, the following sections provide summarized details.

3.5.1 Testing

ISCP testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. Testing can take on several forms and accomplish several objectives but should be conducted in as close to an operating environment as possible. Each information system component should be tested to confirm the accuracy of individual recovery procedures. The following areas should be addressed in a contingency plan test, as applicable:

- Notification procedures;
- System recovery on an alternate platform from backup media;
- Internal and external connectivity;
- System performance using alternate equipment;
- Restoration of normal operations; and

- Other plan testing (where coordination is identified, i.e., COOP, BCP).

To derive the most value from the test, the ISCP Coordinator should develop a test plan designed to examine the selected element(s) against explicit test objectives and success criteria. The use of test objectives and success criteria enable the effectiveness of each system element and the overall plan to be assessed. The test plan should include a schedule detailing the time frames for each test and test participants. The test plan should also clearly delineate scope, scenario, and logistics. The scenario chosen may be a worst-case incident or an incident most likely to occur. It should mimic reality as closely as possible.

Testing	*Tests are evaluation tools that use quantifiable metrics to validate the operability of an information system or system component in an operational environment. For example, an organization could test call tree lists to determine if calling can be executed within prescribed time limits; another test may be removing power from a system or system component. A test is conducted in as close to an operational environment as possible; if feasible, an actual test of the components or systems used to conduct daily operations for the organization should be used.*[27] *The scope of testing can range from individual system components or systems to comprehensive tests of all systems and components that support an ISCP. Tests often focus on recovery and backup operations; however, testing varies depending on the FIPS 199 impact level, the goal of the test, and its relation to a specific ISCP.*

3.5.2 Training

Training for personnel with contingency plan responsibilities should focus on familiarizing them with ISCP roles and teaching skills necessary to accomplish those roles. This approach helps ensure that staff is prepared to participate in tests and exercises as well as actual outage events. Training should be provided at least annually. Personnel newly appointed to ISCP roles should receive training shortly thereafter. Ultimately, ISCP personnel should be trained to the extent that that they are able to execute their respective recovery roles and responsibilities without aid of the actual ISCP document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours, as a result of the disruption. 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 and Notification, Recovery, and Reconstitution Phases); and
- Individual responsibilities (Activation and Notification, Recovery, and Reconstitution Phases).

[27] Special consideration should be given to Industrial Control Systems (ICS) where systems typically have a need for real-time response and extremely high availability, predictability, and reliability. Thorough testing of these systems may not be possible during a single testing event. NIST SP 800-53, Appendix I, includes supplemental guidance for ICSs.

Training	*For the purposes of this publication and as documented in NIST SP 800-84, training refers only to informing personnel of their roles and responsibilities within a particular information system plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the ISCP. Training personnel on their roles and responsibilities before an exercise or test event is typically split between a presentation on their roles and responsibilities and activities that allow personnel to demonstrate their understanding of the subject matter.*

3.5.3 Exercises

NIST SP 800-84 identifies the following types of exercises widely used in information system TT&E programs by single organizations:

- **Tabletop Exercises.** Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates a discussion among the participants of roles, responsibilities, coordination, and decision making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.
- **Functional Exercises.** Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.[28] Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

Exercises	*An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an ISCP. In an exercise, personnel with roles and responsibilities in a particular ISCP meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that do not involve using the actual operational environment. Exercises are scenario-driven, such as a power failure in one of the organization's data centers or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise.*

3.5.4 TT&E Program Summary

A TT&E program provides an overall framework for determining, scheduling, and setting objectives for TT&E activities. Guidance on establishing an effective ISCP TT&E program and the various methods

[28] Planned and unplanned maintenance activities may also present opportunities to execute and document a Functional Exercise. This is often applicable to operational systems (such as ICS) where it may be otherwise disruptive to test certain aspects of the system or contingency plan. NIST SP 800-53, Appendix I, contains supplemental guidance.

and approaches for conducting TT&E activities is provided in NIST SP 800-84. The depth and rigor of ISCP TT&E activities increases with the FIPS 199 availability security objective. All tests and exercises should include some kind of determination of the effects on the organization's operations and provide for a mechanism to update and improve the plan as a result.

Each of the three ISCP Templates (FIPS 199 low, moderate, and high) included as appendices to this guide contain details for conducting TT&E activities appropriate to their respective impact level.

- **For low-impact systems, a tabletop exercise at an organization-defined frequency is sufficient.** The tabletop should simulate a disruption, include all main ISCP points of contact, and be conducted by the system owner or responsible authority.
- **For moderate-impact systems, a functional exercise at an organization-defined frequency should be conducted.** The functional exercise should include all ISCP points of contact and be facilitated by the system owner or responsible authority. Exercise procedures should be developed to include an element of system recovery from backup media.
- **For high-impact systems, a full-scale functional exercise at an organization-defined frequency should be conducted.** The full-scale functional exercise should include a system failover to the alternate location. This could include additional activities such as full notification and response of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an alternate location. The test should also include a full recovery and reconstitution of the information system to a known state.

Table presents a sample TT&E activity using NIST SP 800-53 guidance and as required by the FIPS 199 impact level.

Table 3-6: ISCP TT&E Activities

TT&E Event	Sample Activity	FIPS 199 Availability Security Objective
ISCP Training (CP-3)	A seminar and/or briefing used to familiarize personnel with the overall ISCP purpose, phases, activities, and roles and responsibilities.	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Instruction (CP-3)	Instruction of contingency personnel on their roles and responsibilities within the ISCP and includes refresher training. (For a high-impact system, incorporate simulated events.)	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Contingency Plan Test / Exercise (CP-4)	Test and/or exercise the contingency plan to determine effectiveness and the organization's readiness. This could include planned and unplanned maintenance activities	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Tabletop Exercise (CP-4)	Discussion-based simulation of an emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing ISCP and individual state of preparedness.	Low Impact = Yes

TT&E Event	Sample Activity	FIPS 199 Availability Security Objective
Functional Exercise (CP-4)	Simulation of a disruption with a system recovery component such as backup tape restoration or server recovery.	Mod. Impact = Yes High Impact = Yes
Full-Scale Functional Exercise (CP-4)	Simulation prompting a full recovery and reconstitution of the information system to a known state and ensures that staff are familiar with the alternate facility.	High Impact = Yes
Alternate Processing Site Recovery (CP-4,CP-7)	Test/exercise the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and evaluate the site's capabilities to support contingency operations. Includes a full recovery and return to normal operations to a known secure state. *(*For a high-impact system, the alternate site should be fully configured as defined in the plan.*)*	Low Impact = N/A Mod. Impact = N/A High Impact = Yes
System Backup (CP-9)	Test backup information to verify media reliability and information integrity. (For a high-impact system, use sample backup information and ensure that backup copies are stored in a separate facility.)	Low Impact = N/A Mod. Impact = Yes High Impact = Yes

3.6 Plan Maintenance

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the ISCP be reviewed and updated regularly as part of the organization's change management process to ensure that new information is documented and contingency measures are revised if required. As identified as part of RMF Step 6 (Continuous Monitoring), a continuous monitoring process can provide organizations with an effective tool for plan maintenance, producing ongoing updates to security plans, security assessment reports, and plans of action and milestone documents.

As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews. The plans for moderate- or high-impact systems should be reviewed more often. At a minimum, plan reviews should focus on the following elements:

- Operational requirements;
- Security 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 vendor POCs;
- Alternate and offsite facility requirements; and
- Vital records (electronic and hardcopy).

Because the ISCP contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled. Typically, copies of the plan are provided to recovery personnel for storage. A copy should also be stored at the alternate site and with the backup media. Storing a copy of the plan at the alternate site ensures its availability and good condition in the event local plan copies cannot be accessed because of disaster. The ISCP Coordinator should maintain a record of copies of the plan and to whom they were distributed. Other information that should be stored with the plan includes contracts with vendors (SLAs and other contracts), software licenses, system user manuals, security manuals, and operating procedures.

Changes made to the plan, strategies, and policies should be coordinated through the ISCP Coordinator, who should communicate changes to the representatives of associated plans or programs, as necessary. The ISCP Coordinator 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 , should be integrated into the plan as discussed in Section 4.1.

Table 3-7: Sample Record of Changes

Record of Changes			
Page #	Change Comment	Date of Change	Signature

The ISCP Coordinator should coordinate frequently with associated internal and external organizations and system POCs to ensure that impacts caused by changes within any organization will be reflected in the contingency plan. Strict version control must be maintained by requesting old plans or plan pages to be returned to the ISCP Coordinator in exchange for the new plan or plan pages. The ISCP Coordinator also should evaluate supporting information to ensure that the information is current and continues to meet system requirements adequately. This information includes the following:

- Alternate site contract, including testing times;
- Offsite storage contract;
- Software licenses;
- MOUs or vendor SLAs;
- Hardware and software requirements;

- System interconnection agreements;
- Security requirements;
- Recovery strategy;
- Contingency policies;
- Training and awareness materials;
- Testing scope; and
- Other plans, e.g., COOP, BCP.

Although some changes may be quite visible, others will require additional analysis. When a significant change occurs, the BIA should be updated with the 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. Finally, plan maintenance should be continued as the information system passes through the Disposal phase of its life cycle to ensure that the plan accurately reflects recovery priorities and concurrent processing changes.

Chapter 4. Information System Contingency Plan Development

This chapter discusses the key elements that compose the ISCP. As described in Chapter 3, ISCP development is a critical step in the process of implementing a comprehensive contingency planning program. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an information system following a disruption. The ISCP should document technical capabilities designed to support contingency operations and should be tailored to the organization and its requirements. Plans need to balance detail with flexibility; usually, the more detailed the plan, the less scalable and versatile the approach. The information presented here is meant to be a guide; nevertheless, 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 templates that organizations may use to develop ISCPs for their information systems at the appropriate FIPS 199 impact level. The information and templates provided are guides and may be modified, customized, and/or adapted as necessary to best meet the specific system, operational, and organizational requirements for contingency planning. Appendix D discusses planning considerations regarding personnel which should be coordinated with the ISCP development.

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

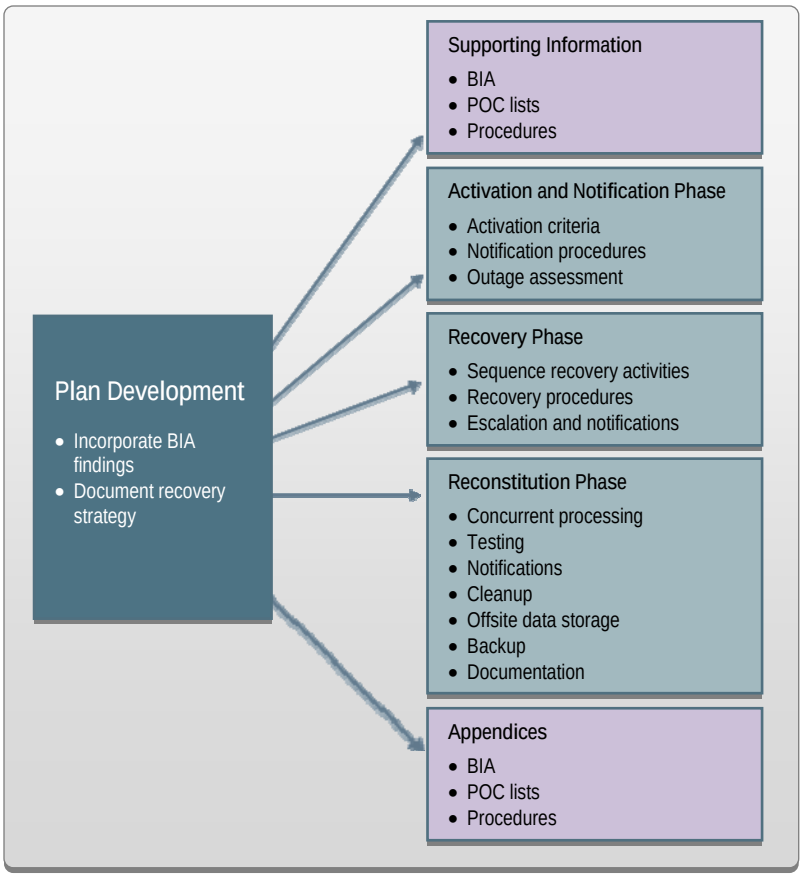

Figure 4-1: Contingency Plan Structure

Plans should be formatted to provide quick and clear directions in the event that personnel unfamiliar with the plan or the systems are called on to perform 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 reduces the likelihood of creating an overly complex or confusing plan.

4.1 Supporting Information

The supporting information component includes an introduction and concept of operations section providing essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. These details aid in understanding the applicability of the guidance, in making decisions on how to use the plan, and in providing information on where associated plans and information outside the scope of the plan may be found.

The introduction section orients the reader to the type and location of information contained in the plan. Generally, the section includes the background, scope, and assumptions.[29] These subsections are described below.

- **Background.** This subsection establishes the reason for developing the ISCP and defines the plan objectives.
- **Scope.** The scope identifies the FIPS 199 impact level and associated RTOs as well as the alternate site and data storage capabilities (as applicable).
- **Assumptions.** This section includes the list of assumptions that were used in developing the ISCP as well as a list of situations that are not applicable. See Appendix A Sample Information System Contingency Plan Templates, for a sample of assumptions and situations.

The concept of operations section provides additional details about the information system, the three phases of the contingency plan (Activation and Notification, Recovery, and Reconstitution), and a description of the information system contingency plan roles and responsibilities. This section may include the following elements:

- **System description**. It is necessary to include a general description of the information system addressed by the contingency plan. The description should include the information system architecture, location(s), and any other important technical considerations. An input/output (I/O) diagram and system architecture diagram, including security devices (e.g., firewalls, internal and external connections) are useful. The content for the system description can usually be taken from the System Security Plan.[30]
- **Overview of three phases**. The ISCP recovery is implemented in three phases: (1) Activation and Notification, (2) Recovery, and (3) Reconstitution.
- **Roles and responsibilities**. The roles and 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.

[29] 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 and organization's contingency planning requirements.

[30] NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, can be referenced for further details concerning information system documentation.

4.2 Activation and Notification Phase

The Activation and Notification Phase defines initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the plan. At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures to restore system functions.

4.2.1 Activation Criteria and Procedure

The ISCP should be activated if one or more of the activation criteria for that system are met. If an activation criterion is met, the designated authority should activate the plan.[31] Activation criteria for system outages or disruptions are unique for each organization and should be stated in the contingency planning policy. Criteria may be based on:

- Extent of any damage to the system (e.g., physical, operational, or cost);
- Criticality of the system to the organization's mission (e.g., critical infrastructure protection asset); and
- Expected duration of the outage lasting longer than the RTO.

The appropriate recovery teams may be notified once the system outage or disruption has been identified and the ISCP Coordinator has determined that activation criteria have been met. Notification procedures should follow the procedures outlined in Section 4.2.2 below.

4.2.2 Notification Procedures

An outage or disruption may occur with or without prior notice. For example, advance notice is often given that a hurricane is predicted to 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 both types of situation. The procedures should describe the methods used to notify recovery personnel during business and non business hours. Prompt notification is important for reducing the effects of a disruption on the system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash. Following the outage or disruption, notification should be sent to the Outage Assessment Team[32] so that it may determine the status of the situation and appropriate next steps. Outage assessment procedures are described in Section 4.2.3. When outage assessment is complete, the appropriate recovery and system support personnel should be notified.

Notifications can be accomplished through a variety of methods, either automated or manual and include telephone, pager, electronic mail (email), cell phone, and messaging. Automated notification systems follow established protocols and criteria and can include rapid authentication and acceptance and secure messaging. Automated notification systems require up-front investment and learning curve, but may be an effective way for some organizations to ensure prompt and accurate delivery.

---

[31] The designated authority (typically a senior manager or CIO) has the authority to activate the contingency plan. That authority may vary based on the organization or system, but the individual with this authority should be designated clearly in the plan. Only one individual should have this authority, and a successor should be clearly identified to assume that responsibility if necessary.

[32] The Outage Assessment Team is a representative title. Depending on how the organization establishes their roles and responsibilities, other names and titles may be used.

Notifications sent via email should be done with caution because there is no way to ensure receipt and acknowledgement. Although email has potential as an effective method of disseminating notifications to work or personal accounts, there is no way to guarantee that the message will be read. If using an email notification method, recovery personnel should be informed of the necessity to frequently and regularly check their accounts. Notifications sent during business hours should be sent to the work address, whereas personal email messaging may be useful in the event that the local area network (LAN) is down.

The notification strategy should define procedures to be followed in the event that specific personnel cannot be contacted. Notification procedures should be documented clearly in the contingency plan. Copies of the procedures can be made and located securely at alternate locations. A common manual 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.

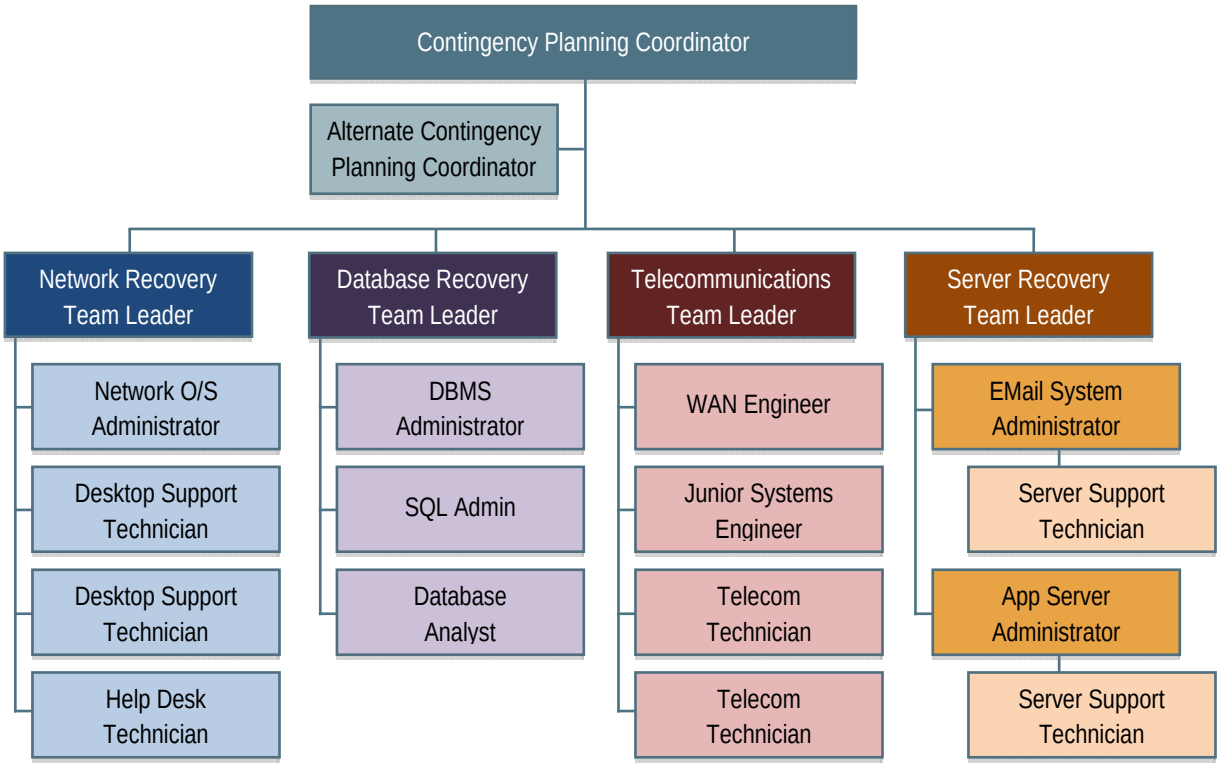

Figure 4-2: Sample Call Tree

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 (e.g., home, work, cell phone, email 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
Email: jones@organization.ext; jones@home.ext

Notifications also should be sent to POCs of external organizations or interconnected system partners that may be adversely affected if they are unaware of the situation. Depending on the type of outage or disruption, the POC may have recovery responsibilities. For each system interconnection with an external organization, a POC should be identified. These POCs should be listed in an appendix to the plan.

The type of information to be relayed to those being notified should be documented in the plan. The amount and detail of information relayed may depend on the specific team being notified. As necessary, notification information may include the following:

- Nature of the outage or disruption that has occurred or is impending;
- Any known outage estimates;
- Response and recovery details;
- Where and when to convene for briefing or further response instructions;
- Instructions to prepare for relocation for estimated time period (if applicable); and
- Instructions to complete notifications using the call tree (if applicable).

4.2.3 Outage Assessment

To determine how the ISCP will be implemented following a system disruption or outage, it is essential to assess the nature and extent of the disruption. The outage assessment should be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. When possible, the Outage Assessment Team is the first team notified of the disruption. Outage assessment procedures may be unique for the particular system, but the following minimum areas should be addressed:

- Cause of the outage or disruption;
- Potential for additional disruptions or damage;
- 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 system equipment (e.g., fully functional, partially functional, nonfunctional);
- Type of damage to system equipment or data (e.g., water, fire and heat, physical impact, electrical surge);
- Items to be replaced (e.g., hardware, software, firmware, supporting materials); and
- Estimated time to restore normal services.

Personnel with outage assessment responsibilities should understand and be able to perform these procedures in the event the plan is inaccessible during the situation. Once impact to the system has been determined, the appropriate teams should be notified of updated information and the planned response to the situation. Based upon the results of the outage assessment, ISCP notifications may be revisited and expanded using the procedures described in Section 4.2.2.

4.3 Recovery Phase

Formal recovery operations begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BIA will be recovered at this stage.

4.3.1 Sequence of Recovery Activities

When recovering a complex system, such as a wide area network (WAN) or virtual local area network (VLAN) involving multiple independent components, recovery procedures should reflect system priorities identified in the BIA. The sequence of activities should reflect the system's MTD to avoid significant impacts to related systems. Procedures should be written in a stepwise, sequential format so system components may be restored in a logical manner. For example, if a LAN is being recovered after a disruption, then 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 escalation steps and instructions to coordinate with other teams where relevant 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; and
- Other system-specific concerns exist.

If conditions require the system to be recovered at an alternate site, certain materials will need to be transferred or procured. These items may include shipment of data backup media 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 appendices, such as equipment lists or vendor contact information, should be made in the plan where necessary. Procedures should clearly describe requirements to package, transport, and purchase materials required to recover the system.

4.3.2 Recovery Procedures

To facilitate Recovery Phase operations, the ISCP should provide detailed procedures to restore the information system or components to a known state. Given the extensive variety of system types, configurations, and applications, this planning guide does not provide specific recovery procedures. Recovery considerations are detailed for each of the platform types in Chapter 5.

Procedures should be assigned to the appropriate recovery team and typically address the following actions:

- Obtaining authorization to access damaged facilities and/or geographic area;
- Notifying internal and external business partners associated with the system;
- Obtaining necessary office supplies and work space;
- Obtaining and installing necessary hardware components;
- Obtaining and loading backup media;
- Restoring critical operating system and application software;
- Restoring system data to a known state;
- Testing system functionality including security controls;
- Connecting system to network or other external systems; and
- Operating alternate equipment successfully.

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 and for troubleshooting problems if the system cannot be recovered properly. Figure 4-3 provides a partial example of a procedural checklist for a LAN Recovery Team.

SAMPLE Recovery Process for the LAN Recovery Team:
These procedures are used for recovering a file from backup tapes. The LAN Recovery Team is responsible for reloading all critical files necessary to continue production.

1. **Identify file and date from which file is to be recovered.**
2. **Identify tape number using tape log book.**
3. **If tape is not in tape library, request tape from recovery facility; fill out with appropriate authorizing signature.**
4. **When tape is received, log date and time.**
5. **Place tape into drive and begin recovery process.**
6. **When file is recovered, notify LAN Recovery Team Leader.**

Figure 4-3: Sample Recovery Process

4.3.3 Recovery Escalation and Notification

As identified as part of the BIA, system components, infrastructure, and associated facilities are critical components supporting daily mission/business processes. The systems, applications, and infrastructure that connect users to these are subject to events causing service interruptions and outages. Including an escalation and notification component within the Recovery Phase helps to ensure that overall, a repeatable, structured, consistent, and measurable recovery process is followed.

Effective escalation and notification procedures should define and describe the events, thresholds, or other types of triggers that are necessary for additional action. Actions would include additional notifications for more recovery staff, messages and status updates to leadership, and notices for additional resources. Procedures should be included to establish a clear set of events, actions and results, and should be documented for teams or individuals as appropriate.

4.4 Reconstitution Phase

The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan. Validation of recovery typically includes these steps:

- **Concurrent Processing**.[33] Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

- **Validation Data Testing**. Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.

- **Validation Functionality Testing**. Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

At the successful completion of the validation testing, ISCP personnel will be prepared to declare that reconstitution efforts are complete and that the system is operating normally. This declaration may be made in a recovery/reconstitution log or other documentation of reconstitution activities. The ISCP Coordinator, in coordination with the Information System Owner, ISSO, SAISO and with the concurrence of the Authorizing Official, must determine if the system has undergone significant change and will require reassessment and reauthorization.[34] The utilization of a continuous monitoring strategy/program can guide the scope of the reauthorization to focus on those environment/facility controls and any other controls which would be impacted by the reconstitution efforts. Assessment and authorization guidance is available in NIST SP 800-37, Rev. 1 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*
Deactivation of the plan is the process of returning the system to normal operations and finalizing reconstitution activities to prepare the system against another outage or disruption. These activities include:

- **Notifications**. Upon return to normal operations, users should be notified by the ISCP Coordinator (or designee) using predefined notification procedures.

- **Cleanup**. Cleanup is the process of cleaning up work space or dismantling any temporary recovery locations, restocking supplies, returning manuals or other documentation to their original locations, and readying the system for another contingency event.

[33] According to NIST SP 800-53 Contingency Plan security controls, information systems are not required to have concurrent processing capabilities.

[34] Examples of significant changes that would possibly apply in a contingency situation are: 1) new or upgraded hardware platform, and 2) moving to a new facility.

- **Offsite Data Storage.**[35] If offsite data storage is used, procedures should be documented for returning retrieved backup or installation media to its offsite data storage location.

- **Data Backup**. As soon as reasonable following reconstitution, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup should be stored with other system backups and comply with applicable security controls.

- **Event Documentation**. All recovery and reconstitution events should be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts. An after-action report with lessons learned should be documented and included for updating the ISCP.

Once all activities and steps have been completed and documentation has been updated, the ISCP can be formally deactivated. An announcement with the declaration should be sent to all business and technical contacts.

4.5 Plan Appendices

Contingency plan appendices provide key details not contained in the main body of the plan. Common contingency plan appendices include the following:

- Contact information for contingency planning team personnel;
- Vendor contact information, including offsite storage and alternate site POCs;
- BIA;
- Detailed recovery procedures and checklists;
- Detailed validation testing procedures and checklists;
- 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;
- Alternate mission/business processing procedures that may occur while recovery efforts are being done to the system;
- ISCP testing and maintenance procedures;
- System interconnections (systems that directly interconnect or exchange information); and
- Vendor SLAs, reciprocal agreements with other organizations, and other vital records.

[35] According to NIST SP 800-53 Contingency Plan security controls, a low-impact system is not required to have offsite data storage capabilities.

Chapter 5. Technical Contingency Planning Considerations

This chapter complements the process and framework guidelines presented in earlier sections by discussing technical contingency planning considerations for specific types of information systems. The information presented in this section will assist the reader in selecting, developing, and implementing specific technical contingency strategies based on the type of information system. Because each system is unique, considerations are provided at a level that may be used by the widest audience. The list of platforms is not comprehensive, but is representative of commonly found systems in production or development. Not all of the information presented may apply to a specific information system; the ISCP Coordinator should draw on the considerations as appropriate and customize them to meet a system's particular contingency requirements. The following representative platform types are addressed in this section:

- Client/server systems;
- Telecommunications systems; and
- Mainframe systems.

For each system type, contingency measures are considered from two perspectives. First, the document discusses technical requirements or factors that the ISCP Coordinator should consider when planning a system recovery strategy during the Development/Acquisition Phase of the SDLC.[36] Second, the document provides technology-based solutions for each type of system.

5.1 Common Considerations

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. When developing solutions for technical contingency plans, there are several areas that should be considered regardless of the platform or type of system. These considerations provide a common foundation for any type of contingency planning effort. Several of these contingency measures are common to all information systems. Common considerations include the following:

- Use of information gathered from the BIA process;
- Development of data security, integrity, and backup policies and procedures;
- Protection of equipment and system resources;
- Adherence and compliance with security controls in NIST SP 800-53;
- Development of primary and alternate sites with appropriately sized and configured power management systems and environmental controls; and
- Use of high availability (HA) processes to provide for online real-time resilient access to alternate system resources. HA denotes systems that can achieve an uptime of 99.999 percent or better. Note that HA is a process for achieving high availability and should not be confused with FIPS 199 high-impact category systems.

[36] An overview of contingency planning and the SDLC is presented in Appendix F.

5.1.1 Use of the BIA

The BIA is the first source for determining resiliency and contingency planning strategies. BIA results determine how critical the system is to the supported mission/business processes, what impact the loss of the system could have on the organization, and the system RTO. The BIA results can help determine the type and frequency of backup, the need for redundancy or mirroring of data, and the type of alternate site needed to meet system recovery objectives. Each of these strategy decisions have cost versus availability or recovery implications. Availability and recovery implications are discussed throughout the rest of this chapter.

5.1.2 Maintenance of Data Security, Integrity, and Backup

Maintaining the integrity and security of system data and software is a key component in contingency planning. Data integrity involves keeping data safe and accurate on the system's primary storage devices. There are several methods available to maintain the integrity of stored data. These methods use redundancy and fault tolerance processes to store data on more than one drive and eliminate loss of data from single drive failures. Data security involves protecting data both onsite and offsite from unauthorized access or use. Encryption is a common method for securing stored system data. Encryption is most effective when applied to both the primary data storage device and on backup media going to an offsite location.[37] If using encryption for offsite data storage, it is important that media readers (e.g., tape drives, CD or DVD readers) are available at the alternate site location to correctly read the encrypted data during recovery efforts. A solid key management process must be established so encrypted data is available as needed. Keying material, which is the data used to establish and maintain the keys, needs to be managed, ideally at a central location in the organization. These keys should be stored separate from, but accessible to, the primary encrypted backup data.[38]

Keeping backups of data in a secure offsite location allows for a ready access to backups during a contingency event. An effective data backup process is crucial to an ISCP Coordinator's overall recovery strategy. Data backups are done primarily for recovery purposes. Backups can be done through many different methods and techniques. MTD determinations and security requirements from the BIA help dictate the best method for backing up a particular system for recovery.

Data backups should be conducted on all systems on a regular basis. Systems can be backed up for individual computers or on a centralized storage device, such as network attached storage (NAS) or storage area network (SAN). There are three common methods for performing system backups:

- **Full.** A full backup captures all files on the disk or within the folder selected for backup. Because all backed-up files are recorded to a single media or media set, locating a particular file or group of files is simple. However, the time required to perform a full backup can be lengthy. In addition, maintaining multiple iterations of full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary media 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 an incremental backup, media from different backup operations may be required. For example, consider a case in which a directory needs to be recovered. If the last full backup was performed three days prior and one

[37] For further information on encryption, see NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, December 2005.
[38] For further information on key management, see NIST SP 800-57, *Recommendation for Key Management*, March 2007.

file had changed each day, then the media for the full backup and 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 after the previous full backup, a differential backup will save the file each time until the next full backup is completed. A differential backup takes less time to complete than a full backup. Restoring from a differential backup may require fewer media than an incremental backup because only the full backup media and the last differential media would be needed. As a disadvantage, differential backups take longer to complete than incremental backups because the amount of data since the last full backup increases each day until the next full backup is executed.

A combination of backup operations can be used depending on system configuration and recovery requirements. For example, a full backup can be conducted on the weekend with differential backups conducted each evening. In developing a system backup policy, the following questions should be considered:

- Where and how will media be stored?
- What data should be backed up and how often should it be backed up?
- How quickly are the backups to be retrieved in the event of an emergency?
- Who is authorized to retrieve the media?
- Where will the media be delivered and what is the rotation schedule of backup media?
- Who will restore the data from the media?
- What is the media-labeling scheme?
- How long will the backup media be retained?
- When the media are stored onsite, what environmental controls are provided to preserve the media?
- What is the appropriate backup medium for the types of backups to be performed?

Certain factors should be considered when choosing the appropriate backup solution:

- **Equipment interoperability.** To facilitate recovery, the backup device must be compatible with the platform operating system and applications and should be easy to install onto different models or types of systems.
- **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 medium 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 back up data should be considered. In some cases, the backup solution 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.

5.1.3 Protection of Resources

Part of a successful contingency planning policy is making a system resilient to environmental and component-level failures that would otherwise cause system disruptions. There are several methods for making valuable hardware and software resilient. Determination of the appropriate methods should be based on risk-informed decisions. Depending on results of the risk management process, these methods may or may not be applicable for a particular system.

The system and its data can become corrupt as a result of a power failure. Critical hardware, such as servers, can be configured with dual power supplies to prevent corruption. The two power supplies should be used simultaneously 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, a UPS can protect the system if power is lost. A UPS usually provides 30 to 60 minutes of temporary backup power to permit a graceful shutdown. A UPS can also protect against power fluctuations by filtering incoming power and providing a steady power source. 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 configured to start automatically when a power interruption is detected. A combination UPS/generator system can provide clean, secure power for a system as long as fuel is available for the generator. Fuel availability should be considered for those who opt for a UPS/generator to support their system environment.

In addition to backing up data, organizations should also back up system software and drivers. Organizations should store software and software licenses in an alternate location. This includes original installation media, license terms and conditions, and license keys, if required. Image loads for client systems (such as desktops and portable systems) should also be backed up and stored at an alternate location, along with complete documentation of the software included in the image load, any configuration information for the type of computer for which the image is intended, and installation instructions.

Organizations may use third-party vendors to recover data from failed storage devices. Organizations should consider the security risk of having their data handled by an outside company and ensure that proper security vetting of the service provider is conducted before turning over equipment. The service provider and employees should sign non disclosure agreements, be properly bonded, and adhere to organization-specific security policies.

5.1.4 Adherence to Security Controls

The security controls established in NIST SP 800-53 provide a solid foundation for establishing information system security, integrity, and contingency policies. Adherence to these controls for contingency planning purposes helps protect an information system against threats that can disrupt operations.

5.1.5 Identification of Alternate Storage and Processing Facilities

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. The ISCP Coordinator should reference the organization's resilience policy and the BIA to assist in determining how often backup media should be tested. 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 organization develop an effective media marking and tracking strategy.

Alternate processing facilities provide a location for an organization to resume system operations in the event of a catastrophic event that disables or destroys the systems primary facility. There are three primary types of alternate processing facilities, corresponding to the level of readiness to function as a system's operations facility.

- **Cold Sites.** Cold sites are locations that have the basic infrastructure and environmental controls available (such as electrical and HVAC), but no equipment or telecommunications established or in place. There is sufficient room to house needed equipment to sustain a system's critical functions. Examples of cold sites include unused areas of a data center and unused office space (if specialized data center environments are not required). Cold sites are normally the least expensive alternate processing site solution, as the primary costs are only the lease or maintenance of the required square footage for recovery purposes. However, the recovery time is the longest, as all system equipment (including telecommunications) will need to be acquired or purchased, installed, tested, and have backup software and data loaded and tested before the system can be operational. Depending on the size and complexity of a system, recovery could take several days to weeks to complete.

- **Warm Sites.** Warm sites are locations that have the basic infrastructure of cold sites, but also have sufficient computer and telecommunications equipment installed and available to operate the system at the site. However, the equipment is not loaded with the software or data required to operate the system. Warm sites should have backup media readers that are compatible with the system's backup strategy. Warm sites may not have equipment to run all systems or all components of a system, but rather only enough to operate critical mission/business processes. An example of a warm site is a test or development site that is geographically separate from the production system. Equipment may be in place to operate the system, but would require reverting to the current production level of the software, loading the data from backup media, and establishing communications to users. Another example is available equipment at an alternate facility that is running noncritical systems and that could be transitioned to run a critical system during a contingency event. A warm site is more expensive than a cold site, as equipment is purchased and maintained at the warm site, with telecommunications in place. Some costs may be offset by using equipment for noncritical functions or for testing. Recovery to a warm site can take several hours to several days, depending on system complexity and the amount of data to be restored.

- **Hot Sites.** Hot sites are locations with fully operational equipment and capacity to quickly take over system operations after loss of the primary system facility. A hot site has sufficient equipment and the most current version of production software installed, and adequate storage for the production system data. Hot sites should have the most recent version of backed-up data loaded, requiring only updating with data since the last backup. In many cases, hot site data and databases are updated concurrently with or soon after the primary data and databases are updated. Hot sites also need a way to quickly move system users' connectivity from the primary site. One example of a hot site is two identical systems at alternate locations that are in production, serving different geographical locations or load balancing production workload. Each location is built to handle the full workload, and data is continuously synchronized between the systems. This is the most expensive option, requiring full operation of a system at an alternate location and all telecommunications capacity, with the ability to maintain or quickly update the operational data and databases. Hot sites also require having operational support nearly equal to the production

The ISCP Coordinator should look at information provided in the BIA to determine what critical mission/business processes a system supports, the MTD, and the impact loss of the system would have on the business to establish what type of recovery site is needed. An information system recovery strategy may incorporate one or more of these types of alternate processing facilities. For example, some functionality of a system may be highly critical and require a hot site to minimize the downtime and impact on mission/business processes. However, other functionality of the same system, such as a reporting or batch printing process, may be able to be down for several days with little impact and would just need extra space in the alternate facility to place additional equipment after it is purchased.

5.1.6 Use of High Availability (HA) Processes

HA is a process where redundancy and failover processes are built into a system to maximize its uptime and availability. The concept of HA is to achieve an uptime of 99.999 percent or higher, which equates to just a few minutes per year of downtime. Several vendors offer HA products and services designed to minimize downtime by building redundancy and resiliency into the architecture.

HA can be an expensive option for systems, with duplicate hardware and special failover software to eliminate any single point of failure. Normally, there are higher cost maintenance and support requirements associated with HA systems. Therefore, HA is not a viable option for many systems and should be considered only for those systems that cannot tolerate downtime. Examples of this may be air traffic systems and financial systems. Also, HA systems cannot be a replacement for a solid backup strategy, as a corruption of data on a system may propagate through an HA system, making the system unusable. Without a backup of the system separate from the system itself, recovery may not be possible.

HA can be implemented at a single site, with all system redundancy resident at that site. This will keep the system running at an HA level as long as there is no interruption of the facility housing the system. However, when implementing HA products or services in a system, the ISCP Coordinator should have HA processes extended to an alternate location. Mechanisms such as block mirroring to an alternate site should be considered to provide redundancy and backup of system data outside of the system facility. Whenever a write is made to a block on a primary storage device, the same write is made to an alternate storage device, either within the same storage system, or between separate storage systems, at different locations.

5.2 Client/Server Systems

Client/server systems can have processing and data at both the server and client workstation levels. Client workstations are normally desktop computers, although portable devices may be connected to servers as clients. Portable devices include laptops, notebook computers, and handheld devices (e.g., smart phones and specialized equipment such as inventory collection bar code readers).

Wireless and smart phone technology advances have allowed users access to key server functionality and services such as email from their mobile phones. This is normally done by using proprietary third-party software that establishes the communications and data transfer to and from the phone via the network provided by mobile cell carriers.

Servers support file sharing and storage, data processing, central application hosting (such as email or a central database), printing, access control, user authentication, remote access connectivity, and other

shared system services. Local users log into the server through networked client machines to access resources that the server provides.

5.2.1 Client/Server Systems Contingency Considerations

Contingency considerations for client/server systems should emphasize data availability, confidentiality, and integrity at both the server system level and the client level. To address these requirements, regular and frequent backups of data should be stored offsite. Specifically, the system manager should consider each of the following practices for client/server systems:

- **Store backups offsite or at an alternate site**. As mentioned in Section 3.4.2, backup media should be stored offsite or at an alternate site in a secure, environmentally controlled facility.
- **Standardize hardware, software, and peripherals**. System recovery is faster if hardware, software, and peripherals are standardized throughout the organization. Additionally, critical hardware components that need to be recovered immediately in the event of a disaster should be compatible with off-the-shelf computer components. This compatibility 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 for vendors that supply essential hardware, software, and other components should be listed in the contingency plan so that replacement components may be purchased quickly.
- **Coordinate with security policies and system security controls.** Client/server contingency solutions should be coordinated with security policies and system security controls. In choosing the appropriate technical contingency solution, similar security controls and security-related activities (e.g., risk assessment, vulnerability scanning) applied in the production system should be implemented in the contingency solution to ensure that executing the system contingency solution does not compromise or disclose sensitive data during a system disruption or emergency.
- **Use results from the BIA.** Impacts and priorities of associated information systems discovered through the BIA should be reviewed to determine related requirements.

> CLIENT/SERVER AND PORTABLE SYSTEM CONTINGENCY STRATEGIES:
>
> - STORE BACKUPS OFFSITE/ALTERNATE SITE.
> - STANDARDIZE HARDWARE, SOFTWARE, AND PERIPHERALS.
> - DOCUMENT SYSTEM CONFIGURATIONS AND VENDOR INFORMATION.
> - COORDINATE WITH SECURITY POLICIES AND CONTROLS.
> - USE RESULTS OF BIA.
> - MINIMIZE DATA ON CLIENT SYSTEMS.
> - AUTOMATE BACKUP OF DATA.
> - DEVELOP AND PROVIDE GUIDANCE ON BACKING UP DATA.
> - STORE BACKUP INFORMATION AT AN ALTERNATE SITE.
> - COORDINATE CONTINGENCY SOLUTIONS WITH CYBER INCIDENT RESPONSE PROCEDURES.

Additional considerations for client computers include:

- **Minimize the amount of data stored on a client computer.** Critical user data should be stored on central servers that are backed up as part of an organization's enterprise backup strategy, rather than on the client computer hard drive.

- **Automate backup of data**. Client/server systems should have software installed that automatically schedules data backups to a central data backup location. Data for backup should be stored at a common directory name (such as \My Documents) to ease in automated backup and to make sure that only pertinent data is backed up. If the client system backup process is not automated from the network, users should be encouraged to back up data on a regular basis. Automated backup schedulers should be set up for stand-alone desktops and portable devices whenever possible.
- **Provide guidance on saving data on client computers**. Instructing users to save data to a particular folder on the computer eases the IT department's client support requirements. If a machine must be rebuilt, the technician will know which folders to copy and preserve during recovery.
- **Store backup information at an alternate site.** 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. Software licenses and original system software, vendor SLAs and contracts, and other important documents relevant to the stand-alone should be stored with the backup media. 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 contingency event.

Contingency considerations for servers in a client/server system rely extensively on LAN and WAN connectivity to communicate with their clients. Because of this, server components must consider system contingency measures similar to those for LANs and WANs.

- **Standardize hardware, software, and peripherals.** System recovery may be expedited if hardware, software, and peripherals are standardized throughout the client/server 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 server architecture and the configurations of its various components. In addition, the contingency plan should identify vendors and model specifications to facilitate rapid equipment replacement after a disruption.
- **Coordinate with security policies and security controls.** Server contingency solution(s) should be coordinated with network security policies where similar security controls and security-related activities (e.g., risk assessment, vulnerability scanning) in the production environment should be implemented in the contingency solution(s) to ensure that, during a system disruption, executing the technical contingency solution(s) does not compromise or disclose sensitive data. Security of data within a client/server system is key as most systems are multi-tenancy, having multiple users and applications residing on the same system, with different security requirements and controls.
- **Coordinate contingency solutions with cyber incident response procedures.** Because many application servers use Web services to provide an image of the organization to the public, the organization's public image could be damaged if the application server were defaced or taken down by a cyber attack. To reduce the consequences of such an attack, contingency solutions should be coordinated closely with cyber incident response procedures designed to limit the impacts of a cyber attack.
- **Use results from the BIA.** Impacts and priorities discovered through the BIA of associated LANs and/or WANs should be reviewed to determine recovery requirements and priorities.

5.2.2 Client/Server Systems Contingency Solutions

Wide ranges of technical contingency solutions are available for client/server systems; several efficient practices are discussed in this section.

Encryption is a popular security tool used on client devices. With increased use of digital signatures for non-repudiation and the use of encryption for confidentiality and/or integrity, organizations should consider including encryption in their backup strategy. Encryption should also be considered for backup media that goes offsite for storage, to secure data should it be lost or stolen en route or at the alternate site.

If encrypted data is sent offsite for storage, there should be a cryptographic key management system in place to make sure the data is readable if it needs to be recovered onto a new or replaced system. The cryptographic key and the encryption software both need to be on the new system, along with the keying material. Keying material is the data, such as the keys and initialization points for encryption, used to establish and maintain the encryption parameters. The keying material can be stored at a central location (such as an enterprise key management and encryption system) or on removable media separate from the backup media itself.[39]

Client/server system data backups can be accomplished in various ways, including those listed below:[40]

- **Digital video disc (DVD).** DVD-read only memory (DVD-ROM) drives come standard in most desktop computers; however, not all computers are equipped with writable DVD-ROM drives. DVDs are low-cost storage media and have a higher storage capacity of around 4.7 gigabytes (GB). To read from a DVD-ROM, the operating system's file manager is sufficient; to write to a DVD-ROM, a rewritable DVD (DVD-RW) drive and the appropriate software are required.
- **Network Storage.** Data stored on networked client/server systems can be backed up to a networked disk. The amount of data that can be backed up from a client/server system is limited by the network disk storage capacity or disk allocation to the particular user. 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. Common types of network storage architecture include network attached storage (NAS) and storage area network (SAN). These storage systems incorporate resiliency and redundancy within their design and can be configured to maintain redundancy across several locations.
- **External Hard Drives.** Data replication or synchronization to an external hard drive is a common backup method for portable computers and stand-alone devices. Handheld devices or laptops may be connected to an external hard drive and replicate the desired data from the portable device to the external hard drive. Many external hard drives have backup software included for use in backing up primary drives.
- **Internet Backup.** Internet Backup, or Online Backup, is a commercial service that allows desktop and portable device users to back up data to a remote location over the Internet for a fee. A utility is installed onto the desktop or portable device 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 overwritten. Data can be encrypted for transmission; however, this will impede the data transfer. The advantage of Internet Backup is that the user is not required to purchase data

[39] For more information on encryption for desktops and portable devices, refer to NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, November 2007.
[40] Section 5.1.2 discusses various backup methods that can be used: full, incremental, and differential.

backup hardware or media and that the data is readily available to be downloaded for recovery in a contingency situation.

Servers normally have much larger amounts of data that need to be maintained and secured. It is recommended in environments with multiple servers, that storage not be dedicated to each server but rather centralized for use by multiple servers. SAN and NAS are common multi-server storage systems. Centralizing the data of multiple servers allows for a common backup of data for offsite storage. Given the large amount of data that must be backed up, it is recommended that a separate and dedicated network be used just for the data transfers required for backing up data. This will enable the primary network to be dedicated to production traffic, and not impact the backup process.

Contingency solutions may be built into the client/server system during design and implementation. A client/server system, for example, 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 client/server 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 hourly from local sites to the headquarters' site, then the headquarters' server would act as a backup for the local servers.

As the example above illustrates, the client/server 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 organization's 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.

If considering the use of remote sites for system backups, or the use of Internet or other means of backup, the ISCP Coordinator should ensure that the remotely hosted storage services can provide the same level of protection of data as the original site. This can be done through SLAs and periodic reviews and assessments of the remote storage facility and processes.

5.3 Telecommunications Systems

There are two primary classes of telecommunications systems: LANs and WANs. Wireless connectivity, prevalent for use with portable devices, can be used in either LAN or WAN environments.

A LAN is located within an office or campus environment. It can be as small as two PCs attached to a single network switch, or it may support hundreds of users and multiple servers. LANs can be developed using any of several topologies. Each connection on a LAN is considered a node.

A WAN is a data communications network that consists of connecting two or more systems that are dispersed over a wide geographical area. Communications links, usually provided by a public carrier, provide the connection to enable one system to interact with other systems.

WANs can connect LANs together, connect to mainframe systems, and connect client computers to servers. WANs provide much of the communications requirements of geographically dispersed environments. Types of WAN communications links include the following methods:

- **T-1.** T-1 is a dedicated phone connection supporting data rates of 1.544 Megabits per second (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 communications links also can be provided when multiples of 64-kbps lines are required.

- **T-3.** T-3 is a dedicated phone connection supporting data rates of about 45 Mbps. A T-3 line consists of 672 individual channels, each of which supports 64 kbps. T-3 is also referred to as a Digital Signal (DS) 3.
- **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.
- **Asynchronous Transfer Mode (ATM).** 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 and provide guaranteed throughput.
- **Synchronous Optical Network (SONET).** SONET is the standard for synchronous data transmission on optical media. SONET supports gigabit transmission rates.

5.3.1 Telecommunications Contingency Considerations

When developing the telecommunications recovery strategy, the ISCP Coordinator should apply considerations that were provided in Section 5.2.1 regarding client/server systems. In addition, the following practices should be considered:

- **Telecommunications documentation.** Physical and logical telecommunications diagrams should be up to date. The physical diagram should display the physical layout of the facility that houses the LAN and/or WAN, and cable jack numbers should be documented on the physical diagram. Diagrams should also identify network-connecting devices, IP addresses, Domain Name System (DNS) names, and types of communications links and vendors. The logical diagram should present the telecommunications infrastructure and its nodes. Network discovery software can provide an accurate picture of the telecommunications environment. Both diagrams help recovery personnel to identify where problems have occurred and to restore telecommunications services more quickly.
- **System configuration and vendor information documentation.** Document configurations of network connective devices that facilitate telecommunication (e.g., circuits, switches, bridges, and hubs) to ease recovery. Vendors and their contact information should be documented in the contingency plan to provide for prompt hardware and software repair or replacement. The plan also should document the communications providers, including POC and contractual or SLA information.
- **Coordinate with security policies and security controls.** Telecommunications contingency solution(s) should be coordinated with network security policies to protect against threats that could disrupt the network. Therefore, in choosing the appropriate technical telecommunications contingency solution(s), similar security controls and security-related activities (e.g., risk

> TELECOMMUNICATIONS CONTINGENCY STRATEGIES:
>
> - DOCUMENT TELECOMMUNICATIONS NETWORKS.
> - COORDINATE WITH VENDORS.
> - COORDINATE WITH SECURITY POLICIES AND CONTROLS.
> - IDENTIFY SINGLE POINTS OF FAILURE.
> - IMPLEMENT REDUNDANCY IN CRITICAL COMPONENTS.
> - MONITOR TELECOMMUNICATIONS NETWORKS.
> - INTEGRATE REMOTE ACCESS AND WIRELESS LOCAL AREA NETWORK TECHNOLOGY.

assessment, vulnerability scanning) in the production systems should be implemented in the contingency solution(s) to ensure that, during a network disruption, executing the technical contingency solution(s) does not compromise or disclose sensitive data.

- **Use results from the BIA.** Impacts and priorities discovered through the BIA of associated systems should be reviewed to determine telecommunications recovery priorities. The BIA should identify the high-availability FIPS 199 impact levels for any data networks and email that support COOP Mission, Primary, or National Essential Functions.

5.3.2 Telecommunications Contingency Solutions

While similar contingencies exist for both LAN and WAN telecommunications systems, there are different strategies and solutions the ISCP Coordinator should consider when determining an overall telecommunications recovery strategy. Differences in solutions primarily exist due to geographic and connectivity ownership. While LANs are typically in small areas (offices or campuses) and the routing and wiring is owned or managed by the organization, WANs typically rely on network service providers (NSPs) for both routing and wiring.

When developing an ISCP for a LAN, the ISCP Coordinator should identify single points of failure that affect critical systems or processes outlined in the BIA. This analysis could include threats to the cabling system, such as cable cuts, electromagnetic and radio frequency interference, and damage resulting from 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 might be cost-effective to install a gigabit cable between floors so that hosts on both floors could be reconnected if the primary cable were cut.

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 failed.

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, primarily through a virtual private network (VPN). If an emergency or serious system disruption occurs, 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. Additionally, security controls such as multifactor authentication and data encryption should be implemented if the communications contain FIPS 199 moderate- or high-impact information. Remote access will work only if the remote access server and the network are both functioning at either the primary or the alternate location.

Wireless (or WiFi) local area networks 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 data over a radio signal, enabling the data to be intercepted. When implementing a wireless network, security controls, such as data encryption, should be employed if the communications traffic contains FIPS 199 moderate- or high-impact information. Wireless LANs allow for quick temporary access of portable devices, which typically have wireless antennae built into them.

Wireless routers commonly provide password authentication and transmission encryption as standard features.[41]

For organizations considering remote connectivity, several security requirements and guidelines must be implemented. This includes verification of a user's identity through electronic authentication, or e-authentication. E-authentication guidelines provide four basic levels of protection, from minimal identity verification (Level 1) to cryptographic two-factor authentication keys (Level 4). NIST SP 800-63, *Electronic Authentication Guideline*,[42] provides more information on the four levels and implementing e-authentication into a system.[43]

WAN contingency solutions include all of the measures discussed for client/server systems and LANs. In addition, WAN contingency planning must consider the communications links that connect the disparate systems. WAN contingency strategies are influenced by the type of data routed on the network. A WAN that hosts a mission-critical system (see Section 5.4) may require a 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-1 connections, or the backup link could provide reduced bandwidth to accommodate only critical transmissions in a contingency situation. For example, an Integrated Services Digital Network (ISDN) line with a bandwidth of 128Kbps could be used as a contingency communications link for a primary T-1 connection. If redundant links are used, the ISCP Coordinator 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 near 100 percent connectivity is required, redundant communications links can be provided through multiple NSPs. If this solution is chosen, the ISCP Coordinator should ensure that the NSPs do not share common facilities at any point, including building entries or demarcations (places where the WAN connection ends within a facility).
- **Redundant network-connecting devices.** Duplicate network-connecting devices, such as routers, switches, and firewalls, can create high availability at the LAN interfaces and provide redundancy if one device fails. Duplicate devices also provide load balancing in routing traffic.
- **Redundancy from NSP or Internet Service Provider (ISP).** The ISCP Coordinator should consult with the selected NSP or ISP to assess the robustness and reliability within their core networks (e.g., redundant network-connecting devices and power protection).

To reduce the effects of a telecommunications disruption through prompt detection, monitoring software can be installed. The monitoring software issues an alert if a node or connection 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 or email to a designated individual(s) automatically when a system parameter falls out of its specification range.

---

[41] See NIST SP 800-97, *Establishing Wireless Robust Security Networks*: *A Guide to IEEE 802.11i*, for information on establishing and maintaining a robust security wireless network.

[42] NIST SP 800-63 is supported by OMB M-04-04, *E-Authentication Guidance for Federal Agencies (December, 16, 2003)*, which establishes rules and regulations regarding e-authentication in federal systems.

[43] NIST SP 800-53 control IA-2 (Identification and Authentication [Organizational Users]) also provides guidance and reference to remote access of systems. Depending on the impact level of the system, certain control enhancements in IA-2 must be incorporated as part of remote and WiFi user identification and authentication.

SLAs can facilitate prompt recovery following software or hardware problems associated with the telecommunications. An SLA also may be developed with the NSP or ISP to guarantee the desired network availability and establish tariffs if the vendor's network is 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.

5.4 Mainframe Systems

Unlike the client/server architecture, the mainframe architecture is centralized. The clients that access the mainframe are terminals with no processing or data storage capabilities. All the processing power for the system is within the mainframe itself. The terminals accept output only from the mainframe. Early on, these terminals were primarily monitors and keyboards without processors. Now, however, mainframes normally do not have traditional terminals. Instead, desktops and portable computers access mainframes through the use of terminal emulation software.

A mainframe is a multiuser computer designed to meet the computing needs of a large organization. The term (*mainframe*) was created to describe the large central computers developed in the late 1950s and 1960s to perform bulk accounting and information management functions. Mainframe systems store all data in a central location rather than dispersing data among multiple machines.

5.4.1 Mainframe Contingency Considerations

Although processing on a mainframe computer is more powerful and centralized than on other types of platforms, 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 media offsite.** Backup media should be labeled, logged, and 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. Additionally, depending on the FIPS 199 impact level, data encryption may be required for protecting system backup information while in transit and at rest to minimize the risk if backup media is lost or stolen.
- **Document system configurations and vendors.** Maintaining detailed records of system configurations enhances system recovery capabilities. In addition, 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 include duplicating interfaces and telecommunications infrastructure as well as coordinating with network security policies, such as stringent access controls.
- **Utilize results from the BIA.** Impacts and priorities identified through the BIA of associated systems supporting organizational critical mission/business processes should be reviewed to determine recovery requirements and priorities.

5.4.2 Mainframe Contingency Solutions

Mainframes require different contingency strategies from 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. UPS and power monitoring and management systems also should be used to ensure that 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 direct access storage devices (DASDs) by implementing a RAID solution.

Because each mainframe architecture is unique and centralized, a contingency strategy is to have a replacement system available at an alternate warm or hot site. Since backup mainframe platforms are very costly to purchase and maintain, many agencies share commercial systems.[44] Agencies also typically maintain vendor-support contracts to repair damaged units. However, vendor support alone may not restore system functions within the allowable outage time. In all cases, vendor SLAs 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 regularly, and backup media should be stored offsite. Backup and retention schedules should be based on the criticality of the data being processed and 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. In addition, disk replication, virtualization, or NAS or SAN technologies that replicate various platforms to one replicating server could be used in some cases.

5.5 System Contingency Planning Considerations Summary

For information system contingency planning, the ISCP Coordinator should consider technical measures from two perspectives when planning a system recovery strategy:

- Contingency considerations discuss technical requirements or factors to complement the contingency solution.
- Contingency solutions are technically based and are used to implement the contingency strategy.

Table 5-1 provides a summary of contingency considerations and solutions.

[44] The GSA's Federal Technology Service Federal Computer Acquisition Center has a governmentwide acquisition contract on behalf of the federal government. The program has been in place since 1993 and provides disaster recovery services to more than forty federal organizations.

Table 5-1: Summary

	Client/Server System	Telecommunications System	Mainframe System
Contingency Consideration			
Document System, Configurations, and Vendor Information	X	X	X
Encourage Individuals to Back Up Data	X		
Coordinate Contingency Solution with Security Policy	X	X	X
Coordinate Contingency Solution with System Security Controls	X	X	X
Consider Hot Site and Reciprocal Agreements	X		X
Coordinate With Vendors		X	X
Institute Vendor SLAs	X	X	X
Provide Guidance on Saving Data on Personal Computers	X		
Standardize Hardware, Software, and Peripherals	X		
Store Backup Media Offsite	X	X	X
Store Software Offsite	X	X	X
Contingency Solution			
Back Up System, Applications, and/or Data	X	X	X
Ensure Interoperability Among Components	X		
Identify Single Points of Failure		X	
Image Disks	X		
Implement Fault Tolerance in Critical Components			X
Implement Load Balancing	X		X
Implement Redundancy in Critical Components	X	X	X
Implement Storage Solutions			X
Integrate Remote Access and Wireless Technologies	X	X	
Replicate Data	X		X
Use Uninterruptible Power Supplies	X		X

Appendix A—Sample Information System Contingency Plan Templates

Sample templates are provided to address NIST SP 800-53 security controls for each of the three different FIPS 199 impact levels. The templates provided are guides and may be customized and adapted as necessary to best fit the system or organizational requirements for contingency planning. Appendix A.1 can be used for low-impact systems, Appendix A.2 for moderate- impact systems, and Appendix A.3 for high-impact systems.

A.1 Sample Template for Low-Impact Systems

{System name}

Security Categorization: Low

{Organization Name}

Information System Contingency Plan (ISCP)

Version [Insert #]

[Date]

Prepared by

[Organization Name]
[Street Address]
[City, State, and Zip Code]

TABLE OF CONTENTS

Plan Approval……A.1-3

1. Introduction ……A.1-4

1.1 Background……A.1-4
1.2 Scope……A.1-4
1.3 Assumptions……A.1-4

2. Concept of Operations ……A.1-5

2.1 System Description……A.1-5
2.2 Overview of Three Phases……A.1-5
2.3 Roles and Responsibilities……A.1-5

3. Activation and Notification……A.1-6

3.1 Activation Criteria and Procedure ……A.1-6
3.2 Notification……A.1-6
3.3 Outage Assessment……A.1-6

4. Recovery……A.1-7

4.1 Sequence of Recovery Activities ……A.1-7
4.2 Recovery Procedures ……A.1-8
4.3 Recovery Escalation Notices/Awareness……A.1-8

5. Reconstitution……A.1-8

5.1 Validation Data Testing……A.1-8
5.2 Validation Functionality Testing……A.1-8
5.3 Recovery Declaration……A.1-8
5.4 Notification (users)…… ……A.1-8
5.5 Cleanup ……A.1-8
5.6 Data Backup……A.1-8
5.7 Event Documentation……A.1-9
5.8 Deactivation……A.1-9

APPENDICES

Plan Approval

Provide a statement in accordance with the agency's contingency planning policy to affirm that the ISCP is complete and has been tested sufficiently. The statement should also affirm that the designated authority is responsible for continued maintenance and testing of the ISCP. This statement should be approved and signed by the system designated authority. Space should be provided for the designated authority to sign, along with any other applicable approving signatures. Sample language is provided below:

As the designated authority for *{system name}*, I hereby certify that the information system contingency plan (ISCP) is complete, and that the information contained in this ISCP provides an accurate representation of the application, its hardware, software, and telecommunication components. I further certify that this document identifies the criticality of the system as it relates to the mission of the *{organization}*, and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

I further attest that this ISCP for *{system name}* will be tested at least annually. This plan was last tested on *{insert exercise date}*; the test, training, and exercise (TT&E) material associated with this test can be found *{TT&E results appendix or location}*. This document will be modified as changes occur and will remain under version control, in accordance with *{organization}*'s contingency planning policy.

_____ _____

{System Owner Name} Date
{System Owner Title}

1. Introduction

Information systems are vital to {*Organization's*} mission/business processes; therefore, it is critical that services provided by *{system name}* are able to operate effectively without excessive interruption. This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover {*system name}* quickly and effectively following a service disruption.

1.1 Background

This *{system name}* ISCP establishes procedures to recover *{system name}* following a disruption. The following recovery plan objectives have been established:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - ***Activation and Notification phase*** to activate the plan and determine the extent of damage;
  - ***Recovery phase*** to restore *{system name}* operations; and
  - ***Reconstitution phase*** to ensure that *{system name}* is validated through testing and that normal operations are resumed.
- Identify the activities, resources, and procedures to carry out {*system name}* processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated *{organization name}* personnel and provide guidance for recovering *{system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other personnel responsible for *{organization name}* contingency planning strategies. Ensure coordination with external points of contact and vendors associated with *{system name}* and execution of this plan.

1.2 Scope

This ISCP has been developed for *{system name}*, which is classified as a low-impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – *Standards for Security Categorization of Federal Information and Information Systems.* Procedures in this ISCP are for Low-Impact systems and designed to recover {*system name}* within *{RTO hours}*. This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than *{RTO hours};* or loss of data at the onsite facility or at the user-desktop levels. As *{system name}* is a low-impact system, alternate data storage and alternate site processing are not required.

1.3 Assumptions

The following assumptions were used when developing this ISCP:

- *{System name}* has been established as a low-impact system, in accordance with *FIPS 199.*
- Alternate processing sites and offsite storage are not required for this system.
- The *{system name}* is inoperable and cannot be recovered within *{RTO 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.
- *Additional assumptions as appropriate.*

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

- **Overall recovery and continuity of mission/business operations.** The Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) address continuity of mission/business operations.
- **Emergency evacuation of personnel.** The Occupant Emergency Plan (OEP) addresses employee evacuation.
- *Any additional constraints and associated plans should be added to this list.*

2. Concept of Operations

The Concept of Operations section provides details about *{system name}*, an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of {*Organization's*} personnel during a contingency activation.

2.1 System Description

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures.

2.2 Overview of Three Phases

This ISCP has been developed to recover and reconstitute the *{system name}* using a three-phased approach. This approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions.

The three system recovery phases are:

Activation and Notification Phase – Activation of the ISCP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss.

Once the ISCP is activated, system owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

Recovery Phase – The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.

Reconstitution –The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing.

Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

2.3 Roles and Responsibilities

The ISCP establishes several roles for *{system name}* recovery and reconstitution support. Persons or teams assigned ISCP roles have been trained to respond to a contingency event affecting *{system name}*.

Describe each team and role responsible for executing or supporting system recovery and reconstitution. Include responsibilities for each team/role, leadership roles, and coordination with other recovery and reconstitution teams, as applicable. At a minimum, a role should be established for a system owner or business unit point of contact, a recovery coordinator, and a technical recovery point of contact.

Leadership roles should include an ISCP Director, who has overall management responsibility for the plan, and an ISCP Coordinator, who is responsible to oversee recovery and reconstitution progress, initiate any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate.

3. Activation and Notification

The Activation and Notification Phase defines initial actions taken once a *{system name}* disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ISCP. At the completion of the Activation and Notification Phase, *{system name}* ISCP staff will be prepared to perform recovery measures.

3.1 Activation Criteria and Procedure

The *{system name}* ISCP may be activated if one or more of the following criteria are met:

1. The type of outage indicates *{system name}* will be down for more than *{RTO hours};*
2. The facility housing *{system name}* is damaged and may not be available within *{RTO hours}; and*
3. *Other criteria, as appropriate.*

The following persons or roles may activate the ISCP if one or more of these criteria are met:

Establish one or more roles that may activate the plan based on activation criteria. Authorized persons may include the system or business owner, or the operations point of contact (POC) for system support.

3.2 Notification

The first step upon activation of the *{system name}* ISCP is notification of appropriate mission/business and system support personnel. Contact information for appropriate POCs is included in *{Contact List Appendix name}*.

For *{system name}*, the following method and procedure for notifications are used:

Describe established notification procedures. Notification procedures should include who makes the initial notifications, the sequence in which personnel are notified (e.g., system owner, technical POC, ISCP Coordinator, business unit or user unit POC, and recovery team POC), and the method of notification (e.g., email blast, call tree, automated notification system, etc.).

3.3 Outage Assessment

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. This outage assessment is conducted by *{name of recovery team}*. Assessment results are provided to the ISCP Coordinator to assist in the coordination of the recovery of *{system name}*.

Outline detailed procedures to include how to determine the cause of the outage; identification of potential for additional disruption or damage; assessment of affected physical area(s); and determination of the physical infrastructure status, IS equipment functionality, and inventory. Procedures should include notation of items that will need to be replaced and estimated time to restore service to normal operations.

4. Recovery

The Recovery Phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, *{system name}* will be functional and capable of performing the functions identified in Section 2.1 of this plan.

4.1 Sequence of Recovery Activities

The following activities occur during recovery of *{system name}:*

Modify the following list as appropriate for the selected system recovery strategy.

1. Identify recovery location (if not at original location);
2. Identify required resources to perform recovery procedures;
3. Retrieve backup and system installation media;
4. Recover hardware and operating system (if required); and
5. Recover system from backup and system installation media.

4.2 Recovery Procedures

The following procedures are provided for recovery of *{system name}* at the original location. Recovery procedures are outlined per team and should be executed in the sequence presented to maintain an efficient recovery effort.

Provide general procedures for the recovery of the system from backup media. If an alternate location is part of the recovery strategy, include procedures for recovery to that site. Specific keystroke level procedures may be provided in an appendix. If specific procedures are provided in an appendix, a reference to that appendix should be included in this section. Teams or persons responsible for each procedure should be identified.

4.3 Recovery Escalation Notices/Awareness

Provide appropriate procedures for escalation notices during recovery efforts. Notifications during recovery include problem escalation to leadership and status awareness to system owners and users. Teams or persons responsible for each escalation/awareness procedure should be identified.

5. Reconstitution

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

5.1 Validation Data Testing

Validation data testing is the process of testing and validating data to ensure that data files or databases have been recovered completely at the permanent location. The following procedures will be used to determine that the data is complete and current to the last available backup:

Provide procedures for testing and validation of data to ensure that data is correct and up to date. This section may be combined with the Functionality Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a validation data test for a low-impact system would be to see if the last known complete transaction was updated in the database. Detailed data test procedures may be provided in Appendix E, System Validation Test Plan.

5.2 Validation Functionality Testing

Validation functionality testing is the process of verifying that *{system name}* functionality has been tested, and the system is ready to return to normal operations.

Provide system functionality testing and/or validation procedures to ensure that the system is operating correctly. This section may be combined with the Data Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a functional test for a low-impact system may be logging into the system and running a report or performing a transaction to see if the system is operating correctly. Detailed functionality test procedures may be provided in Appendix E, System Validation Test Plan.

5.3 Recovery Declaration

Upon successfully completing testing and validation, the *{system owner}* will formally declare recovery efforts complete, and that *{system name}* is in normal operations. *{System name}* business and technical POCs will be notified of the declaration by the ISCP Coordinator.

5.4 Notifications (users)

Upon return to normal system operations, {*system name*} users will be notified by *{role}* using *predetermined notification procedures (e.g., email, broadcast message, phone calls, etc.).*

5.5 Cleanup

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manuals or other documentation to their original locations, and readying the system for a possible future contingency event.

Provide any specific cleanup procedures for the system including preferred locations for manuals and documents and returning backup or installation media to its original location.

5.6 Data Backup

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are:

Provide appropriate procedures for ensuring that a full system backup is conducted within a reasonable time frame, ideally at the next scheduled backup period.

5.7 Event Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ISCP. It is the responsibility of each ISCP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the ISCP Coordinator.

Provide details about the types of information each ISCP team member is required to provide or collect for updating the ISCP with lessons learned. Types of documentation that should be generated and collected after a contingency activation include:

- *Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities);*
- *Functionality and data testing results;*
- *Lessons learned documentation; and*
- *After Action Report.*

Event documentation procedures should detail responsibilities for development, collection, approval, and maintenance.

5.8 Deactivation

Once all activities have been completed and documentation has been updated, the *{system owner}* will formally deactivate the ISCP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

SUGGESTED APPENDICES

ISCP appendices included should be based on system and plan requirements. The following appendices are recommended:

APPENDIX A PERSONNEL CONTACT LIST

Provide contact information for each person with a role or responsibility for activation or implementation of the ISCP, or coordination with the ISCP. For each person listed, at least one office and one non-office contact number is recommended. Note: Information may contain personally identifiable information and should be protected.

{System name} **ISCP Key Personnel**		
Key Personnel	**Contact Information**	
ISCP Director	Work	*Insert number*
Insert Name and Title	Home	*Insert number*
Insert Street Address	Cellular	*Insert number*
Insert City, State, and Zip Code	Email	*Insert email address*
ISCP Director – Alternate	Work	
	Home	
	Cellular	
	Email	
ISCP Coordinator	Work	
	Home	
	Cellular	
	Email	
ISCP Coordinator – Alternate	Work	
	Home	
	Cellular	
	Email	
ISCP Team – Team Lead	Work	
	Home	
	Cellular	
	Email	
ICSP Team – Team Members	Work	
	Home	
	Cellular	
	Email	

APPENDIX B VENDOR CONTACT LIST

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

APPENDIX C DETAILED RECOVERY PROCEDURES

This appendix includes the detailed recovery procedures for the system, which may include items such as:

- *Keystroke-level recovery steps;*
- *System installation instructions from tape, CD, or other media;*
- *Required configuration settings or changes;*
- *Recovery of data from tape and audit logs; and*
- *Other system recovery procedures, as appropriate.*

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

APPENDIX D ALTERNATE PROCESSING PROCEDURES

This section should identify any alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system. Examples of alternate processes include manual forms processing, input into workstations to store data until it can be uploaded and processed, or queuing of data input.

APPENDIX E SYSTEM VALIDATION TEST PLAN

This appendix includes system acceptance procedures that are performed after the system has been recovered and prior to putting the system into full operation and returned to users. The system validation test plan may include data testing and the regression or functionality testing conducted prior to implementation of a system upgrade or change.

An example of a system validation test plan:

Once the system has been recovered, the following steps will be performed to validate system data and functionality:

Procedure	Expected Results	Actual Results	Successful?	Performed by
At the Command Prompt, type in `sysname`	System Log-in Screen appears			
Log in as user `testuser,` using password `testpass`	Initial Screen with Main Menu shows			
From Menu - select `5-Generate Report`	Report Generation Screen shows			
- Select `Current Date Report` - Select `Weekly` - Select `To Screen`	Report is generated on screen with last successful transaction included			
- Select `Close`	Report Generation Screen Shows			
- Select `Return to Main Menu`	Initial Screen with Main Menu shows			
- Select `Log-Off`	Log-in Screen appears			

APPENDIX F DIAGRAMS (SYSTEM AND INPUT/OUTPUT)

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. Include any system architecture, input/output, or other technical or logical diagrams that may be useful in recovering the system. Diagrams may also identify information about interconnection with other systems.

APPENDIX G HARDWARE AND SOFTWARE INVENTORY

Provide the hardware and software inventory for the system. Inventory information should include type of server or hardware on which the system runs, processors and memory requirements, storage requirements, and any other pertinent details. The software inventory should identify the operating system (including service pack or version levels, and any other applications necessary to operate the system, such as database software).

APPENDIX H INTERCONNECTIONS TABLE

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. This appendix includes information on other systems that directly interconnect or exchange information with the system. Interconnection information should include the type of connection, information transferred, and contact person for that system.

If the system does not have any direct interconnections, then this appendix may be removed, or the following statement may be used:

{System name} does not directly interconnect with any other systems.

APPENDIX I TEST AND MAINTENANCE SCHEDULE

All ISCPs should be reviewed and tested at the organization defined frequency (e.g. yearly) or whenever there is a significant change to the system. Provide information and a schedule for the testing of the system. For low-impact systems, a yearly tabletop exercise is sufficient. The tabletop exercise should include all ISCP points of contact, and be conducted by an outside or impartial observer. A formal test plan is developed prior to the tabletop, and an exercise and questions are developed to include key sections of the ISCP, including a walk-through of the following:

- *Notification procedures;*
- *System recovery on an alternate platform from backup media;*
- *Internal and external connectivity; and*
- *Reconstitution procedures.*

Results of the test are documented in an After Action Report, and Lessons Learned are developed for updating information in the ISCP.

The following is a sample of a yearly test and maintenance schedule for a low-impact system:

Step	Date Due by	Responsible Party	Date Scheduled	Date Held
Identify tabletop facilitator.	April 1	ISCP Coordinator		
Develop tabletop test plan.	May 1	Tabletop Facilitator		
Invite participants.	May 10	Tabletop Facilitator		
Conduct tabletop test.	May 31	Facilitator, ISCP Coordinator, POCs		
Finalize after action report and lessons learned.	June 10	ISCP Coordinator		
Update ISCP based on lessons learned.	June 30	ISCP Coordinator		
Approve and distribute updated version of ISCP.	July 15	ISCP Director, ISCP Coordinator		

APPENDIX J ASSOCIATED PLANS AND PROCEDURES

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. ISCPs for other systems that either interconnect or support the system should be identified in this appendix. The most current version of the ISCP, location of ISCP, and primary point of contact (such as the ISCP Coordinator) should be noted.

APPENDIX K BUSINESS IMPACT ANALYSIS

The Business Impact Analysis results should be included in this appendix.

APPENDIX L DOCUMENT CHANGE PAGE

Modifications made to this plan since the last printing are as follows:

Record of Changes			
Page No.	**Change Comment**	**Date of Change**	**Signature**

A.2 Sample Template for Moderate-Impact Systems

[System Name]

Security Categorization: Moderate

[Organization Name]

Information System Contingency Plan (ISCP)

Version [#]

[Date]

Prepared by

[Organization Name]
[Street Address]
[City, State, and Zip Code]

TABLE OF CONTENTS

Plan Approval……A.2-3

1. Introduction ……A.2-4

1.1 Background……A.2-4
1.2 Scope……A.2-4
1.3 Assumptions……A.2-4

2. Concept of Operations ……A.2-5

2.1 System Description……A.2-5
2.2 Overview of Three Phases……A.2-5
2.3 Roles and Responsibilities……A.2-6

3. Activation and Notification……A.2-6

3.1 Activation Criteria and Procedure ……A.2-6
3.2 Notification……A.2-7
3.3 Outage Assessment……A.2-7

4. Recovery……A.2-7

4.1 Sequence of Recovery Activities ……A.2-7
4.2 Recovery Procedures ……A.2-8
4.3 Recovery Escalation Notices/Awareness……A.2-8

5. Reconstitution……A.2-8

5.1 Validation Data Testing……A.2-8
5.2 Validation Functionality Testing……A.2-8
5.3 Recovery Declaration……A.2-9
5.4 Notification (users)…… ……A.2-9
5.5 Cleanup ……A.2-9
5.6 Offsite Data Storage…… ……A.2-9
5.7 Data Backup……A.2-9
5.8 Event Documentation……A.2-9
5.9 Deactivation……A.2-10

APPENDICES

Plan Approval

Provide a statement in accordance with the agency's contingency planning policy to affirm that the ISCP is complete and has been tested sufficiently. The statement should also affirm that the designated authority is responsible for continued maintenance and testing of the ISCP. This statement should be approved and signed by the system designated authority. Space should be provided for the designated authority to sign, along with any other applicable approving signatures. Sample language is provided below:

As the designated authority for *{system name}*, I hereby certify that the information system contingency plan (ISCP) is complete, and that the information contained in this ISCP provides an accurate representation of the application, its hardware, software, and telecommunication components. I further certify that this document identifies the criticality of the system as it relates to the mission of the *{organization name}*, and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

I further attest that this ISCP for *{system name}* will be tested at least annually. This plan was last tested on *{insert exercise date}*; the test, training, and exercise (TT&E) material associated with this test can be found *{TT&E results appendix or location}*. This document will be modified as changes occur and will remain under version control, in accordance with *{organization name}*'s contingency planning policy.

_____ _____

{System Owner Name} Date
{System Owner Title}

1. Introduction

Information systems are vital to {*Organization's*} mission/business processes; therefore, it is critical that services provided by *{system name}* are able to operate effectively without excessive interruption. This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover {*system name}* quickly and effectively following a service disruption.

1.1 Background

This *{system name}* ISCP- establishes procedures to recover *{system name}* following a disruption. The following recovery plan objectives have been established:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - ***Activation and Notification phase*** to activate the plan and determine the extent of damage;
  - ***Recovery phase*** to restore *{system name}* operations; and
  - ***Reconstitution phase*** to ensure that *{system name}* is validated through testing and that normal operations are resumed.
- Identify the activities, resources, and procedures to carry out {*system name}* processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated *{organization name}* personnel and provide guidance for recovering *{system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other personnel responsible for *{organization name}* contingency planning strategies. Ensure coordination with external points of contact and vendors associated with *{system name}* and execution of this plan.

1.2 Scope

This ISCP has been developed for *{system name}*, which is classified as a moderate-impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – *Standards for Security Categorization of Federal Information and Information Systems.* Procedures in this ISCP are for moderate-impact systems and designed to recover {*system name}* within *{RTO hours}*. This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than *{RTO hours}*, or loss of data at the onsite facility or at the user-desktop levels.

1.3 Assumptions

The following assumptions were used when developing this ISCP:

- *{System name}* has been established as a moderate-impact system, in accordance with *FIPS 199.*
- Alternate processing sites and offsite storage are required and have been established for this system.
- Current backups of the system software and data are intact and available at the offsite storage facility in *{City, State}*.
- Alternate facilities have been established at *{City, State}* and are available if needed for relocation of *{system name}*.

- The *{system name}* is inoperable at the *{organization name}* and cannot be recovered within *{RTO 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.
- *Additional assumptions as appropriate.*

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

- **Overall recovery and continuity of mission/business operations.** The Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) address continuity of business operations.
- **Emergency evacuation of personnel.** The Occupant Emergency Plan (OEP) addresses employee evacuation.
- *Any additional constraints and associated plans should be added to this list.*

2. Concept of Operations

The Concept of Operations section provides details about *{system name}*, an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of {*Organization's*} personnel during a contingency activation.

2.1 System Description

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. Provide a general description of system architecture and functionality.

Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures.

2.2 Overview of Three Phases

This ISCP has been developed to recover and reconstitute the *{system name}* using a three-phased approach. This approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions.

The three system recovery phases are:

Activation and Notification Phase – Activation of the ISCP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss.

Once the ISCP is activated, system owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

Recovery Phase – The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.

Reconstitution – The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing.

Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

2.3 Roles and Responsibilities

The ISCP establishes several roles for *{system name}* recovery and reconstitution support. Persons or teams assigned ISCP roles have been trained to respond to a contingency event affecting *{system name}*.

Describe each team and role responsible for executing or supporting system recovery and reconstitution. Include responsibilities for each team/role, leadership roles, and coordination with other recovery and reconstitution teams, as applicable. At a minimum, a role should be established for a system owner or business unit point of contact, a recovery coordinator, and a technical recovery point of contact.

Leadership roles should include an ISCP Director, who has overall management responsibility for the plan, and an ISCP Coordinator, who is responsible to oversee recovery and reconstitution progress, initiate any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate.

3. Activation and Notification

The Activation and Notification Phase defines initial actions taken once a *{system name}* disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ISCP. At the completion of the Activation and Notification Phase, *{system name}* ISCP staff will be prepared to perform recovery measures to restore system functions.

3.1 Activation Criteria and Procedure

The *{system name}* ISCP may be activated if one or more of the following criteria are met:

1. The type of outage indicates *{system name}* will be down for more than *{RTO hours};*
2. The facility housing *{system name}* is damaged and may not be available within *{RTO hours}; and*
3. *Other criteria, as appropriate.*

The following persons or roles may activate the ISCP if one or more of these criteria are met:

Establish one or more roles that may activate the plan based on activation criteria. Authorized persons may include the system or business owner, or the operations point of contact (POC) for system support.

3.2 Notification

The first step upon activation of the *{system name}* ISCP is notification of appropriate business and system support personnel. Contact information for appropriate POCs is included in *{Contact List Appendix name}*.

For *{system name}*, the following method and procedure for notifications are used:

Describe established notification procedures. Notification procedures should include who makes the initial notifications, the sequence in which personnel are notified (e.g., system owner, technical POC, ISCP Coordinator, business unit or user unit POC, and recovery team POC), and the method of notification (e.g., email blast, call tree, automated notification system, etc.).

3.3 Outage Assessment

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. This outage assessment is conducted by *{name of recovery team}*. Assessment results are provided to the ISCP Coordinator to assist in the coordination of the recovery of *{system name}*.

Outline detailed procedures to include how to determine the cause of the outage; identification of potential for additional disruption or damage; assessment of affected physical area(s); and determination of the physical infrastructure status, IS equipment functionality, and inventory. Procedures should include notation of items that will need to be replaced and estimated time to restore service to normal operations.

4. Recovery

The Recovery Phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, *{system name}* will be functional and capable of performing the functions identified in Section 2.1 of this plan.

4.1 Sequence of Recovery Activities

The following activities occur during recovery of *{system name}:*

Modify the following list as appropriate for the selected system recovery strategy.

1. Identify recovery location (if not at original location);
2. Identify required resources to perform recovery procedures;
3. Retrieve backup and system installation media;

4. Recover hardware and operating system (if required); and
5. Recover system from backup and system installation media.

4.2 Recovery Procedures

The following procedures are provided for recovery of *{system name}* at the original or established alternate location. Recovery procedures are outlined per team and should be executed in the sequence presented to maintain an efficient recovery effort.

Provide general procedures for the recovery of the system from backup media. Specific keystroke-level procedures may be provided in an appendix. If specific procedures are provided in an appendix, a reference to that appendix should be included in this section. Teams or persons responsible for each procedure should be identified.

4.3 Recovery Escalation Notices/Awareness

Provide appropriate procedures for escalation notices during recovery efforts. Notifications during recovery include problem escalation to leadership and status awareness to system owners and users. Teams or persons responsible for each escalation/awareness procedure should be identified.

5. Reconstitution

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

5.1 Validation Data Testing

Validation data testing is the process of testing and validating data to ensure that data files or databases have been recovered completely at the permanent location. The following procedures will be used to determine that the data is complete and current to the last available backup:

Provide procedures for testing and validation of data to ensure that data is correct and up to date. This section may be combined with the Functionality Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a validation data test for a moderate-impact system would be to compare a database audit log to the recovered database to make sure all transactions were properly updated. Detailed data test procedures may be provided in Appendix E, System Validation Test Plan.

5.2 Validation Functionality Testing

Validation functionality testing is the process of verifying that recovered *{system name}* functionality has been tested, and the system is ready to return to normal operations.

Provide system functionality testing and/or validation procedures to ensure that the system is operating correctly. This section may be combined with the Data Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a functional test for a moderate-impact system may be logging into the system and running

a series of operations as a test or real user to ensure that all parts of the system are operating correctly. Detailed functionality test procedures may be provided in Appendix E, System Validation Test Plan.

5.3 Recovery Declaration

Upon successfully completing testing and validation, the *{designated authority}* will formally declare recovery efforts complete, and that *{system name}* is in normal operations. *{System name}* business and technical POCs will be notified of the declaration by the ISCP Coordinator.

5.4 Notifications (users)

Upon return to normal system operations, {*system name*} users will be notified by *{role}* using *predetermined notification procedures (e.g., email, broadcast message, phone calls, etc.).*

5.5 Cleanup

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manuals or other documentation to their original locations, and readying the system for a possible future contingency event.

Provide any specific cleanup procedures for the system, including preferred locations for manuals and documents and returning backup or installation media to its original location.

5.6 Offsite Data Storage

It is important that all backup and installation media used during recovery be returned to the offsite data storage location. The following procedures should be followed to return backup and installation media to its offsite data storage location.

Provide procedures for returning retrieved backup or installation media to its offsite data storage location. This may include proper logging and packaging of backup and installation media, preparing for transportation, and validating that media is securely stored at the offsite location.

5.7 Data Backup

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are:

Provide appropriate procedures for ensuring that a full system backup is conducted within a reasonable time frame, ideally at the next scheduled backup period. This backup should go offsite with the other media in Section 5.6.

5.8 Event Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ISCP. It is the responsibility of each ISCP team or person to document their actions during the recovery and reconstitution effort and to provide that documentation to the ISCP Coordinator.

Provide details about the types of information each ISCP team member is required to provide or collect for updating the ISCP with lessons learned. Types of documentation that should be generated and collected after a contingency activation include:

- *Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities);*
- *Functionality and data testing results;*
- *Lessons learned documentation; and*
- *After Action Report.*

Event documentation procedures should detail responsibilities for development, collection, approval, and maintenance.

5.9 Deactivation

Once all activities have been completed and documentation has been updated, the *{designated authority}* will formally deactivate the ISCP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

SUGGESTED APPENDICES

ISCP appendices included should be based on system and plan requirements. The following appendices are recommended:

APPENDIX A PERSONNEL CONTACT LIST

Provide contact information for each person with a role or responsibility for activation or implementation of the ISCP, or coordination with the ISCP. For each person listed, at least one office and one non-office contact number is recommended. Note: Information may contain personally identifiable information and should be protected.

{System name} **ISCP Key Personnel**		
Key Personnel	**Contact Information**	
ISCP Director	Work	*Insert number*
Insert Name and Title	Home	*Insert number*
Insert Street Address	Cellular	*Insert number*
Insert City, State, and Zip Code	Email	*Insert email address*
ISCP Director – Alternate	Work	
	Home	
	Cellular	
	Email	
ISCP Coordinator	Work	
	Home	
	Cellular	
	Email	
ISCP Coordinator – Alternate	Work	
	Home	
	Cellular	
	Email	
ISCP Team – Team Lead	Work	
	Home	
	Cellular	
	Email	
ISCP Team – Team Members	Work	
	Home	
	Cellular	
	Email	

APPENDIX B VENDOR CONTACT LIST

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

APPENDIX C DETAILED RECOVERY PROCEDURES

This appendix includes the detailed recovery procedures for the system, which may include items such as:

- *Keystroke-level recovery steps;*
- *System installation instructions from tape, CD, or other media;*
- *Required configuration settings or changes;*
- *Recovery of data from tape and audit logs; and*
- *Other system recovery procedures, as appropriate.*

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

APPENDIX D ALTERNATE PROCESSING PROCEDURES

This section should identify any alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system. Examples of alternate processes include manual forms processing, input into workstations to store data until it can be uploaded and processed, or queuing of data input.

APPENDIX E SYSTEM VALIDATION TEST PLAN

This appendix includes system acceptance procedures that are performed after the system has been recovered and prior to putting the system into full operation and returned to users. The system validation test plan may include the regression or functionality testing conducted prior to implementation of a system upgrade or change.

An example of a system validation test plan:

Once the system has been recovered, the following steps will be performed to validate system data and functionality:

Procedure	Expected Results	Actual Results	Successful?	Performed by
At the Command Prompt, type in `sysname`	System Log-in Screen appears			
Log-in as user `testuser,` using password `testpass`	Initial Screen with Main Menu shows			
From Menu - select `5-Generate Report`	Report Generation Screen shows			
- Select `Current Date Report` - Select `Weekly` - Select `To Screen`	Report is generated on screen with last successful transaction included			
- Select `Close`	Report Generation Screen Shows			
- Select `Return to`	Initial Screen with			

Procedure	Expected Results	Actual Results	Successful?	Performed by
`Main Menu`	Main Menu shows			
- Select `Log-Off`	Log-in Screen appears			

APPENDIX F ALTERNATE STORAGE, SITE AND TELECOMMUNICATIONS

This appendix provides information for alternate storage, alternate processing site, and alternate telecommunications for the system. Alternate Storage, Site, and Telecommunications information is required for moderate-impact systems, per NIST SP 800-53, Rev.3. Refer to NIST SP 800-53 Rev. 3, for details on control specifics. Information that should be provided for each area includes:

Alternate Storage:

- *City and state of alternate storage facility, and distance from primary facility;*
- *Whether the alternate storage facility is owned by the organization or is a third-party storage provider;*
- *Name and points of contact for the alternate storage facility;*
- *Delivery schedule and procedures for packaging media to go to alternate storage facility;*
- *Procedures for retrieving media from the alternate storage facility;*
- *Names and contact information for those persons authorized to retrieve media;*
- *Any potential accessibility problems to the alternate storage site in the event of a widespread disruption or disaster;*
- *Mitigation steps to access alternate storage site in the event of a widespread disruption or disaster;*
- *Types of data located at alternate storage site, including databases, application software, operating systems, and other critical information system software; and*
- *Other information as appropriate.*

Alternate Processing Site:

- *City and state of alternate processing site, and distance from primary facility;*
- *Whether the alternate processing site is owned by the organization or is a third-party site provider;*
- *Name and points of contact for the alternate processing site;*
- *Procedures for accessing and using the alternate processing site, and access security features of alternate processing site;*
- *Names and contact information for those persons authorized to go to alternate processing site;*
- *Type of alternate processing site, and equipment available at site;*
- *Any potential accessibility problems at the alternate processing site in the event of a widespread disruption or disaster;*
- *Mitigation steps to access alternate processing site in the event of a widespread disruption or disaster;*

- *SLAs or other agreements of use of alternate processing site, available office/support space, setup times, etc.; and*
- *Other information as appropriate.*

Alternate Telecommunications:

- *Name and contact information of alternate telecommunications vendors;*
- *Contracted capacity of alternate telecommunications;*
- *SLAs or other agreements for implementation of alternate telecommunications capacity;*
- *Names and contact information for those persons authorized to implement or use alternate telecommunications capacity; and*
- *Other information as appropriate.*

APPENDIX G DIAGRAMS (SYSTEM AND INPUT/OUTPUT)

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. Include any system architecture, input/output, or other technical or logical diagrams that may be useful in recovering the system. Diagrams may also identify information about interconnection with other systems.

APPENDIX H HARDWARE AND SOFTWARE INVENTORY

Provide the hardware and software inventory for the system. Inventory information should include type of server or hardware on which the system runs, processors and memory requirements, storage requirements, and any other pertinent details. The software inventory should identify the operating system (including service pack or version levels, and any other applications necessary to operate the system, such as database software).

APPENDIX I INTERCONNECTIONS TABLE

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. This appendix includes information on other systems that directly interconnect or exchange information with the system. Interconnection information should include the type of connection, information transferred, and contact person for that system.

If the system does not have any direct interconnections, then this appendix may be removed, or the following statement may be used:

{System name} does not directly interconnect with any other systems.

APPENDIX J TEST AND MAINTENANCE SCHEDULE

All ISCPs should be reviewed and tested at the organization defined frequency (e.g. yearly) or whenever there is a significant change to the system. Provide information and a schedule for the testing of the system. The functional test should include all ISCP points of contact and be facilitated by an outside or impartial observer. A formal test plan is developed prior to the functional test, and test procedures are developed to include key sections of the ISCP, including the following:

- *Notification procedures;*
- *System recovery on an alternate platform from backup media;*
- *Internal and external connectivity; and*
- *Reconstitution procedures.*

Results of the test are documented in an After Action Report, and Lessons Learned are developed for updating information in the ISCP.

Examples of functional tests that may be performed include:

- *Full notification and response of key personnel to recovery location;*
- *Recovery of a server or database from backup media;*
- *Setup and processing from a server at an alternate location.*

The following is a sample of a yearly test and maintenance schedule for a moderate-impact system:

Step	Date Due by	Responsible Party	Date Scheduled	Date Held
Identify functional test facilitator.	March 1	ISCP Coordinator		
Determine type and scope of functional test.	March 15	ISCP Coordinator, Test Facilitator		
Develop functional test plan.	April 1	Test Facilitator		
Invite participants.	May 10	Test Facilitator		
Conduct functional test.	May 31	Test Facilitator, ISCP Coordinator, POCs		
Finalize after action report and lessons learned.	June 10	ISCP Coordinator		
Update ISCP based on lessons learned.	June 30	ISCP Coordinator		
Approve and distribute updated version of ISCP.	July 15	ISCP Director, ISCP Coordinator		

APPENDIX K ASSOCIATED PLANS AND PROCEDURES

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. ISCPs for other systems that either interconnect or support the system should be identified in this appendix. The most current version of the ISCP, location of ISCP, and primary point of contact (such as the ISCP Coordinator) should be noted.

APPENDIX L BUSINESS IMPACT ANALYSIS

The Business Impact Analysis results should be included in this appendix.

APPENDIX M DOCUMENT CHANGE PAGE

Modifications made to this plan since the last printing are as follows:

Record of Changes			
Page No.	**Change Comment**	**Date of Change**	**Signature**

A.3 Sample Template for High-Impact Systems

[System Name]

Security Categorization: High

[Organization Name]

Information System Contingency Plan (ISCP)

Version [#]

[Date]

Prepared by

[Organization Name]
[Street Address]
[City, State, and Zip Code]

TABLE OF CONTENTS

Plan Approval……A.3-3

1. Introduction ……A.3-4

1.1 Background……A.3-4
1.2 Scope……A.3-4
1.3 Assumptions……A.3-4

2. Concept of Operations ……A.3-5

2.1 System Description……A.3-5
2.2 Overview of Three Phases……A.3-5
2.3 Roles and Responsibilities……A.3-6

3. Activation and Notification……A.3-6

3.1 Activation Criteria and Procedure ……A.3-6
3.2 Notification……A.3-6
3.3 Outage Assessment……A.3-7

4. Recovery……A.3-7

4.1 Sequence of Recovery Activities ……A.3-7
4.2 Recovery Procedures ……A.3-8
4.3 Recovery Escalation Notices/Awareness……A.3-8

5. Reconstitution……A.3-8

5.1 Concurrent Processing ……A.3-8
5.2 Validation Data Testing……A.3-8
5.3 Validation Functionality Testing……A.3-9
5.4 Recovery Declaration……A.3-9
5.5 Notification (users)…. ……A.3-9
5.6 Cleanup ……A.3-9
5.7 Offsite Data Storage……A.3-9
5.8 Data Backup……A.3-9
5.9 Event Documentation……A.3-10
5.10 Deactivation……A.3-10

APPENDICES

Plan Approval

Provide a statement in accordance with the agency's contingency planning policy to affirm that the ISCP is complete and has been tested sufficiently. The statement should also affirm that the designated authority is responsible for continued maintenance and testing of the ISCP. This statement should be approved and signed by the system designated authority. Space should be provided for the designated authority to sign, along with any other applicable approving signatures. A sample language is provided below:

As the designated authority for *{system name}*, I hereby certify that the information system contingency plan (ISCP) is complete, and that the information contained in this ISCP provides an accurate representation of the application, its hardware, software, and telecommunication components. I further certify that this document identifies the criticality of the system as it relates to the mission of the *{organization name}*, and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

I further attest that this ISCP for *{system name}* will be tested at least annually. This plan was last tested on *{insert exercise date}*; the test, training, and exercise (TT&E) material associated with this test can be found *{TT&E results appendix or location}*. This document will be modified as changes occur and will remain under version control, in accordance with *{organization name}*'s contingency planning policy.

_____ _____

{System Owner Name} Date
{System Owner Title}

1. Introduction

Information systems are vital to {*Organization's*} mission/business processes; therefore, it is critical that services provided by *{system name}* are able to operate effectively without excessive interruption. This Information System Contingency Plan (ISCP) establishes comprehensive procedures to recover {*system name}* quickly and effectively following a service disruption.

1.1 Background

This *{system name}* ISCP establishes procedures to recover *{system name}* following a disruption. The following recovery plan objectives have been established:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - ***Activation and Notification phase*** to activate the plan and determine the extent of damage;
  - ***Recovery phase*** to restore *{system name}* operations; and
  - ***Reconstitution phase*** to ensure that *{system name}* is validated through testing and that normal operations are resumed.
- Identify the activities, resources, and procedures to carry out {*system name}* processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated *{organization name}* personnel and provide guidance for recovering *{system name}* during prolonged periods of interruption to normal operations.
- Ensure coordination with other personnel responsible for *{organization name}* contingency planning strategies. Ensure coordination with external points of contact and vendors associated with *{system name}* and execution of this plan.

1.2 Scope

This ISCP has been developed for *{system name}*, which is classified as a high-impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – *Standards for Security Categorization of Federal Information and Information Systems.* Procedures in this ISCP are for high-impact systems and designed to recover {*system name}* within *{RTO hours}*. This plan does not address replacement or purchase of new equipment, short-term disruptions lasting less than *{RTO hours}*, or loss of data at the onsite facility or at the user-desktop levels.

1.3 Assumptions

The following assumptions were used when developing this ISCP:

- *{System name}* has been established as a high-impact system, in accordance with *FIPS 199.*
- Alternate processing sites and offsite storage are required and have been established for this system.
- Current backups of the system software and data are intact and available at the offsite storage facility in *{City, State}*.
- Alternate facilities have been established at *{City, State}* and are available if needed for relocation of *{system name}*.

- The *{system name}* is inoperable at the *{organization name}* and cannot be recovered within *{RTO 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.
- *Additional assumptions as appropriate.*

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

- **Overall recovery and continuity of mission/business operations.** The Business Continuity Plan (BCP) and Continuity of Operations Plan (COOP) address continuity of business operations.
- **Emergency evacuation of personnel.** The Occupant Emergency Plan (OEP) addresses employee evacuation.
- *Any additional constraints and associated plans should be added to this list.*

2. Concept of Operations

The Concept of Operations section provides details about *{system name}*, an overview of the three phases of the ISCP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of {*Organization's*} personnel during a contingency activation.

2.1 System Description

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. Provide a general description of system architecture and functionality

Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures.

2.2 Overview of Three Phases

This ISCP has been developed to recover the *{system name}* using a three-phased approach. This approach ensures that system recovery efforts are performed in a methodical sequence to maximize the effectiveness of the recovery effort and minimize system outage time due to errors and omissions.

The three system recovery phases are:

Activation and Notification Phase – Activation of the ISCP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in long-term loss.

Once the ISCP is activated, system owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

Recovery Phase – The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.

Reconstitution – The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing.

Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

2.3 Roles and Responsibilities

The ISCP establishes several roles for *{system name}* recovery and reconstitution support. Persons or teams assigned ISCP roles have been trained to respond to a contingency event affecting *{system name}*.

Describe each team and role responsible for executing or supporting system recovery and reconstitution. Include responsibilities for each team/role, leadership roles, and coordination with other recovery and reconstitution teams, as applicable. At a minimum, a role should be established for a system owner or business unit point of contact, a recovery coordinator, and a technical recovery point of contact.

Leadership roles should include an ISCP Director, who has overall management responsibility for the plan, and an ISCP Coordinator, who is responsible to oversee recovery and reconstitution progress, initiate any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate.

3. Activation and Notification

The Activation and Notification Phase defines initial actions taken once a *{system name}* disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the ISCP. At the completion of the Activation and Notification Phase, *{system name}* ISCP staff will be prepared to perform recovery measures.

3.1 Activation Criteria and Procedure

The *{system name}* ISCP may be activated if one or more of the following criteria are met:

1. The type of outage indicates *{system name}* will be down for more than *{RTO hours};*
2. The facility housing *{system name}* is damaged and may not be available within *{RTO hours}; and*
3. *Other criteria, as appropriate.*

The following persons or roles may activate the ISCP if one or more of these criteria are met:

Establish one or more roles that may activate the plan based on activation criteria. Authorized persons may include the system or business owner, or the operations point of contact (POC) for system support.

3.2 Notification

The first step upon activation of the *{system name}* ISCP is notification of appropriate business and system support personnel. Contact information for appropriate POCs is included in *{Contact List Appendix name}*.

For *{system name}*, the following method and procedure for notifications are used:

Describe established notification procedures. Notification procedures should include who makes the initial notifications, the sequence in which personnel are notified (e.g., system owner, technical POC, ISCP Coordinator, business unit or user unit POC, and recovery team POC), and the method of notification (e.g., email blast, call tree, automated notification system, etc.).

3.3 Outage Assessment

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. This outage assessment is conducted by *{name of recovery team}*. Assessment results are provided to the ISCP Coordinator to assist in the coordination of the recovery of *{system name}*.

Outline detailed procedures to include how to determine the cause of the outage; identification of potential for additional disruption or damage; assessment of affected physical area(s); and determination of the physical infrastructure status, IS equipment functionality, and inventory. Procedures should include notation of items that will need to be replaced and estimated time to restore service to normal operations.

4. Recovery

The Recovery Phase provides formal recovery operations that begin after the ISCP has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, *{system name}* will be functional and capable of performing the functions identified in Section 2.1 of this plan.

4.1 Sequence of Recovery Activities

The following activities occur during recovery of *{system name}:*

Modify the following list as appropriate for the selected system recovery strategy:

1. Identify recovery location (if not at original location);
2. Identify required resources to perform recovery procedures;
3. Retrieve backup and system installation media;
4. Recover hardware and operating system (if required); and
5. Recover system from backup and system installation media.

4.2 Recovery Procedures

The following procedures are provided for recovery of *{system name}* at the original or established alternate location. Recovery procedures are outlined per team and should be executed in the sequence presented to maintain an efficient recovery effort.

Provide general procedures for the recovery of the system from backup media. Specific keystroke-level procedures may be provided in an appendix. If specific procedures are provided in an appendix, a reference to that appendix should be included in this section. Teams or persons responsible for each procedure should be identified.

4.3 Recovery Escalation Notices/Awareness

Provide appropriate procedures for escalation notices during recovery efforts. Notifications during recovery include problem escalation to leadership and status awareness to system owners and users. Teams or persons responsible for each escalation/awareness procedure should be identified.

5. Reconstitution

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

5.1 Concurrent Processing

High-impact systems are not required to have concurrent processing as part of the validation effort. If concurrent processing does occur for the system prior to making it operational, procedures should be inserted here. Procedures should include length of time for concurrent processing, processing information on both concurrent systems, and validating information on the new permanent system.

For high-impact systems without concurrent processing, this section may either be removed or the following may be used:

In concurrent processing, a system operates at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly. *{System name}* does not have concurrent processing as part of validation. Once the system has been tested and validated, it will be placed into normal operations.

5.2 Validation Data Testing

Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely. The following procedures will be used to determine that the recovered data is complete and current to the last available backup:

Provide procedures for testing or validation of recovered data to ensure that data is correct and up to date. This section may be combined with the Functionality Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified.

An example of a validation data test for a high-impact system would be to log into the system database and check the audit logs to determine that all transactions and updates are current. Detailed data test procedures may be provided in Appendix E, System Validation Test Plan.

5.3 Validation Functionality Testing

Validation functionality testing is the process of verifying that *{system name}* functionality has been tested, and the system is ready to return to normal operations.

Provide system functionality testing and validation procedures to ensure that the system is operating correctly. This section may be combined with the Data Testing section if procedures test both the functionality and data validity. Teams or persons responsible for each procedure should be identified. An example of a functional test for a high-impact system may be logging into the system and running a series of operations as a test or real user to ensure that all parts of the system are operating correctly. Detailed functionality test procedures may be provided in Appendix E, System Validation Test Plan.

5.4 Recovery Declaration

Upon successfully completing testing and validation, the *{designated authority}* will formally declare recovery efforts complete, and that *{system name}* is in normal operations. *{System name}* business and technical POCs will be notified of the declaration by the ISCP Coordinator.

5.5 Notifications (users)

Upon return to normal system operations, {*system name*} users will be notified by *{role}* using *predetermined notification procedures (e.g., email, broadcast message, phone calls, etc.).*

5.6 Cleanup

Cleanup is the process of cleaning up or dismantling any temporary recovery locations, restocking supplies used, returning manuals or other documentation to their original locations, and readying the system for a possible future contingency event.

Provide any specific cleanup procedures for the system, including preferred locations for manuals and documents and returning backup or installation media to its original location.

5.7 Offsite Data Storage

It is important that all backup and installation media used during recovery be returned to the offsite data storage location. The following procedures should be followed to return backup and installation media to its offsite data storage location.

Provide procedures for returning retrieved backup or installation media to its offsite data storage location. This may include proper logging and packaging of backup and installation media, preparing for transportation, and validating that media is securely stored at the offsite location.

5.8 Data Backup

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are:

Provide appropriate procedures for ensuring that a full system backup is conducted within a reasonable time frame, ideally at the next scheduled backup period. This backup should go offsite with the other media in Section 5.7.

5.9 Event Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this ISCP. It is the responsibility of each ISCP team or person to document their actions during the recovery and reconstitution effort, and to provide that documentation to the ISCP Coordinator.

Provide details about the types of information each ISCP team member is required to provide or collect for updating the ISCP with lessons learned. Types of documentation that should be generated and collected after a contingency activation include:

- *Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities);*
- *Functionality and data testing results;*
- *Lessons learned documentation; and*
- *After Action Report.*

Event documentation procedures should detail responsibilities for development, collection, approval, and maintenance.

5.10 Deactivation

Once all activities have been completed and documentation has been updated, the *{designated authority}* will formally deactivate the ISCP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.

SUGGESTED APPENDICES

ISCP appendices included should be based on system and plan requirements. The following appendices are recommended:

APPENDIX A PERSONNEL CONTACT LIST

Provide contact information for each person with a role or responsibility for activation or implementation of the ISCP, or coordination with the ISCP. For each person listed, at least one office and one non-office contact number is recommended. Note: Information may contain personally identifiable information and should be protected.

{System name} **ISCP Key Personnel**		
Key Personnel	**Contact Information**	
ISCP Director	Work	*Insert number*
Insert Name and Title	Home	*Insert number*
Insert Street Address	Cellular	*Insert number*
Insert City, State, and Zip Code	Email	*Insert email address*
ISCP Director – Alternate	Work	
	Home	
	Cellular	
	Email	
ISCP Coordinator	Work	
	Home	
	Cellular	
	Email	
ISCP Coordinator – Alternate	Work	
	Home	
	Cellular	
	Email	
ISCP Team – Team Lead	Work	
	Home	
	Cellular	
	Email	
ISCP Team – Team Members	Work	
	Home	
	Cellular	
	Email	

APPENDIX B VENDOR CONTACT LIST

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

APPENDIX C DETAILED RECOVERY PROCEDURES

This appendix includes the detailed recovery procedures for the system, which may include items such as:

- *Keystroke-level recovery steps;*
- *System installation instructions from tape, CD, or other media;*
- *Required configuration settings or changes;*
- *Recovery of data from tape and audit logs; and*
- *Other system recovery procedures, as appropriate.*

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

APPENDIX D ALTERNATE PROCESSING PROCEDURES

This section should identify any alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system. Examples of alternate processes include manual forms processing, input into workstations to store data until it can be uploaded and processed, or queuing of data input.

APPENDIX E SYSTEM VALIDATION TEST PLAN

This appendix includes system acceptance procedures that are performed after the system has been recovered and prior to putting the system into full operation and returned to users. The system validation test plan may include the regression or functionality testing conducted prior to implementation of a system upgrade or change.

An example of a system validation test plan:

Once the system has been recovered, the following steps will be performed to validate system data and functionality:

Procedure	Expected Results	Actual Results	Successful?	Performed by
At the Command Prompt, type in `sysname`	System Log-in Screen appears			
Log in as user `testuser,` using password `testpass`	Initial Screen with Main Menu shows			
From Menu - select `5-Generate Report`	Report Generation Screen shows			
- Select `Current Date Report` - Select `Weekly` - Select `To Screen`	Report is generated on screen with last successful transaction included			
- Select `Close`	Report Generation Screen Shows			
- Select `Return to Main Menu`	Initial Screen with Main Menu shows			
- Select `Log-Off`	Log-in Screen appears			

APPENDIX F ALTERNATE STORAGE, SITE, AND TELECOMMUNICATIONS

This appendix provides information for alternate storage, alternate processing site, and alternate telecommunications for the system. Alternate storage, site, and telecommunications information is required for high-impact systems, per NIST SP 800-53 Rev. 3. Refer to NIST SP 800-53 Rev. 3, for details on control specifics. Information that should be provided for each area includes:

Alternate Storage:

- *City and state of alternate storage facility, and distance from primary facility;*
- *Whether the alternate storage facility is owned by the organization or is a third-party storage provider;*
- *Name and points of contact for the alternate storage facility;*
- *Delivery schedule and procedures for packaging media to go to alternate storage facility;*
- *Procedures for retrieving media from the alternate storage facility;*
- *Names and contact information for those persons authorized to retrieve media;*
- *Alternate storage configuration features that facilitate recovery operations (such as keyed or card reader access by authorized retrieval personnel);*
- *Any potential accessibility problems to the alternate storage site in the event of a widespread disruption or disaster;*
- *Mitigation steps to access alternate storage site in the event of a widespread disruption or disaster;*
- *Types of data located at alternate storage site, including databases, application software, operating systems, and other critical information system software; and*
- *Other information as appropriate.*

Alternate Processing Site:

- *City and state of alternate processing site, and distance from primary facility;*
- *Whether the alternate processing site is owned by the organization or is a third-party site provider;*
- *Name and points of contact for the alternate processing site;*
- *Procedures for accessing and using the alternate processing site, and access security features of alternate processing site;*
- *Names and contact information for those persons authorized to go to alternate processing site;*
- *Type of alternate processing site, and equipment available at site;*
- *Alternate processing site configuration information (such as available power, floor space, office space, telecommunications availability, etc.);*
- *Any potential accessibility problems to the alternate processing site in the event of a widespread disruption or disaster;*
- *Mitigation steps to access alternate processing site in the event of a widespread disruption or disaster;*

- *SLAs or other agreements of use of alternate processing site, available office/support space, setup times, etc.; and*
- *Other information as appropriate.*

Alternate Telecommunications:

- *Name and contact information of alternate telecommunications vendors;*
- *Geographic locations of alternate telecommunications vendors facilities (such as central offices, switch centers, etc.);*
- *Contracted capacity of alternate telecommunications;*
- *SLAs or other agreements for implementation of alternate telecommunications capacity;*
- *Information on alternate telecommunications vendor contingency plans;*
- *Names and contact information for those persons authorized to implement or use alternate telecommunications capacity; and*
- *Other information as appropriate.*

APPENDIX G DIAGRAMS (SYSTEM AND INPUT/OUTPUT)

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. Include any system architecture, input/output, or other technical or logical diagrams that may be useful in recovering the system. Diagrams may also identify information about interconnection with other systems.

APPENDIX H HARDWARE AND SOFTWARE INVENTORY

Provide the hardware and software inventory for the system. Inventory information should include type of server or hardware on which the system runs, processors and memory requirements, storage requirements, and any other pertinent details. The software inventory should identify the operating system (including service pack or version levels, and any other applications necessary to operate the system, such as database software).

APPENDIX I INTERCONNECTIONS TABLE

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. This appendix includes information on other systems that directly interconnect or exchange information with the system. Interconnection information should include the type of connection, information transferred, and contact person for that system.

If the system does not have any direct interconnections, then this appendix may be removed, or the following statement may be used:

{System name} does not directly interconnect with any other systems.

APPENDIX J TEST AND MAINTENANCE SCHEDULE

All ISCPs should be reviewed and tested at the organization defined frequency (e.g. yearly) or whenever there is a significant change to the system. Provide information and a schedule for the testing of the

system. The full functional test should include all ISCP points of contact and be facilitated by an outside or impartial observer. A formal test plan is developed prior to the functional test, and test procedures are developed to include key sections of the ISCP, including the following:

- *Notification procedures;*
- *System recovery on an alternate platform from backup media;*
- *Internal and external connectivity; and*
- *Reconstitution procedures.*

Results of the test are documented in an After Action Report, and Lessons Learned are developed for updating information in the ISCP.

NOTE: Full functional tests of systems normally are failover tests to the alternate locations, and may be very disruptive to system operations if not planned well. Other systems located in the same physical location may be affected by or included in the full functional test. It is highly recommended that several functional tests be conducted and evaluated prior to conducting a full functional (failover) test.

Examples of functional tests that may be performed prior to a full functional test include:

- *Full notification and response of key personnel to recovery location;*
- *Recovery of a server or database from backup media; and*
- *Setup and processing from a server at an alternate location.*

The following is a sample of a yearly test and maintenance schedule for a high-impact system:

Step	Date Due by	Responsible Party	Date Scheduled	Date Held
Identify failover test facilitator.	March 1	ISCP Coordinator		
Determine scope of failover test (include other systems?).	March 15	ISCP Coordinator, Test Facilitator		
Develop failover test plan.	April 1	Test Facilitator		
Invite participants.	July 10	Test Facilitator		
Conduct functional test.	July 31	Test Facilitator, ISCP Coordinator, POCs		
Finalize after action report and lessons learned.	August 15	ISCP Coordinator		
Update ISCP based on lessons learned.	September 15	ISCP Coordinator		
Approve and distribute updated version of ISCP.	September 30	ISCP Director, ISCP Coordinator		

APPENDIX K ASSOCIATED PLANS AND PROCEDURES

NOTE: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan. ISCPs for other systems that either interconnect or support the system should be identified in this appendix. The most current version of the ISCP, location of ISCP, and primary point of contact (such as the ISCP Coordinator) should be noted.

APPENDIX L BUSINESS IMPACT ANALYSIS

The Business Impact Analysis results should be included in this appendix.

APPENDIX M DOCUMENT CHANGE PAGE

Modifications made to this plan since the last printing are as follows:

Record of Changes			
Page No.	**Change Comment**	**Date of Change**	**Signature**

Appendix B—Sample Business Impact Analysis (BIA) and BIA Template

This sample template is designed to assist the user in performing a Business Impact Analysis (BIA) on an information system. The template is meant only as a basic guide and may not apply equally to all systems. The user may modify this template or the general BIA approach as required to best accommodate the specific system. In this template, words in ***italics*** *are for guidance only and should be deleted from the final version. Regular (non-italic) text is intended to remain.*

1. Overview

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the *{system name}{system acronym}*. It was prepared on {*insert BIA completion date*}.

1.1 Purpose

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system were unavailable.

The BIA is composed of the following three steps:

1. **Determine mission/business processes and recovery criticality.** Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

This document is used to build the *{system name}* Information System Contingency Plan (ISCP) and is included as a key component of the ISCP. It also may be used to support the development of other contingency plans associated with the system, including, but not limited to, the Disaster Recovery Plan (DRP) or Cyber Incident Response Plan.

2. System Description

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including inputs and outputs and telecommunications connections.

Note: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan.

3. BIA Data Collection

Data collection can be accomplished through individual/group interviews, workshops, email, questionnaires, or any combination of these.

3.1 Determine Process and System Criticality

Step one of the BIA process - Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), identify the specific mission/business processes that depend on or support the information system.

Mission/Business Process	Description
Pay vendor invoice	*Process of obligating funds, issuing check or electronic payment and acknowledging receipt*

If criticality of mission/business processes has not been determined outside of the BIA, the following subsections will help to determine criticality of mission/business processes that depend on or support the information system.

3.1.1 Identify Outage Impacts and Estimated Downtime

This section identifies and characterizes the types of impact categories that a system disruption is likely to create in addition to those identified by the FIPS 199 impact level, as well as the estimated downtime that the organization can tolerate for a given process. Impact categories should be created and values assigned to these categories in order to measure the level or type of impact a disruption may cause. An example of cost as an impact category is provided. Organizations could consider other categories like harm to individuals and ability to perform mission. The template should be revised to reflect what is appropriate for the organization.

Outage Impacts

Impact categories and values should be created in order to characterize levels of severity to the organization that would result for that particular impact category if the mission/business process could not be performed. These impact categories and values are samples and should be revised to reflect what is appropriate for the organization.

The following impact categories represent important areas for consideration in the event of a disruption or impact.

Impact category: {*insert category name*}

Impact values for assessing category impact:

- Severe = {*insert value*}
- Moderate = {*insert value*}

Example impact category = Cost

- ***Severe*** *- temp staffing, overtime, fees are greater than $1 million*
- ***Moderate*** *– fines, penalties, liabilities potential $550k*
- ***Minimal*** *– new contracts, supplies $75k*

- Minimal = {*insert value*}

The table below summarizes the impact on each mission/business process if *{system name}* were unavailable, based on the following criteria:

Mission/Business Process	Impact Category				
	{insert}	***{insert}***	***{insert}***	***{insert}***	**Impact**
Pay vendor invoice					

Estimated Downtime

Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the downtime factors for consideration as a result of a disruptive event.

- **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.

- **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

- **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

The table below identifies the MTD, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on *{system name}*. *Values for MTDs and RPOs are expected to be specific time frames, identified in hourly increments (i.e., 8 hours, 36 hours, 97 hours, etc.).*

Mission/Business Process	MTD	RTO	RPO
Pay vendor invoice	*72 hours*	*48 hours*	*12 hours (last backup)*

Include a description of the drivers for the MTD, RTO, and RPOs listed in the table above (e.g., mandate, workload, performance measure, etc.).

Include a description of any alternate means (secondary processing or manual work-around) for recovering the mission/business process(es) that rely on the system. If none exist, so state.

3.2 Identify Resource Requirements

The following table identifies the resources that compose *{system name}* including hardware, software, and other resources such as data files.

System Resource/Component	Platform/OS/Version (as applicable)	Description
Web Server 1	***Optiplex GX280***	***Web Site Host***

It is assumed that all identified resources support the mission/business processes identified in Section 3.1 unless otherwise stated.

Note: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan.

3.3 Identify Recovery Priorities for System Resources

The table below lists the order of recovery for *{system name}* resources. The table also identifies the expected time for recovering the resource following a "worst case" (complete rebuild/repair or replacement) disruption.

- **Recovery Time Objective (RTO) -** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

Priority	System Resource/Component	Recovery Time Objective
Web Server 1	*Optiplex GX280*	*24 hours to rebuild or replace*

A system resource can be software, data files, servers, or other hardware and should be identified individually or as a logical group.

Identify any alternate strategies in place to meet expected RTOs. This includes backup or spare equipment and vendor support contracts.

Appendix C—Frequently Asked Questions

1. What is Information System Contingency Planning?

Information system contingency planning refers to the dynamic development of a coordinated recovery strategy for information systems, operations, and data after a disruption. The planning process requires seven steps: develop contingency planning policy statement; conduct the business impact analysis (BIA); identify preventive controls; develop recovery strategies; develop the Information System Contingency Plan (ISCP); test and exercise the plan and train personnel; and maintain the plan.

2. What are the differences among a Continuity of Operations Plan (COOP), a Business Continuity Plan (BCP), a Critical Infrastructure Protection (CIP) Plan, a Disaster Recovery Plan (DRP), an Information System Contingency Plan (ISCP), a Cyber Incident Response Plan, and an Occupant Emergency Plan (OEP)?

Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope; however, because of the lack of standard definitions for these types of plans, in some cases, the scope of actual plans developed by organizations may vary from the following basic descriptions.

A **COOP** is required by Homeland Security Presidential Directive (HSPD) - 20/National Security Presidential Directive (NSPD) - 51, *National Continuity Policy* and Federal Continuity Directive (FCD) - 1, *Federal Executive Branch National Continuity Program and Requirements* for sustaining an organization's (usually a headquarters element) *mission essential functions* (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. A **BCP** addresses sustaining mission/business processes and the information systems that support those mission/business processes during and after a significant disruption. BCPs are often developed at the organization's field level or for mission/business processes that are not prioritized as mission essential. A **CIP** plan is a set of policies and procedures that serve to protect and recover those components of the national infrastructure that are deemed so vital that their loss would have a debilitating effect of the safety, security, economy, and/or health of the United States. A **DRP** refers to an information system-focused plan designed to restore operability of one or more information systems at an alternate site after a major disruption usually causing physical damage to the original data center. An **ISCP** provides recovery and resumption procedures for a single information system resulting from disruptions that do not necessarily require relocation to an alternate site. A **Cyber Incident Response Plan** establishes procedures to enable security personnel to identify, mitigate, and recover from cyber attacks against an organization's information system(s). An **OEP** provides directions for facility occupants to follow in the event of an emergency situation that threatens the health and safety of personnel, the environment, or property.

Careful coordination must be maintained between plan developers to ensure that their respective policies and procedures complement one another. Any changes in one plan, system, or process must be communicated to plan developers of associated systems and functions.

3. What is the difference between mission/business processes supported by an information system and a COOP MEF?

Information systems are designed and developed to support mission/business processes (or functions). When conducting a BIA, the mission/business processes are identified and prioritized in terms of

criticality. COOP MEFs are a set of prioritized mission/business processes that support the organization's mission and must be sustained within 12 hours and for up to 30 days following a disruption. Federal Continuity Directive-2, *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, provides detailed guidance on how to determine if a mission/business process meets the requirements of a MEF. Because COOP MEFs may also be supported by information systems, ISCPs must be developed for those systems as well.

4. What is the connection between the risk management framework and information system contingency planning?

The risk management framework (RMF) encompasses a broad range of activities to identify, control, and mitigate risks to an information system during the system development life cycle. One of the activities is the development of an ISCP. Implementing the risk management framework can prevent or reduce the *likelihood* of natural, human, and environmental threats and limit the *consequences* of risks in the event of a system disruption.

5. How do risk management and information system contingency planning fit into a resilience program?

The goal of a resilient organization is to continue functions at all times during any type of disruption. Resilient organizations continually work to adapt to changes and risks that can affect their ability to sustain operations. Risk management, contingency, and continuity planning are individual security and emergency management activities that can be implemented in a holistic manner across an organization as components of a resiliency program.

6. Into what phase of the system development life cycle (SDLC) should contingency planning and related security controls be incorporated?

Although contingency planning is associated with activities occurring in the Operation/Maintenance phase, contingency measures should be identified and integrated into ALL phases of the SDLC. Incorporating contingency planning into the SDLC reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is implemented.

7. What is the first step I need to take before writing an ISCP?

The first step in the contingency planning process is to develop a contingency planning policy statement supported by senior leadership (typically the Chief Information Officer). This policy should define the agency's overall contingency objectives and should establish the organizational framework and responsibilities for information system contingency planning. The policy statement should also address roles and responsibilities. The policy should be supported with procedures covering training requirements, frequency of backups, offsite storage shipments, plan exercises, testing, and maintenance.

8. The BIA guidance in this guide is a different process than the one required by Federal Continuity Directive-2, *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process.* Which is the correct process for my organization to use?

The BIA process recommended in this guide is specifically designed to utilize the identify impact categories and values, determine recovery time objectives (RTOs), and prioritize system components for information systems. This BIA format uses FIPS 199 impact levels as a baseline to help determine the impact categories, values, and priorities and allows the organization to further customize the BIA to identify impact categories unique to the organization's mission. The BIA in this guide is a *recommended format for information systems*; organizations may adapt the format to their needs or use a different process.

The BIA process *required* by FCD-2 is designed to identify the threats, vulnerabilities, impacts, and mitigation strategies for the organization's *primary mission essential functions* (PMEFs). BIAs for information systems that support PMEFs should use the FCD-2 BIA as input to the system-focused BIA.

9. How can I determine which contingency solutions I should implement to ensure availability of my information systems?

The ISCP Coordinator can use the BIA results to determine contingency planning requirements and priorities. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's COOP, BCP, and DRP. The BIA should be performed during the Initiation phase of the SDLC. As the system design evolves and components change, the BIA may need to be conducted again during the Development/Acquisition phase of the SDLC.

The BIA, which is the second step in the information system contingency planning process, is central to determining what recovery strategies should be implemented to ensure availability. The BIA enables the ISCP Coordinator to fully characterize the system components, supported mission/business processes, and interdependencies. The BIA should be developed with input from all associated system owners, end users, and interconnected system partners. Possible mission/business impacts attributed to the unavailability of the information system can then be determined, leading to the RTO, mean tolerable downtime (MTD), and sequencing recovery of information system components. Thus, recovery prioritizations will form the basis for developing appropriate contingency solutions.

10. What type of alternate site should I choose as a recovery strategy?

The type of alternate site should be determined through the BIA with consideration of the FIPS 199 impact level. The alternate site choice must be cost-effective and match the availability needs of the organization's information systems. Thus, if a system requires near 100 percent availability, then a mirrored or hot site might be the right choice. However, if the system can allow for several days of downtime, then a cold site might be a better option.

11. When an event occurs, who should be notified?

Notification procedures must be outlined in the ISCP. The ISCP Coordinator should determine who should be notified if a disruption occurs to the information system and in what sequence they should be contacted. Parties notified typically include the system owners, users, and interconnected information system points of contact. External entities that might be interconnected to the information system should also be included in the notification procedures. Design of a call tree will assist the sequence and responsibilities of executing notifications to appropriate contacts.

12. How often should my ISCP be tested?

Testing helps evaluate the viability of plan procedures, determine the ability of recovery staff to implement the plan, and identify deficiencies in the plan. Testing should occur based on organization requirements and when significant changes are made to the information system, supported mission/business process(s), or the ISCP. Each element of the ISCP should be tested first individually and then as a whole to confirm the accuracy of recovery procedures and the overall effectiveness. Test and exercise schedules should be stated in the ISCP policy statement.

13. How often should my ISCP be updated?

An up-to-date ISCP is essential for successful ISCP operations. As a general rule, the ISCP should be reviewed for accuracy and completeness at least annually, as well as upon significant changes to any element of the ISCP, system, mission/business processes supported by the system, or resources used for recovery procedures. Deficiencies identified through testing (see Question 12) should be addressed during plan maintenance. Elements of the plan subject to frequent changes, such as contact lists, should be reviewed and updated more frequently. Maintenance schedules should be stated in the ISCP policy statement.

14. With what other activities should the ISCP and the recovery solutions be coordinated?

In addition to integrating contingency planning into the SDLC, information system contingency planning should be coordinated with network security policies. System security controls can help to protect against malicious code or attacks that could compromise system availability and are closely coordinated with the incident response procedures. The ISCP should be closely coordinated with all other emergency preparedness plans related to the information system or interconnected systems and mission/business processes.

Appendix D—Personnel Considerations in Continuity and Contingency Planning

Information system contingency plans are rarely developed or executed on their own. When an incident occurs that impacts information system operations, it often impacts the organization's personnel. Proper considerations for the safety, security, and well-being of personnel should be planned for in anticipation of a disruptive event. Evacuation procedures and regaining access to the facility should be coordinated and jointly exercised with local response organizations and federal authorities. Organizations should also have in place methods and standards for interfacing with media inquiries and for sending out responsive messages to personnel. Planning for these factors typically falls within the scope of an occupant emergency plan (OEP), business continuity plan (BCP), or crisis communications plan, which are all plans coordinated with the ISCP. In light of heightened awareness of these issues due to the terrorist attacks in 2001, the aftermath of Hurricane Katrina in 2005, the threat of pandemic influenza, and general increased security throughout our society, "personnel considerations" warrant further discussion in all related planning areas.

Personnel Safety and Evacuation

Personnel safety and evacuation during and after a disruption are typically addressed in an OEP. Personnel should be aware of their physical security and exit procedures and should practice these procedures during regular fire drill exercises. OEPs and ISCPs may include instructions for securing office spaces, personal workstations, and laptop computers to prevent access to information and to reduce the likelihood of vandalism or theft. Plans may also include reminders to collect identification, car keys, and other important belongings if the nature of the incident and time allows. In addition, procedures may need to address how to regain access. Instructions for the most appropriate ways to exit the facility are based on specific site requirements and local fire code regulations. A "floor warden" methodology may be incorporated into the plan and instituted as a normal practice. This methodology involves designating and training one or two specific people from each floor to be responsible for the evacuation of all personnel. This responsibility usually rotates so that the same people are not responsible for overseeing evacuations all year.

The OEP should also include procedures and multiple contact methods for collecting a personnel head count after the disaster. It is important for senior management to know who was in the building prior to the event and who has been accounted for (both onsite and offsite personnel) so that civil authorities (fire, police, and rescue) and families can be properly informed of the situation. Procedures should be developed to instruct personnel to meet and be accounted for at a specific preplanned site, away from the building. Personnel should be provided alternate procedures to contact the organization and provide information on their whereabouts in the event the preplanned location is not safe. A centralized reporting methodology to one person or to a team will reduce possible confusion and conflicting information. During the September 11, 2001 terrorist attacks, many organizations were successful using television and radio announcements or Internet Web sites as a means to communicate accounting procedures to staff. Contact methods may be developed to be sent out and/or received by telephone, answering service, electronic mail (email), instant messenger (IM), Web site, meeting at a physical location, or by a combination of methods. As the use of social networking within the federal government increases, approved and verifiable means for crisis communications may be another option. Automated notification services are applications that use a combination of methods that are designed to contact large groups or multiple types of groups within the organization in a very short time period. Emergency contact information can be printed on small cards, along with contact information of coworkers, and issued to personnel to be stored with their identification badges as a normal practice. It is important to remember that personnel contact information is considered privacy information, and it must be appropriately protected.

While the OEP provides guidance on facility evacuation, it may be safer to remain within the facility in response to certain emergency situations. Shelter-in-place plans provide instruction to personnel on how to take refuge indoors in response to unsafe environment outside of the facility or contaminations inside the facility which could be carried outside and spread. Shelter-in-place planning identifies "safe rooms" on each floor of the facility. Safe rooms are equipped with emergency resources such as flashlights, radios for communication, and water. Safe rooms are also identifiable from the window so that first responders can locate offices where personnel may have taken shelter.

The General Serves Administration provides a template and guidance on OEP development at http://www.gsa.gov/gsa/cm_attachments/GSA_BASIC/OEP_Guide_R2-qR1-n_0Z5RDZ-i34K-pR.pdf.

Personnel Health

Pandemic Influenza (PI) is a global outbreak of disease that occurs when a new influenza virus emerges in human populations and causes serious illness. Because there is little natural immunity, the disease can spread easily from person to person, rapidly moving across the country and around the world. The Homeland Security Council, *The National Strategy for Pandemic Influenza Implementation Plan*, May 2006, requires federal organizations to develop plans to address how the organization will:

- Protect employees during a pandemic;
- Sustain essential functions during significant times of absenteeism;
- Support the overall federal response during a pandemic; and
- Communicate guidance to stakeholders during a pandemic.

Common strategies to protect personnel health during a pandemic outbreak include stricter hygiene precautions and reducing the number of personnel working in close contact with one another through implementation of "social distancing." Approved telework arrangements facilitate social distancing through working at home while sustaining productivity. Government-run telework sites are also available to federal employees who cannot work from home or the office. The Office of Personnel Management provides guidance and resources for developing Pandemic Influenza plans in coordination with the organization's Continuity of Operations Plan, human capital policy and strategies during a pandemic, and telework arrangements.

The World Health Organization provides fact sheets on Avian Influenza at http://www.who.int/mediacentre/factsheets/avian_influenza/en/.

OPM provides information and guidance on Pandemic Influenza planning at http://www.opm.gov/pandemic/index.asp. The Web site also provides human capital guidance on issues including pay, leave, hiring, and alternate work arrangements.

OPM and GSA provide information and guidance on federal telework programs from the manager, employee, and Telework coordinator perspectives at www.telework.gov. Telework centers are also listed on this site.

Personnel Welfare

During a serious situation, addressing personnel and family matters often takes priority over resuming business. Planning for such matters may involve pre-identification of temporary housing, work space, and staffing. In some situations, the organization may need to use personnel from associated organizations or contract with vendors or consultants if both primary and alternate team members are unavailable or unable to fulfill responsibilities. Preparations should be made during contingency planning development for this possibility to ensure that the vendors or consultants can achieve the same access as the team members could in the event of a disaster. Once personnel are ready to return to work,

arrangements should be made for them to work at an alternate site or at home if the facility is unsafe or unavailable for use. This is an alternate space *in addition to* the alternate site for information system recovery. Personnel with home computers or laptops should be given instruction, if appropriate, on how to access the organization's network from home. It may also be necessary to assist personnel with procuring temporary housing. Planning for long-term relocations, such as those that took place in response to Hurricane Katrina, should consider locating the alternate site near areas with available housing in safe neighborhoods with schools and other family necessities.

Disasters may take a heavy psychological toll on personnel, especially if there has been loss of life or extensive physical destruction. Organizations should be prepared to provide grief counseling and other mental health support. The Employee Assistance Program (EAP), which is available to all federal organizations, is a useful and confidential resource for these issues. Nonprofit organizations, such as the American Red Cross, also provide referrals for counseling services as well as food, clothing, and other assistance programs. Personnel will be most interested in the status of the health benefits and resumption of payroll. It is very important that the organization communicate this status. *Every effort should be made to continue to pay personnel as per normal operations*. Due to grief and stress, productivity may also be low during the adjustment period.

The Department of Homeland Security provides family readiness guidance at www.Ready.gov. The Family Emergency Plan is available through this site at http://www.ready.gov/america/_downloads/familyemergencyplan.pdf.

Information on the Federal Employee Assistance Program can be found at http://www.opm.gov/Employment_and_Benefits/WorkLife/HealthWellness/EAP/index.asp.

Nonprofit disaster assistance information is available at http://www.redcross.org.

Relationships with Response Organizations

A relationship should be built with local fire and police departments in order to achieve a thorough understanding of the first response procedures and to achieve a trust relationship so that the organization is not first meeting local fire and police departments in a disaster. Fire and police officials or federal authorities may assume authority over the facility if the situation warrants. The organization should be aware of why this may happen and what points of contact (POCs) and documentation will be needed to regain access to their facility. Fire, police, and rescue organizations are often willing to work with the organization to develop safe and coordinated procedures and participate in the organization's exercises. Based on the organization's requirements, joint planning and exercises with federal or military respondents may also be necessary.

Local response organizations should be contacted directly or through state emergency management.

Communication Planning

The crisis communication plan typically addresses internal communication flows to personnel and management and external communication with the public. The most effective way to provide helpful information and to reduce rumors is to *communicate clearly and often*. The plan should also prepare the organization for the possibility that during a significant disaster, the organization may be a communication-forwarding point between personnel, civil and federal authorities, and affected families and friends.

One of the most important activities is internal communication within the organization. Staff and management need to know what has occurred, the status of the situation, what actions they should take,

and who is in charge of the situation. One person or team should be responsible for internal communication. This person should have access to the organization's senior leadership. In addition, the organization should be prepared to use multiple communication methods such as voicemail, email, flyers, Web site announcements, or social networking (if approved).[45] Clear and frequent communications from senior executives to all personnel, interconnected POCs, and end users is necessary after a disruption to assist calming internal anxiousness, worry, and answering general questions.

Like internal communication, organizations should pay deliberate attention to the message being communicated to external parties. Again, an effective method is to designate a specific POC or team from the organization to be responsible for press releases and media communication. The POC or team's procedures often involve input from Counsel in approving public statements. This ensures that there is a single responsible message delivered stating the facts of the situation, as known, and what actions are being taken. Personnel should be trained to refer all media requests to a single POC or public information office without making any of their own comments on behalf of the organization. These procedures may also be stated in the OEP or in public information office guidance.

Some federal departments have internal social networking tools. Governmentwide social networks are also available such as www.GovLoop.com .

[45] At the time of publication, social networking is an emerging communication tool. Federal government policies on the use of social networking are being established but do not yet exist across all departments. Social networking may prove to be an effective means to push crisis information out to personnel, but must be an approved method and have a way to ensure that the message is received and authenticated.

Appendix E—Contingency Planning Controls

The following Contingency Planning (CP) controls are from NIST SP 800-53, Rev. 3.

Table E-1: Summary of NIST SP 800-53 Contingency Planning Controls for Low-, Moderate- and High- Impact Systems of Contingency-Related Plans[46]

Control No.	Control Name	Security Controls and Enhancements		
		Low	Moderate	High
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2) (3)
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercise	CP-4	CP-4 (1)	CP-4 (1) (2) (4)
CP-5	Contingency Plan Update (Withdrawn)	------	-----	------
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3) (4) (5)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10 (2) (3)	CP-10 (2) (3) (4)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of the security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy.

Control Enhancements: None.

LOW CP-1	**MOD** CP-1	**HIGH** CP-1

[46] Numbers in parentheses in this table refer to Control Enhancements defined for that control in NIST SP 800-53, Rev. 3. A control enhancement either adds related functionality or strengthens a basic control. Starting with NIST SP 800-53, Rev. 3, CP-5 has been incorporated into CP-2, and has been removed as a control.

CP-2 CONTINGENCY PLAN

Control: The organization:

a. Develops a contingency plan for the information system that:

- Identifies essential mission and business processes and associated contingency requirements;
- Provides restoration priorities and metrics;
- Addresses contingency roles, responsibilities, and assigned individuals with contact information;
- Addresses maintaining essential missions and business processes despite an information system disruption, compromise, or failure;
- Addresses eventual full information system restoration without deterioration of the security measures originally planned; and
- Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel and organizational elements, identified by name and/or by role*];

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*];

e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing ; and

f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel and organizational elements, identified by name and/or by role*].

Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack.

Control Enhancements:

(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.

> **Enhancement Supplemental Guidance:** Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.

(2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

(3) The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

(4) The organization plans for the full resumption of missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

(5) The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

(6) The organization provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.

LOW CP-2	**MOD** CP-2 (1)	**HIGH** CP-2 (1) (2) (3)

CP-3 CONTINGENCY TRAINING

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

LOW CP-3	**MOD** CP-3	**HIGH** CP-3 (1)

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization:

a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and

b. Reviews the contingency plan test/exercise results and initiates corrective actions.

Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation; parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on organizational

operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.

Control Enhancements:

(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

> **Enhancement Supplemental Guidance**: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.

(2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

(3) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.

(4) The organization includes a full recovery and reconstitution of the information system to a known [*Selection: secure; safe*] state as part of contingency plan testing.

LOW CP-4	**MOD** CP-4 (1)	**HIGH** CP-4 (1) (2) (4)

CP-6 ALTERNATE STORAGE SITE

Control: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.

Supplemental Guidance: Related controls: CP-2, CP-9, MP-4.

Control Enhancements:

(1) The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.

(2) The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

> **Enhancement Supplemental Guidance**: Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.

LOW Not Selected	**MOD** CP-6 (1) (3)	**HIGH** CP-6 (1) (2) (3)

CP-7 ALTERNATE PROCESSING SITE

Control: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period consistent with recovery time objectives*] when the primary processing capabilities are unavailable; and

b. Ensures that equipment and supplies required to resume operations within the organization-defined time period, are either available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.

Supplemental Guidance: Related control: CP-2.

Control Enhancements:

(1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.

Enhancement Supplemental Guidance: Hazards that might affect the information system are typically defined in the risk assessment.

(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(4) The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.

(5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

LOW Not Selected	**MOD** CP-7 (1) (2) (3) (5)	**HIGH** CP-7 (1) (2) (3) (4) (5)

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.

Supplemental Guidance: Related control: CP-2.

Control Enhancements:

(1) The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

(2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

(3) The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.

(4) The organization requires primary and alternate telecommunications service providers to have contingency plans.

LOW Not Selected	**MOD** CP-8 (1) (2)	**HIGH** CP-8 (1) (2) (3) (4)

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization:

a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];
b. Conducts backups of system-level information (including system-state information) contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];
c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and
d. Protects the confidentiality and integrity of backup information at the storage location.

Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control. Related controls: CP-6, MP-4.

Control Enhancements:

(1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.

(2) The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

(3) The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware,

software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

(4) [Withdrawn: Incorporated into CP-9].

(5) The organization transfers information system backup information to the alternate storage site [*Assignment: organization-defined transfer rate consistent with the recovery time and recovery point objectives*].

(6) The organization accomplishes information system backup by maintaining a redundant secondary system, not collocated, that can be activated without loss of information or disruption to the operation.

LOW CP-9	**MOD** CP-9 (1)	**HIGH** CP-9 (1) (2) (3)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Supplemental Guidance: Recovery and reconstitution to a known secure state means that all system parameters (default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested. The information system recovery and reconstitution capability employed by the organization is based on organizational priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. The recovery and reconstitution includes the deactivation of any information systems located at the relocation site. Deactivation is the process of finalizing the system recovery and validation operations and includes the necessary activities to prepare the system against another outage or disruption. The recovery and reconstitution capability employed by the organization can be a combination of automated mechanisms and manual procedures.

Control Enhancements:

(1) [Withdrawn: Incorporated into CP-4].

(2) The organization implements transaction recovery for information systems that are transaction-based.

> **Enhancement Supplemental Guidance:** Database management systems and transaction-processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.

(3) The organization provides compensating security controls for [*Assignment: organization-defined circumstances that inhibit recovery to a known, secure state*].

(4) The organization provides the capability to re-image information system components in accordance with [*Assignment: organization defined restoration time-periods*] from configuration-controlled and integrity-protected disk images representing a secure operational state for the components.

(5) The organization provides [*Selection: real-time; near real-time*] [*Assignment: organization-defined failover capability for the information system*].

Enhancement Supplemental Guidance: Examples of failover capability are incorporating mirrored information system operations at an alternate processing site or periodic data mirroring at regular intervals during a time period defined by the organization's restoration time period.

(6) The organization protects backup and restoration hardware, firmware, and software.

Enhancement Supplemental Guidance: Protection of backup and restoration hardware, firmware, and software includes both physical and technical measures. Router tables, compilers, and other security-relevant system software are examples of backup and restoration software.

LOW CP-10	**MOD** CP-10 (2) (3)	**HIGH** CP-10 (2) (3) (4)

Appendix F—Contingency Planning and the System Development Life Cycle (SDLC)

The system development life cycle (SDLC) refers to the full scope of activities conducted by federal information system owners associated with a system during its life span. The life cycle, depicted in Figure F-1, begins with *Initiation* and ends with *Disposition.*[47] Although contingency planning is associated with activities occurring mostly in the *Operation/Maintenance* phase, identification and integration of contingency and continuity strategies at all phases of the information system life cycle allow the owner to build layered protection against risks and assist implementation of effective recovery strategies early on in the system development. This approach reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is implemented. This section introduces common ways in which contingency strategies can be incorporated throughout the SDLC. A summary of implementation periods for CP controls throughout the SDLC is provided in Table F-1. For a specific description of contingency activities and strategies, see Chapter 5, Technical Contingency Planning Considerations.

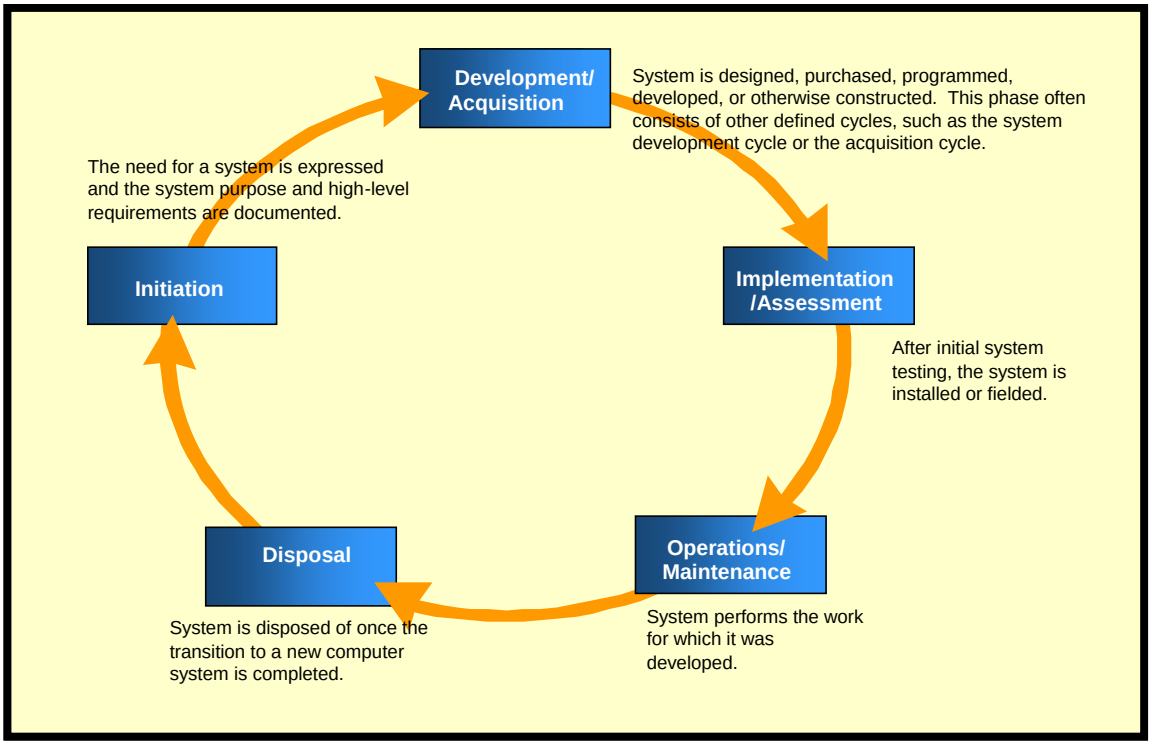

Figure F-1: System Development Life Cycle

Initiation Phase. Contingency planning requirements should be considered when a new information system is conceived. During *Initiation*, early contingency planning considerations may become apparent as information system requirements are identified and matched to their related operational functions, a risk assessment is conducted to understand what the system will need protection against, and confidentiality, integrity, and availability objectives are set. High information system availability requirements may indicate that redundant, real-time mirroring at an alternate site and failover capabilities should be built into the system design. Similarly, if the system is intended as a virtual application, the design may need to include additional features, such as remote diagnostic or self-healing capabilities.

[47] There are several models of the system development life cycle. The model used for this document is consistent with NIST Special Publication 800-64, Rev. 1, *Security Considerations in the Information System Development Life Cycle.*

During the *Initiation*, the mission/business processes that the new information system will support should be evaluated to determine the users' recovery time requirements.

Contingency Planning controls to be addressed during this phase include:

- CP 1: Contingency Planning Policy and Procedures;
- CP 6: Alternate Storage Site;
- CP 7: Alternate Processing Site;
- CP 8: Telecommunications Services; and
- CP 9: Information System Backup.

Development/Acquisition Phase. As initial concepts evolve into information system development, specific contingency solutions may be determined. As in the Initiation phase, technical contingency planning considerations 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 later Operation/Maintenance phase. By considering the recovery strategy during the initial design, costs are reduced and problems associated with retrofitting or modifying the system during the Operation/Maintenance phase are minimized. Security controls are refined during the Development/Acquisition phase, lending an opportunity to ensure that contingency planning controls are appropriately addressed by the recovery strategy. If multiple applications are hosted within the new information system, recovery priority sequence for those applications should be set to assist with selecting the appropriate recovery strategy and sequencing for the contingency plan implementation. Examples of contingency measures that should be considered in this phase are redundant communications paths, elimination 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. If a recovery site is chosen as part of the strategy, requirements for the alternate site should be addressed in this phase.

Contingency Planning controls to be addressed during this phase include:

- CP 6: Alternate Storage Site;
- CP 7: Alternate Processing Site;
- CP 8: Telecommunications Services; and
- CP 9: Information System Backup.

Implementation/Assessment Phase. The recovery strategy selected is now documented into the formal Information System Contingency Plan in coordination with the System Test and Evaluation (ST&E) effort. As the system undergoes an initial testing, contingency strategies also should be exercised to resolve any issues with the procedures. Exercise results may prompt modifications to the recovery procedures and the contingency plan.

Contingency Planning controls to be addressed during this phase include:

- CP 2: Contingency Plan;
- CP 3: Contingency Training; and
- CP 4: Contingency Plan Testing and Exercise.

Operation/Maintenance Phase. When the information system is operational, users, administrators, and managers should maintain a test, training, and exercise program which continually validates the

contingency plan procedures and technical recovery strategy. Exercises and tests should be conducted on a scheduled basis to ensure that procedures continue to be effective. Full and incremental backups should be routinely conducted, stored offsite, rotated, and periodically validated. The contingency plan should be updated to reflect changes to procedures based on lessons learned from tests, exercises, and actual disruptions. When the information system undergoes upgrades or 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.

Contingency Planning controls to be addressed during this phase include:

- CP 2 Contingency Plan;
- CP 3: Contingency Training;
- CP 4: Contingency Plan Testing and Exercise;
- CP 9: Information System Backup; and
- CP 10: Information System Recovery and Reconstitution.

Disposal Phase. Contingency considerations should not be neglected because an information 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 ISCP should be maintained in a ready state for implementation. As legacy systems are replaced, they may provide a valuable capability as a redundant system if a loss or failure of the new information system should occur. In some cases, equipment parts (e.g., hard drives, power supplies, memory chips, or network cards) from hardware that has been replaced can be used as spare parts for new operational equipment. In addition, legacy information systems can be used as test systems for new applications, allowing potentially disruptive system flaws to be identified and corrected in a nonproduction environment.

Contingency Planning controls to be addressed during this phase include:

- CP 2 Contingency Plan;
- CP 9: Information System Backup; and
- CP 10: Information System Recovery and Reconstitution.

Table F-1: CP Control Implementation in the SDLC

Control No.	Control Name	Initiation Phase	Acquisition / Development Phase	Implementation / Assessment Phase	Operation/ Maintenance Phase	Sunset
CP-1	Contingency Planning Policy and Procedures	X				
CP-2	Contingency Plan			X	X	X
CP-3	Contingency Training			X	X	
CP-4	Contingency Plan Testing and Exercise			X	X	
CP-5	Contingency Plan Update (Withdrawn)	------	------	------	------	------
CP-6	Alternate Storage Site	X	X			
CP-7	Alternate Processing Site	X	X			
CP-8	Telecommunica-tions Services	X	X			
CP-9	Information System Backup	X	X		X	X
CP-10	Information System Recovery and Reconstitution				X	X

Appendix G—Glossary

This appendix provides definitions for terminology used within Special Publication 800-34. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST.

Backup:	A copy of files and programs made to facilitate recovery if necessary.
Business Continuity Plan (BCP):	The documentation of a predetermined set of instructions or procedures that describe how an organization's *mission/business processes* will be sustained during and after a significant disruption.
Business Impact Analysis (BIA):	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Cold Site:	A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.
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 Planning:	See Information System Contingency Plan.
Continuity of Operations (COOP) Plan:	A predetermined set of instructions or procedures that describe how an organization's *mission essential functions* will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.
Disaster Recovery Plan (DRP):	A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
Disruption:	An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
Hot Site:	A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption.

Impact: (NIST SP 800-60)	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Impact Level:	High, Moderate, or Low security categories of an information system established in FIPS 199 which classify the intensity of a potential impact that may occur if the information system is jeopardized.
Incident Response Plan:	The 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 information system(s).
Information System: (44 U.S.C., Sec 3502)	A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Contingency Plan (ISCP):	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.
Maximum Tolerable Downtime:	The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission.
Reciprocal Agreement:	An agreement that allows two organizations to back up each other.
Recovery Point Objective:	The point in time to which data must be recovered after an outage.
Recovery Time Objective:	The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.
Resilience:	The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.
Risk Management: (NIST SP 800-53)	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.

Security Controls: (FIPS 199)	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
System Development Life Cycle (SDLC):	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
Warm Site:	An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.

Appendix H—Acronyms

Selected acronyms used in the *Contingency Planning Guide for Federal Information Systems* are defined below.

ATM	Asynchronous Transfer Mode
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CIKR	Critical Infrastructure And Key Resources
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
COOP	Continuity Of Operations
CP	Contingency Plan/Contingency Planning
DASD	Direct Access Storage Device
DNS	Domain Name Service
DRP	Disaster Recovery Plan
DS	Digital Signal
DVD	Digital Video Disc
DVD-ROM	Digital Video Disc - Read-Only Memory
DVD-RW	Digital Video Disc - Rewritable
EAP	Employee Assistance Program
FCD	Federal Continuity Directive
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTE	Full-Time Equivalent
GB	Gigabyte
GSA	General Services Administration
HA	High Availability
HSPD	Homeland Security Presidential Directive
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation, And Air Conditioning
I/O	Input/Output
IS	Information System
ISA	Interconnection Security Agreement
ISP	Internet Service Provider
ISCP	Information System Contingency Plan
ISSM	Information System Security Manager
ISSO	Information System Security Officer
LAN	Local Area Network

MAO	Maximum Allowable Outage
MB	Megabyte
Mbps	Megabits Per Second
MEF	Mission Essential Functions
MOA	Memorandum Of Agreement
MOU	Memorandum Of Understanding
MTD	Maximum Tolerable Downtime
NAS	Network-Attached Storage
NEF	National Essential Functions
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NSP	Network Service Provider
NSPD	National Security Presidential Directive
OEP	Occupant Emergency Plan
OMB	Office of Management and Budget
PI	Pandemic Influenza
PMEF	Primary Mission Essential Functions
POC	Point Of Contact
RAID	Redundant Array Of Independent Disks
RMF	Risk Management Framework
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAISO	**S**enior Agency Information Security Officer
SAN	Storage Area Network
SDLC	System Development Life Cycle
SLA	Service-Level Agreement
SONET	Synchronous Optical Network
SP	Special Publication
ST&E	Security Test And Evaluation
TT&E	Test, Training, And Exercise
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTL	Virtual Tape Library
WAN	Wide Area Network
WiFi	Wireless

Appendix I—Resources

The following laws, policies, directives, standards, and guidelines were used as resources in developing NIST SP 800-34. Rev.1.

Print Resources

Draft NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

Federal Continuity Directive (FCD) 1, *Federal Executive Branch National Continuity Program and Requirements*, February 2008.

FCD 2, *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, February 2008.

Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

Federal Information Security Management Act (P.L. 107-347-Title III), December 2002.

Federal Protective Service, *Occupant Emergency Plans: Development, Implementation, and Maintenance*, November 2007.

Homeland Security Presidential Directive - 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.

Homeland Security Presidential Directive - 20/National Security Presidential Directive - 51, *National Continuity Policy*, May 9, 2007.

National Security Presidential Decision Directive 1, *Organization of the National Security Council System*, February 13, 2001.

National Continuity Policy Implementation Plan, August 2007.

National Institutes of Standards and Technology (NIST) Special Publication (SP) 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010.

NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

NIST SP 800-53, Rev.3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

NIST SP 800-60, *Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

NIST SP 800-84, *Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities*, September 2006.

National Response Framework, March 22, 2008.

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, November 2000.

Office of Personnel Management (OPM) *Human Capital Planning for a Pandemic Influenza Outbreak: Information for Agencies and Departments*, September 2006.

Presidential Decision Directive (PDD) 62, *Protection against Unconventional Threats to the Homeland and Americans Overseas*, May 22, 1998.

PDD 63, *Critical Infrastructure Protection*, May 22, 1998.

Privacy Act of 1974 (P.L. 93-579), December 1974.

Title 36 Code of Federal Regulations Section 1236, *Management of Vital Records*, May 16, 2001.

Title 41, CFR 101.20.003, Occupant Emergency Program, revised July 1, 2000.

Web Resources

Organization	URL
GovLoop	http://www.govloop.com
Contingency Planning and Management	www.contingencyplanning.com
Disaster Recovery Institute International	www.drii.org
Disaster Recovery Journal	www.drj.com
World Health Organization, Avian Influenza Fact Sheet	http://www.who.int/mediacentre/factsheets/avian_influenza/en/
OPM, Pandemic Influenza Information	http://www.opm.gov/pandemic/index.asp
Telework.gov (OPM and GSA)	www.telework.gov/
Ready.gov (Department of Homeland Security)	www.ready.gov/
Ready.gov, Family Emergency Plan	http://www.ready.gov/america/_downloads/familyemergencyplan.pdf
OPM, Employee Assistance Programs	http://www.opm.gov/Employment_and_Benefits/WorkLife/HealthWellness/EAP/index.asp
American Red Cross Disaster Services	https://americanredcross.com/services/disaster/0,1082,0_500_,00.html