# IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29

**Revision 6**

September 16, 2022

*Office of the Chief Information Security Officer*

# VERSION HISTORY/CHANGE RECORD

| Change Number | Person Posting Change | Change | Reason for Change | Page Number of Change |
|---|---|---|---|---|
| | | **Revision 1 – February 22, 2007** | | |
| 1 | Bo Berlas | Clarified functional testing requirement. | NIST 800-53, R1. | 6 |
| 2 | Bo Berlas | New Appendix E | OIG Audit recommendation for agency guidance for contingency plan training, plan maintenance, and backups. | 22 |
| | | **Revision 2 – August 16, 2010** | | |
| 1 | Berlas/Cook | Updated NIST controls to align with SP 800-53 Revision 3. | NIST 800-53, R3. | Throughout |
| | | **Revision 3 – March 9, 2016** | | |
| 1 | Sitcharing/ Wilson | • Updated NIST controls to align with SP 800-53 Revision 4. | NIST 800-53, R4 & IT Security Program Plan | Throughout |
| | | **Revision 4 – April 12, 2018** | | |
| 1 | Feliksa/Dean | • Updated format and NIST SP 800-53 control parameters, added a section on SCRM, included EO 13800 and NIST Cybersecurity Framework. | Biennial update. | Throughout |
| | | **Revision 5 – July 27, 2020** | | |
| 1 | Klemens/Dean | Primary changes:<br>• Changed parameter for NIST SP 800-53 control CP-9, Information System Backup<br>• Updated the ICT SCRM section to include all CP controls/enhancements from NIST 800-161<br>• Modified formatting and style to latest guidance, including 508 compliance. | Biennial update. | Throughout |
| | | **Revision 6 - September 16, 2022** | | |
| 1 | Klemens/Dean | Revisions include:<br>• Updated to NIST SP 800-53, Revision 5 controls, GSA parameters, and implementation statements.<br>• Updated format and content.<br>• Included IR scenario for contingency plan testing. | Align to current NIST guidance and GSA parameters. New or substantively changed controls in Revision 5 are: CP-1, CP-2(5), CP-2(8), CP-3, CP-9, CP-9(8), CP-10. | Throughout |

# APPROVAL

IT Security Procedural Guide: Contingency Planning (CP), CIO-IT Security-06-29, Revision 6 is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

**Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.**

# Table of Contents

**Notes:**

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Section 1.4.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

# 1 Introduction

Contingency planning (CP) focuses on the recovery and restoration of an Information Technology (IT) system following a disruption. General Services Administration (GSA) Order OMA 2430.2, "The U.S. General Services Administration Continuity of Operations Mission Essential Functions" supports the agency Continuity of Operations Plan (COOP) required by Presidential Policy Directive (PPD) 40[1], "National Continuity Policy" ensuring that primary mission-essential functions continue to be performed during a wide range of emergencies. Contingency and continuity of support plans must be developed and tested for all IT systems in accordance with Office of Management and Budget (OMB) Circular No. A-130, "Managing Information as a Strategic Resource," National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems," and GSA policies, directives, and procedures. The CP principles and practices described in this guide are based on guidance from NIST, including NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations." This guide provides an overview of CP roles and responsibilities, NIST SP 800-53 CP requirements per Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," security categorization level, and procedures for implementing these requirements. Throughout the remainder of this guide the identifier CP will be used when referring to the NIST Contingency Planning controls or the control family, otherwise contingency planning will be used.

Every GSA system must follow the practices identified in this guide. Any deviations from the security requirements established in GSA Order Chief Information Officer (CIO) 2100.1, "GSA Information Technology (IT) Security Policy" must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation/Waiver Request Google Form.

Executive Order (EO) 13800, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" requires all agencies to use "The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST or any successor document to manage the agency's cybersecurity risk." This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework (RMF) from NIST SP 800-37, Revision 2, "Risk Management

[1] PPD 40 is not available for public dissemination.

Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." Table 1-1 lists the Categories and Subcategories from the CSF that are identified as related to the implementation of policies, procedures, and processes implementing the CP control family.

**Table 1-1: CSF Categories/Subcategories and the CP Control Family**

| CSF Category/Subcategory Identifier | Definition/Description |
|---|---|
| **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | **ID.AM-5:** Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value *(CP-2)*<br><br>**ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established *(CP-2)* |
| **Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. | **ID.BE-1:** The organization's role in the supply chain is identified and communicated *(CP-2)*<br><br>**ID.BE-4:** Dependencies and critical functions for delivery of critical services are established *(CP-8)*<br><br>**ID.BE-5:** Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations) |
| **Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | **ID.GV-1:** Organizational cybersecurity policy is established and communicated. *(CIO 2100.1 and Sections 1.3 and 3.1 of this guide)*<br><br>**ID.GV-2**: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners *(CIO 2100.1 and Section 2 of this guide)* |
| **Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks. | **ID.SC-5**: Response and recovery planning and testing are conducted with suppliers and third-party providers *(CP-2, CP-4)* |
| **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. | **PR.IP-4:** Backups of information are conducted, maintained, and tested *(CP-4, CP-6, CP-9)*<br><br>**PR.IP-7:** Protection processes are improved *(CP-2)*<br><br>**PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed *(CP-2, CP-7)*<br><br>**PR.IP-10:** Response and recovery plans are tested *(CP-4)* |
| **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. | **PR.PT-4:** Communications and control networks are protected *(CP-8)*<br><br>**PR.PT-5:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations *(CP-7, CP-8)* |

| CSF Category/Subcategory Identifier | Definition/Description |
|---|---|
| **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | ***DE.AE-4:*** *Impact of events is determined (CP-2)* |
| **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. | **RS.RP-1**: Response plan is executed during or after an incident *(CP-2, CP-10)* |
| **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies). | **RS.CO-1**: Personnel know their roles and order of operations when a response is needed (*CP-2)*<br>**RS.CO-4:** Coordination with stakeholders occurs consistent with response plans *(CP-2)* |
| **Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities. | **RS.AN-2:** The impact of the incident is understood *(CP-2)*<br>**RS.AN-4**: Incidents are categorized consistent with response plans *(CP-2)* |
| **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | **RS.IM-1**: Response plans incorporate lessons learned (CP-2)<br>**RS.IM-2:** Response strategies are updated (CP-2) |
| **Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. | **RC.RP-1**: Recovery plan is executed during or after a cybersecurity incident *(CP-10)* |
| **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | **RC.IM-1:** Recovery plans incorporate lessons learned *(CP-2)*<br>**RC.IM-2:** Recovery strategies are updated *(CP-2)* |
| **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). | **RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams *(CP-2)* |

## 1.1 Purpose

The purpose of this guide is to provide guidance for the CP security controls identified in NIST SP 800-53 and contingency planning requirements specified in CIO 2100.1. This procedural guide provides GSA Federal employees and contractors with significant security responsibilities, as identified in CIO 2100.1, and other IT personnel involved in the contingency planning of IT assets, the specific procedures and processes they are to follow for GSA information systems under their purview.

## 1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in the contingency planning of GSA systems and information. All GSA systems must adhere to the requirements and guidance provided with regard to the procedures, processes, and methods for providing contingency planning as described in this guide. Per CIO 2100.1, a GSA system is a system:

- used or operated by GSA; or
- used or operated on behalf of GSA by a contractor of GSA or by another organization.

## 1.3 Policy

CIO 2100.1 contains the following policy statements regarding contingency planning.

***Chapter 3, Policy for Identify Function***

1. *Asset Management.*
   *h. As part of a system's contingency planning process, resources must be prioritized based on their classification, criticality, and business value. A BIA is required as part of the system's contingency plan.*

2. *Business Environment.*
   *e. GSA system contingency plan's BIA should prioritize business missions in relation to the systems supporting the mission objectives and activities.*
   *f. GSA system contingency plan's BIA should identify critical services and any dependencies regarding those services.*
   *i. GSA system contingency plans must address the ability to continue missions under all operating states (e.g., disasters/attacks, recovery, and restoration to normal operations).*

***Chapter 4, Policy for Protect Function***

4. *Information Protection Processes and Procedures.*
   *s. Contingency plans must be developed and revised annually, as necessary, for all IT systems IAW GSA CIO-IT Security-06-29. The plans must include recovery procedures, a separate disaster recovery plan may be developed if necessary.*
   *u. Contingency plans must be annually tested IAW GSA CIO-IT Security-06-29.*

***Chapter 6, Policy for Respond Function***

1. *Response Planning.*
   *a. All information systems must have their contingency plans and incident response plans tested annually.*
   *b. Lessons learned during contingency plan and incident response plan tests must be incorporated into revised plans.*

2. *Communications.*
   *b. Personnel with contingency planning responsibilities must be trained in their contingency roles and responsibilities with respect to the information system annually.*

5. *Improvements.*
   *b. Contingency plans must be updated based on lessons learned during responses to disasters, other events invoking the contingency plan or plan testing.*

***Chapter 7, Policy for Recover Function***

1. *Recovery Planning. As part of a system's contingency planning process, recovery plans are exercised as part of a cybersecurity incident response or after the response, as appropriate.*
2. *Improvements.*
   *a. As part of a system's contingency planning processes, lessons learned from contingency plan tests regarding recovery must be incorporated into a revised contingency plan.*
   *b. As part of the system's contingency plan testing and incident responses or incident response plan testing, any lessons learned regarding recovery strategies will be updated in the appropriate plan.*

## 1.4 References

**Federal Laws, Standards, Regulations, and Publications:**

- EO 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- NIST CSF, Version 1.1, "Framework for Improving Critical Infrastructure Cybersecurity"
- NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems"
- NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- NIST SP 800-84, "Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities"
- OMB Circular A-130, "Managing Information as a Strategic Resource"

**GSA Policies, Procedures, Guidance:**

The GSA policies listed below are available on the GSA.gov Directives Library page with the exception of GSA Order ADM 2430.2, it is available on the internal GSA InSite Directives Library page.

- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"
- GSA Order CIO 2140.4, "GSA Information Technology (I VT) Solutions Life Cycle (SLC) Policy"
- GSA Order ADM 2430.2, "The U.S. General Services Administration Continuity of Operations Mission Essential Functions"

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page with the exception of CIO-IT Security-18-90 which is restricted. It is available on the internal GSA InSite IT Security Procedural Guides page.

- CIO-IT Security-06-30, "Managing Enterprise Cybersecurity Risk"
- CIO-IT Security-09-44, "Plan of Action and Milestones (POA&M)"
- CIO-IT Security-18-90, "Information Security Program Plan (ISPP)"

# 2 Contingency Planning Roles and Responsibilities

There are many roles associated with implementing effective contingency planning for IT systems. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. Throughout this guide, specific processes and procedures for implementing NIST's CP controls are described.

## 2.1 Authorizing Official (AO)

Responsibilities include the following:

- Ensuring cybersecurity is included in management planning, programming budgets, and the IT Capital Planning process.
- Ensuring contingency plans are developed and tested annually IAW OMB Circular A-130, NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, and GSA CIO-IT Security-06-29, "Contingency Planning (CP)."
- Ensuring that GSA information systems under their purview have implemented the required NIST SP 800-53 CP controls in accordance with GSA and Federal policies and requirements.
- Identifying the level of acceptable risk for an information system and determining whether an acceptable level of risk has been obtained, including risks associated with NIST SP 800-53 CP controls.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current Authorization to Operate (ATO) issued per GSA CIO-IT Security-06-30.
- Ensuring a plan of action and milestones (POA&M) entry is developed and managed to address any NIST SP 800-53 CP controls that are not fully implemented.

## 2.2 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Ensuring necessary NIST SP 800-53 CP controls are in place and operating as intended.
- Coordinating with ISSMs and System Owners, as necessary, identifying NIST SP 800-53 CP control implementation and compliance with NIST and GSA requirements.
- Reviewing and coordinating reporting of Security Advisory Alerts (SAAs), compliance reviews, security awareness training, incident reports, contingency plan testing, and other IT security program elements.
- Working with the System Owner and ISSM to develop and manage POA&Ms regarding NIST SP 800-53 CP controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.

## 2.3 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary NIST SP 800-53 CP controls are in place and operating as intended.
- Coordinating with ISSMs and System Owners, as necessary, and identifying NIST SP 800-53 CP control implementation and compliance with NIST and GSA requirements.
- Working with the System Owner and ISSM to develop and manage POA&Ms regarding NIST SP 800-53 CP controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.

## 2.4 System Owners

Responsibilities include the following:

- Participating in activities related to the Assessment & Authorization (A&A) of the system to include security planning, risk assessments, security and incident response testing, configuration management, and contingency planning and testing.
- Developing, implementing, and maintaining an approved IT contingency plan which includes an acceptable Business Impact Analysis (BIA).
- Ensuring necessary NIST SP 800-53 CP security controls are in place and operating as intended.
- Coordinating with ISSOs and ISSMs, as necessary, regarding NIST SP 800-53 CP control implementation and compliance with NIST and GSA requirements.
- Working with ISSOs and ISSMs to develop and manage POA&Ms regarding NIST SP 800-53 CP controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.
- Obtaining the resources necessary to securely implement and manage NIST SP 800-53 CP controls for their respective systems.

## 2.5 Data Owners

Responsibilities include the following:

- Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure data is properly stored, maintained, and protected per GSA policies, regulations, and any additional guidelines established by GSA.
- Coordinating with IT security personnel, including the ISSM and ISSO and System Owners, to ensure implementation of NIST SP 800-53 CP controls in compliance with NIST and GSA requirements.

## 2.6 Custodians

Responsibilities include the following:

- Coordinating with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected.

- Providing and administering general controls, such as back-up and recovery systems, consistent with the policies and standards issued by the Data Owner.
- Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the AO.

### 2.7 System/Network Administrators

Responsibilities include the following:

- Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines.
- Implementing system backups and remediation of security vulnerabilities, including patching, updates, configuration changes, etc.
- Working with the Custodian/ISSO to ensure appropriate technical security requirements are implemented.

## 3 IT Contingency Planning Process

Contingency planning is a coordinated strategy involving plans, procedures, and technical measures that enable a system to be recovered as quickly and effectively as possible following a service disruption. The process 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 its FIPS 199 security categorization level.

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 only for short-term disruptions);
- Recovering information systems operations at an alternate location (typically acceptable only for long-term disruptions or those physically impacting the facility); and
- Implementing appropriate NIST SP 800-53 contingency planning controls based on the information system's FIPS 199 security impact level.

NIST SP 800-34 details a seven-step methodology, depicted in Figure 3-1, which identifies the key elements in the contingency planning process. The seven steps incorporate the need to establish CP policy, determine the business criticality of systems/components, identify appropriate CP (and other controls supporting CP), develop and implement CP strategies and plans, train and test them, and maintain them for the system's lifecycle.

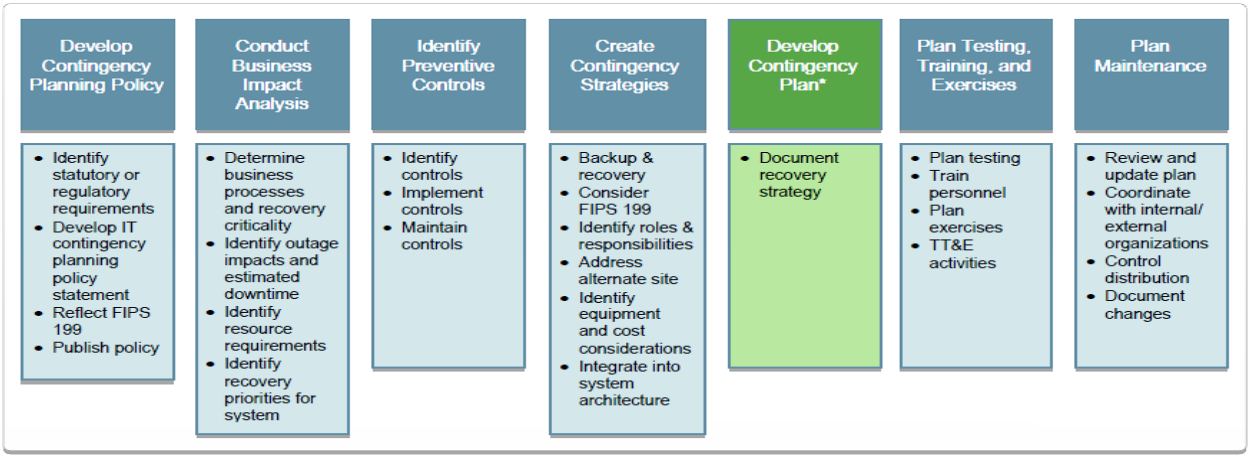


**Figure 3-1: Contingency Planning Process (Figure 3-1 from NIST SP 800-34)**

All information systems must have well developed and tested contingency plans in place to facilitate the recovery of systems, data, and operations after a disruption. The following sections detail the steps in the contingency planning process.

## 3.1 Step 1 – Develop the Contingency Planning Policy Statement

The first step in the process is to develop the contingency planning policy statement. This is critical to ensure personnel fully understand GSA's contingency planning requirements as stated in CIO Order 2100.1 and this guide.

As documented in NIST SP 800-34, the following key elements are reflected in the GSA contingency planning policy statement:

- Roles and responsibilities;
- Scope as applies to common platform types and organization functions (e.g., 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.

## 3.2 Step 2 – Conduct the Business Impact Analysis

Completion of the BIA is one of the key steps in implementing the CP controls in NIST SP 800-53 and in the contingency planning process overall. It enables GSA associates and contractors with contingency planning responsibilities to characterize the system components, supported mission/business functions, and interdependencies. The BIA correlates the system with the critical mission/business processes and services provided, and based on that information, characterizes the consequences of a disruption.

Per NIST SP 800-34, the BIA should be performed during the initiation phase of a system's lifecycle. As the system design evolves and components change, the BIA may need to be updated during the development and acquisition phases of the lifecycle. All information systems are required to conduct a BIA as part of the overall contingency planning process. The BIA development process as detailed by NIST SP 800-34, typically consists of the following steps:

1. Determine mission/business functions and recovery criticality.
2. Identify resource requirements.
3. Identify recovery priorities for system resources.

Results of the BIA are used to determine any system-specific contingency planning requirements and priorities and can be incorporated into the analysis and strategy development efforts for the COOP, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). The BIA process is fully detailed in NIST SP 800-34. A BIA template can be found on the GSA InSite IT Security Forms and Aids page.

## 3.3 Step 3 – Identify Preventive Controls

Outage impacts to the information system that have been identified in the BIA can be mitigated through the implementation of preventive controls. Preventive controls are technical measures or operational procedures taken to deter, reduce, and/or detect impacts to the information system and to prevent system disruption. Where feasible and cost-effective, preventive methods are recommended over any actions necessary to recover the system. Preventive controls are identified in NIST SP 800-53. Depending on the system type and its configuration, common measures may include such things as:

- 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;
- 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 Step 4 – Create Contingency Strategies

Contingency strategies are used to mitigate risks associated with the contingency planning family of controls in NIST SP 800-53 and may vary depending on the FIPS 199 security impact level for the information system. As documented in NIST SP 800-34, these strategies generally cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance of the information system. Detailed backup and recovery guidance for implementing appropriate backup and recovery strategies to restore system operations following a disruption can be found in Section 3.4 of NIST SP 800-34.

## 3.5 Step 5 – Develop an Information System Contingency Plan

Development of the contingency plan 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 contingency plan documents the technical capabilities designed to support contingency operations. The contingency plan format must follow NIST SP 800-34. Contingency Plan Templates for FIPS 199 Low, Moderate, and High impact systems are available on the GSA InSite IT Security Forms and Aids page. The templates may be modified to accommodate system-specific, operational, and/or organization requirements.

Figure 3-2 identifies the five main components of a contingency plan. The supporting information and plan appendices provide essential information to ensure a comprehensive contingency plan. The Activation and Notification, Recovery, and Reconstitution Phases address specific actions that must be taken following a system disruption or emergency. Detailed contingency plan development guidance can be found in Section 4 of NIST SP 800-34.

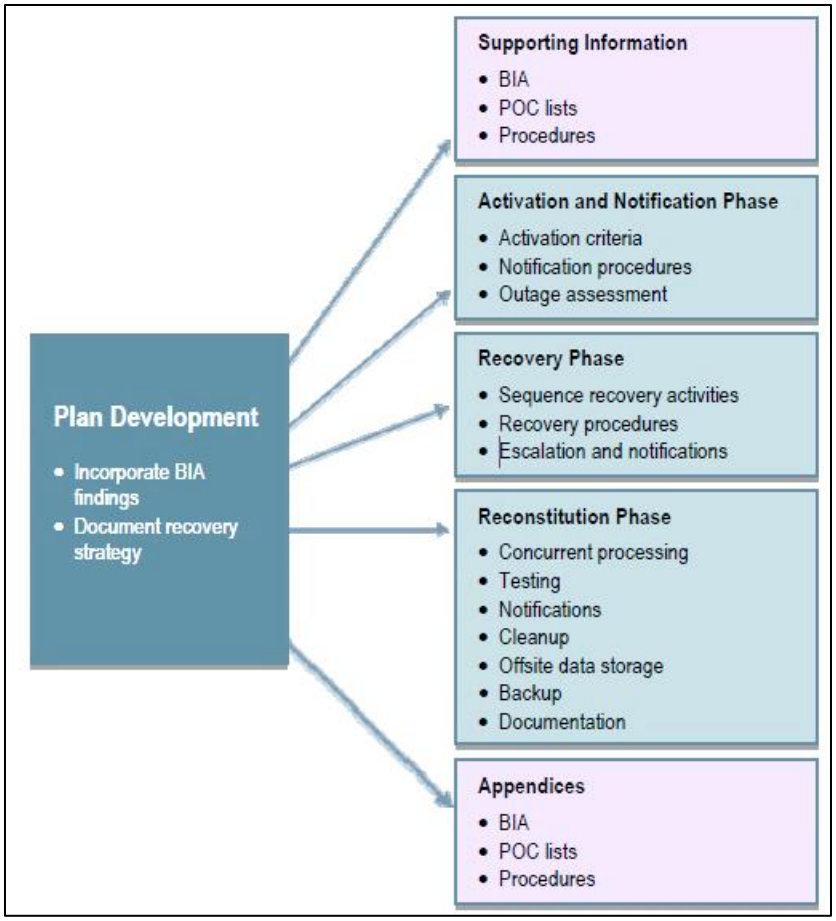


**Figure 3-2: Contingency Plan Structure (Figure 4-1 in NIST SP 800-34)**

## 3.6 Step 6 – Ensure Plan Testing and Exercises

The contingency plan must be maintained routinely and exercised/tested at least annually to continually refine resumption and recovery procedures to reduce the potential for failure. Contingency plan tests aid in determining the plan's overall effectiveness by enabling plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. The scope, scenario, and objective of each test should be varied to ensure that all of the elements of the contingency plan remain current and effective. NIST SP 800-84 provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events to capabilities to prepare for, respond to, manage, and recover from adverse events. Results from testing activities shall be documented in a Contingency Plan Test Report using the template available on the GSA InSite IT Security Forms and Aids page.

There are two categories of testing: *announced* and *unannounced*. In an announced test, personnel are informed about when testing will occur, what the objectives of the test are, and what the scenario will be for the test. Announced testing provides test participants with the opportunity to prepare for the test in advance by becoming familiar with the procedures.

Unannounced testing involves testing without prior notification. Unannounced testing focuses on the adequacy of in-place procedures and team preparedness. The combination of both test types improves the accuracy of recovery procedures and the readiness of test participants. Regardless of the test type selected, all Contingency Plan Tests should address the following key areas (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, e.g., COOP, BCP).

There are two basic formats for contingency plan tests, including:

- **Classroom or Tabletop Exercise:** 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. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

The selection of a contingency plan test format will depend on testing frequency, cost, and time. GSA requires annual contingency plan testing for all systems to determine the plan's effectiveness and the organization's readiness to execute the plan. The depth and rigor of contingency plan testing activities increase with the FIPS 199 availability security objective. All tests and exercises should include a determination of how the test/exercise affected the organization's operations. Any tests or exercises identifying a negative impact on operations should drive updates and improvements to the contingency plan, as appropriate.

- **For low impact systems, an annual tabletop exercise is sufficient.** The tabletop should simulate a disruption, include all main contingency plan points of contact, and be conducted by the system owner or responsible authority;
- **For moderate impact systems, a functional exercise must be conducted at least once every three years. A tabletop exercise is acceptable in other years.** The functional

exercise is a simulation of a disruption to a system recovery component. The test should include all contingency plan 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 backups; and

- **For high impact systems, a functional exercise must be conducted annually.** The functional exercise may vary from a simulation of a disruption to a system recovery component to a complete failure prompting a system failover to an 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 backups or setup, and processing from a server at an alternate location. The test may also include a full recovery and reconstitution of the information system to a known state. The extent of the functional exercise is up to the GSA Service and Staff Offices (SSOs) based on resources, previous exercises, and other system-specific factors.

### 3.6.1 Suggested Contingency Plan Test Actions/Key Processes

The following are suggested contingency plan test actions. These key processes are central to effective contingency plan testing and management. Steps 1-4 form the contingency test plan, step 5 is the exercise of the test plan, and step 6 involves revisions to the contingency plan and the contingency test plan following an exercise.

**Step 1: Identify contingency plan elements to test:** Review the contingency plan to select key procedures that must be tested and periodically revised to ensure that all contingency plan elements remain current and are effective. Refer to the Contingency Plan Logistics Checklist on the GSA InSite IT Security Forms and Aids page for aid in planning.

**Step 2: Define test objectives:** List the specific objective with success criteria for each test element and the overall test plan. Test objectives must include (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).

**Step 3: Identify test participants, pre-test information, location, schedule, and environment:** List each test participant and the specific roles each is to perform within the test, the test location, a test schedule, and affected system components (servers, workstation, and other components that will be tested).

**Step 4: Define test scenario and test procedures:** List the specific scenario that will be utilized for the test. In determining the scenarios, consider both the worst-case incident and those incidents that are most likely to occur. Test scenarios should mimic reality as closely as possible. Appendix B contains sample test scenarios and expected outcomes. Document steps 1-4 in a

contingency plan test plan. A Contingency Test Plan Template is available on the GSA InSite IT Security Forms and Aids page.

**Step 5: Execute test and document results:** Test results and lessons learned should be documented in a test report using the Contingency Plan Test Report Template. The results should be reviewed with the test participants and other personnel as appropriate.

**Step 6: Revision of Contingency Plan:** To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. Periodic reviews of the plan must be conducted in addition to reviews whenever there are changes affecting:

- Operational requirements;
- Security requirements;
- Technical procedures;
- Changes of hardware, software, and other equipment;
- Changes with alternate facility requirements;
- Changes with team members and team members contact information;
- Changes with vendors and vendors contact information (including alternate and off-site vendor POCs); and
- Vital records.

## 3.7 Step 7 – Ensure Plan Maintenance

The contingency plan should be reviewed and updated annually to address system/organizational changes or problems encountered during plan implementation, execution, or testing. The contingency plan is a living document and must always be current. The plan must be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. 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).

The plan reviews should also include review of 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;
- Memorandums of Understanding (MOUs) or Service Level Agreements (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.

Record changes to the plan on a change tracking matrix attached in the front of the document or in an appendix. The matrix should record the following information:

- Change number;
- Person posting change;
- Pages changed, deleted, or inserted;
- Page comment;
- Date change was posted; and
- Plan distribution.

# 4 Implementation Guidance for CP Controls

In the implementation guidance text, the GSA-defined parameter settings included in the control requirements are in blue, italicized text and offset by brackets. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to all GSA systems and must be followed by all GSA Federal employees and contractors involved in the contingency planning of GSA information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the information systems operated on behalf of GSA. Any additional instructions or requirements for contractor systems will be included in the “Additional Contractor System Considerations” portion of each control section.

Table 3-1 identifies the designation of CP controls as Common, Hybrid, or System-Specific controls for Federal and Contractor systems. Effectively, common controls are provided by GSA at the enterprise level or by one of GSA’s Major Information Systems (e.g., General Support System), system-specific controls are implemented at the system level, and hybrid controls

have shared responsibilities. CIO-IT Security 18-90, the ISPP, describes the GSA enterprise-wide common and hybrid controls and outlines the responsible parties for implementing them.

**Note:** Until the ISPP is updated to NIST SP 800-53, Revision 5, contact ispcompliance@gsa.gov for guidance if there is a discrepancy between this guide and the ISPP.

**Table 3-1: Designation of CP Controls**

| Control Designation | Federal System | Contractor System |
|---|---|---|
| **Common** | CP-1 | None |
| **Hybrid** | CP-2, CP-2(1), CP-2(2), CP-2(3), CP-2(5), CP-2(8), CP-3, CP-4, CP-4(1), CP-9, CP-9(1), CP-10, CP-10(2) | CP-1 |
| **System-Specific** | CP-3(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(4), CP-9(2), CP-9(3), CP-9(5), CP-9(8), CP-10(4) | CP-2, CP-2(1), CP-2(2), CP-2(3), CP-2(5), CP-2(8), CP-3, CP-3(1), CP-4, CP-4(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(4), CP-9, CP-9(1), CP-9(2), CP-9(3), CP-9(5), CP-9(8), CP-10, CP-10(2), CP-10(4) |

Table 3-2 identifies CP control applicability at the FIPS 199 Low, Moderate, and High levels, and for GSA's Lightweight (LATO) and Moderate Impact Software-as-a Service (MiSaaS) authorization processes.

**Table 3-2: CP Control Applicability**

| FIPS 199 Level/A&A Process | Applicable Controls |
|---|---|
| **Low** | CP-1, CP-2, CP-3, CP-4, CP-9, CP-10 |
| **Moderate** | CP-1, CP-2, CP-2(1), CP-2(3), CP-2(8), CP-3, CP-4, CP-4(1), CP-6, CP-6(1), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-8, CP-8(1), CP-8(2), CP-9, CP-9(1), CP-9(8), CP-10, CP-10(2) |
| **High** | CP-1, CP-2, CP-2(1), CP-2(2), CP-2(3), CP-2(5), CP-2(8), CP-3, CP-3(1), CP-4, CP-4(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(4), CP-9, CP-9(1), CP-9(2), CP-9(3), CP-9(5), CP-9(8), CP-10, CP-10(2), CP-10(4) |
| **LATO** | CP-7(1) |
| **MiSaaS** | CP-2, CP-4, CP-7, CP-9 |

## 4.1 CP-1 Policy and Procedures

**Control:**

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
   1. [*Organization-level*] contingency planning policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

**GSA Implementation Guidance:** Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

**Common Control Implementation:**
GSA's contingency planning policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding contingency planning for GSA systems. This policy is maintained to be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines by updating the policy via Changes, Instructional Letters, or the annual update as applicable. This policy is disseminated GSA-wide via GSA's InSite centralized agency website.

GSA's contingency planning procedures are documented in GSA IT Security Procedural Guide: CIO-IT Security-06-29, "Contingency Planning (CP)" [this guide]. The procedures facilitate the implementation of the contingency planning policy and associated controls. This guide is disseminated GSA-wide via GSA's InSite centralized agency website.

Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides. The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually. The GSA OCISO is responsible for reviewing and updating CIO-IT Security-06-29 every three years and following changes to Federal or GSA policies, requirements, or guidance.

**Federal System System-Specific Expectation:**
None, CP-1 is a common control.

**Additional Contractor System Considerations:**
Vendors/contractors must implement their own contingency planning policies and procedures which comply with the control statements, GSA's requirements, and are approved by the AO as part of the ATO process.

## 4.2 CP-2 Contingency Plan

**Control:**

a. Develop a contingency plan for the system that:
   1. Identifies essential mission and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
   5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
   6. Addresses the sharing of contingency information; and
   7. Is reviewed and approved by [*the Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), and System Owner*];
b. Distribute copies of the contingency plan to [*the Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), System Owner, Office of the Chief Information Security Officer (OCISO), and the Emergency Response Coordinator (ERC)*];
c. Coordinate contingency planning activities with incident handling activities;
d. Review the contingency plan for the system [*annually*];
e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
f. Communicate contingency plan changes to [*Authorizing Official (AO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), System Owner, and Emergency Response Coordinator (ERC)*];
g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
h. Protect the contingency plan from unauthorized disclosure and modification.

**Control Enhancements:**

(1) Contingency Plan | Coordinate With Related Plans. Coordinate contingency plan development with organizational elements responsible for related plans.
(2) Contingency Plan | Capacity Planning. Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

(3) Contingency Plan | Resume Mission and Business Functions. Plan for the resumption of [*all*] mission and business functions within [*a time period recommended by the GSA SSO or Contractor in accordance with the BIA and approved by the GSA CISO and AO*] of contingency plan activation.
(5) Contingency Plan | Continue Mission and Business Functions. Plan for the continuance of [*essential*] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.
(8) Contingency Plan | Identify Critical Assets. Identify critical system assets supporting [*all*] mission and business functions.

**GSA Implementation Guidance:** Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

GSA 2100.1 requires all information systems to have a contingency plan in accordance with NIST SP 800-34 and this guide. The contingency plan must include a BIA that prioritizes business missions in relation to the systems supporting mission objectives and activities and identifies critical services and any dependencies regarding those services. Sharing of contingency information must be addressed within the plan.

The contingency plan must be reviewed and tested annually and updated as needed. This can be done individually or in coordination with annual incident response plan testing or exercises as described in CIO-IT Security-01-02, "Incident Response (IR)." Copies of the contingency plan must be distributed to personnel who have assigned incident response roles for the information system including the AO, ISSM, ISSO, PM, CISO, and ERC. Lessons learned from testing and exercises should be incorporated into future contingency planning tests and training.

Information System Contingency Plan templates for each of the FIPS 199 impact levels are available on the GSA InSite IT Security Forms and Aids page.

For enhancements CP-2(1), (3) and (8), FIPS 199 Moderate and High impact systems must coordinate their contingency plan testing/exercises with organizational elements responsible for related plans such as Disaster Recovery, Continuity of Operations (COOP) and/or Incident Response plans.

For enhancements CP-2(2) and (5), FIPS 199 High impact systems must plan for the recovery of the systems essential business functions and mission within the recovery timeframes established by the BIA. In addition, capacity planning must be performed to ensure that information processing, telecommunications and environmental support are matched to the needs of the information system, during contingency operations.

***Additional Contractor System Considerations:*** *Vendor/contractor systems are required to comply with the control statements.*

## 4.3 CP-3 Contingency Training

**Control:**

a. Provide contingency training to system users consistent with assigned roles and responsibilities:
   1. Within [*30 days*] of assuming a contingency role or responsibility;
   2. When required by system changes; and
   3. [*Every two years*] thereafter; and

b. Review and update contingency training content [*every two years*] and following [*incidents that impacted continuity of operations*].

**Control Enhancements:**

(1) Contingency Training | Simulated Events. Incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

**GSA Implementation Guidance:** Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

All agency personnel with contingency planning responsibilities for any information system must be trained in their role(s) and responsibilities with respect to the information system. GSA requires contingency plan training to be conducted annually.

System-specific contingency planning training should be integrated as part of GSA's major information systems' annual contingency plan testing or integrated into COOP exercises.

Contingency training should complement testing activities to ensure personnel with contingency planning responsibilities are able to execute their respective recovery procedures without the aid of the actual document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours resulting from the extent of the disaster. NIST SP 800-34 requires that agency personnel with contingency planning responsibilities be provided training on the following plan elements:

- Purpose of the plan;
- Cross-team coordination and communication;
- Reporting procedures;
- Security requirements;
- Team-specific processes (Notification/Activation, Recovery, and Reconstitution Phases); and
- Individual responsibilities (Notification/Activation, Recovery, and Reconstitution Phases).

As stated in Chapter 2 of NIST SP 800-84, training may consist of:

- Informing personnel of their role(s) and responsibilities; and
- Teaching them skills related to those role(s) and responsibilities.

Training prepares personnel to perform the responsibilities when needed. Training should be structured to allow personnel to learn their responsibilities and demonstrate their understanding of them.

For enhancement CP-3(1), FIPS 199 High impact systems must incorporate simulated events into their contingency training, to ensure a more effective response in the event of system disruptions.

***Additional Contractor System Considerations:*** *Vendor/contractor systems are required to comply with the control statements.*

## 4.4 CP-4 Contingency Plan Testing

a. **Control:** Test the contingency plan for the system [*annually*] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [*GSA IT Security Procedural Guide: Contingency Planning (CP) CIO-IT Security-06-29*].
b. Review the contingency plan test results; and
c. Initiate corrective actions, if needed.

**Control Enhancements:**

(1) Contingency Plan Testing | Coordinate With Related Plans. Coordinate contingency plan testing with organizational elements responsible for related plans.
(2) Contingency Plan Testing | Alternate Processing Site. Test the contingency plan at the alternate processing site:
    (a) To familiarize contingency personnel with the facility and available resources; and
    (b) To evaluate the capabilities of the alternate processing site to support contingency operations.

**GSA Implementation Guidance:** Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

Contingency plans for all information systems must be conducted annually in accordance with this guide and NIST SP 800-84. The activity can be implemented separately or integrated with the system's annual incident response plan test as described in Section 4.4 of CIO-IT Security-01-02, "Incident Response (IR)." If testing is integrated with a Major Information System's contingency plan testing, both systems must document participation in the testing. If the contingency plan testing is conducted separately from the annual incident response plan test, it must include an incident response scenario.

Annual testing validates the contingency plan's content to improve the capabilities to prepare for, respond to, manage, and recover from adverse events that may affect GSA information systems. GSA contingency plan testing requirements per system impact level can be found in Section 3.6 of this guide, Step 6 – Ensure Plan Testing, Training, and Exercises.

Sample scenarios for testing activities can be found in (Appendix B) of this guide. Refer to NIST SP 800-84 for more specific guidance in developing, conducting, and evaluating contingency plan testing activities. Results of annual testing should be documented using the contingency plan test report template available on the GSA InSite IT Security Forms and Aids page.

For enhancement CP-4(1), FIPS 199 Moderate and High impact systems must coordinate their contingency plan testing with organizational elements responsible for related plans such as Disaster Recovery, Continuity of Operations (COOP) and/or Incident Response Plans.

For enhancement CP-4(2), FIPS 199 High impact systems must test the contingency plan at its alternate processing site to familiarize personnel with the alternate site and its resources and to gauge the alternate site's capabilities to perform system operations.

***Additional Contractor System Considerations:*** *Vendor/contractor systems are required to comply with the control statements.*

## 4.5 CP-6 Alternate Storage Site

**Control:**

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and
b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

**Control Enhancements:**

(1) Alternate Storage Site | Separation from Primary Site. Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.
(2) Alternate Storage Site | Recovery Time and Recovery Point Objectives. Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.
(3) Alternate Storage Site | Accessibility. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

**GSA Implementation Guidance:** Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

FIPS 199 Moderate and High impact systems must have an alternate storage site that is capable of maintaining duplicate copies of information and data in the event the primary storage site is unavailable. In addition to this requirement, agreements must be made between the system owner/organization and the alternate storage provider to ensure storage and retrieval capabilities are in place and that they meet the system's recovery objectives.

The following criteria must be used when considering alternate storage sites and vendors in accordance with NIST SP 800-34, Chapter 3.

- **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:** the security capabilities of the shipping method, storage facility, and personnel must all 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.

Develop and document a formal agreement such as an MOU or SLA with the alternate site organization addressing the GSA system's requirements. The information listed in NIST SP 800-34, Chapter 3 can be used to guide the development of the agreement.

For enhancements CP-6(1) and (3), FIPS 199 Moderate and High impact systems must have an alternate storage site identified in the system's contingency and security plans. The alternate storage site and accessibility to it must have sufficient physical separation from the primary site to prevent the same hazards from affecting both sites, as identified in the system's risk assessment.

For enhancement CP-6(2), FIPS 199 High impact systems must ensure any selected alternate storage site is configured to ensure the system's recovery time objective is met during recovery operations.

***Additional Contractor System Considerations:*** *Vendor/contractor systems are required to comply with the control statements.*

## 4.6 CP-7 Alternate Processing Site

**Control:**

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [information system operations] for essential mission and business functions within [*GSA SSO or Contractor recommended time period approved by the GSA CISO and AO consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and
c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

**Control Enhancements:**

(1) Alternate Processing Site | Separation from Primary Site. Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.
(2) Alternate Processing Site | Accessibility. Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outline explicit mitigation actions.
(3) Alternate Processing Site | Priority of Service. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).
(4) Alternate Processing Site | Preparation for Use. Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

**GSA Implementation Guidance:** Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

FIPS 199 Moderate and High impact systems must have an alternate processing site containing the appropriate equipment and supplies to support the information system and it must be capable of resuming system operations within the allowable timeframe established by the BIA.

Alternate processing facilities are integral to contingency planning; they enable an information system to resume operation in the event of a system or area-wide disruption at the primary site. NIST SP 800-34, Chapter 3 defines three main alternate site types and provides examples of two variations of such sites as listed 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.
- **Mirrored Sites** are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.
- **Mobile Sites** are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.

To ensure the alternate processing site can support the specific needs and requirements of the system, all FIPS 199 Moderate and High impact systems must develop and document a formal agreement such as an MOU or SLA. The MOU/SLA should address the following items.

- 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 the 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 (e.g., use of onsite office equipment, cafeteria);
- Testing, including scheduling, availability, test time duration, and additional testing, if required;
- Records management (onsite and offsite), including electronic media and hard copy;
- Service-level management (performance measures and management of quality of information system services provided);
- Workspace 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.

For enhancements CP-7(1), (2), and (3), FIPS 199 Moderate and High impact systems must select an alternate processing site that is physically separated from the primary site to ensure it is not susceptible to the same hazards as identified in the risk assessment. The alternate processing site must be reviewed to verify it provides the security measures required by the

system's FIPS 199 impact level, as well as to identify any site-specific problems that may need to be remediated to ensure successful recovery and operation of the information system.

For enhancement CP-7(4), FIPS 199 High impact systems must have an alternate processing facility that is configured to resume operations of the information system or its business/mission critical components.

***Additional Contractor System Considerations:*** *Vendor/contractor systems are required to comply with the control statements.*

## 4.7 CP-8 Telecommunications Services

**Control:** Establish alternate telecommunications services, including necessary agreements to permit the resumption of [*information system operations*] for essential mission and business functions within [*GSA SSO or Contractor recommended time period approved by the GSA CISO and AO*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

**Control Enhancements:**

(1) Telecommunications Services | Priority of Service Provisions.
   (a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and
   (b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

(2) Telecommunications Services | Single Points of Failure. Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

(3) Telecommunications Services | Separation of Primary and Alternate Providers. Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

(4) Telecommunications Services | Provider Contingency Plan.
   (a) Require primary and alternate telecommunications service providers to have contingency plans;
   (b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and
   (c) Obtain evidence of contingency testing and training by providers [*at least annually*].

**GSA Implementation Guidance:** Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

FIPS 199 Moderate and High impact systems must ensure any system disruption caused by a loss of telecommunications is mitigated by an alternate telecommunications service. Similar to

the implementation of alternate processing sites in the event of system failure, the establishment of alternate telecommunications services is important.

For enhancements CP-8(1) and (2), FIPS 199 Moderate and High impact systems must have priority of service provisions in place at the primary and alternate processing sites to ensure the availability requirements of the information system are met. In addition, if a common carrier is used for telecommunications services for national security emergency preparedness, there must be a service priority agreement in place.

For enhancements CP-8(3) and (4), FIPS 199 High impact systems must use an alternate telecommunications provider separate from the primary provider to ensure no single point of failure exists for the system. Alternate communications providers servicing FIPS 199 High impact systems must have contingency plans in place.

***Additional Contractor System Considerations:*** *Vendor/contractor systems are required to comply with the control statements.*

## 4.8 CP-9 System Backup

**Control:**

a. Conduct backups of user-level information contained in [*non-user issued components (e.g., laptops, desktops*] [*at a frequency that meets the system's recovery time and recovery point objectives per its BIA*];
b. Conduct backups of system-level information contained in the system [*at a frequency that meets the system's recovery time and recovery point objectives per its BIA*];
c. Conduct backups of system documentation, including security- and privacy-related documentation [*at a frequency that meets the system's recovery time and recovery point objectives per its BIA*]; and
d. Protect the confidentiality, integrity, and availability of backup information.

**Control Enhancements:**

(1) System Backup | Testing for Reliability and Integrity. Test backup information [*at least annually*] to verify media reliability and information integrity.
(2) System Backup | Test Restoration Using Sampling. Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.
(3) System Backup | Separate Storage for Critical Information. Store backup copies of [*critical software (e.g., operating systems, middleware, key management software) and inventory*] in a separate facility or in a fire rated container that is not collocated with the operational system.
(5) System Backup | Transfer to Alternate Storage Site. Transfer system backup information to the alternate storage site [*GSA SSO or Contractor recommended and GSA CISO and AO approved time period and transfer rate in accordance with the recovery time and recovery point objectives*].

(8) System Backup | Cryptographic Protection. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [*all backup data*].

**GSA Implementation Guidance:** Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

All systems must ensure backups are performed on user and system level information and all relevant system documentation, including security documentation. In addition, the backups must be secured at their storage location. NIST SP 800-34, Chapter 5 provides detailed guidance on selecting and implementing an effective backup strategy and implementing the appropriate data security to maintain the integrity of system data and software.

**Note:** Backup of Information on user-issued components (e.g., laptops, desktops) is the responsibility of the user, not a system.

GSA policy requires backups to be consistent with the system's SSPP, CP, or BIA such that backup frequency supports the system's recovery time and recovery point objectives for each of the information types identified in the control objectives. The protection of backup data in storage must be implemented in accordance with the NIST SP 800-53 requirements per FIPS 199 impact level. Typical protective mechanisms include the use of digital signatures and cryptographic hashes.

For enhancement CP-9(1), FIPS 199 Moderate and High impact systems must test their backup information at least annually. For enhancement CP-9(8), cryptographic mechanisms must be used to prevent unauthorized disclosure and modification of backup information. Such mechanisms must be FIPS validated.

For enhancements CP-9(2), (3), and (5), FIPS 199 High impact systems must use a sample of their backup information for restoration of selected system functions during contingency plan testing. Backup copies of the information system’s inventory and critical software components such as applications and operating systems software, must be maintained separate from the primary operating facility or stored in fire-rated container(s).

***Additional Contractor System Considerations:*** *Vendor/contractor systems are required to comply with the control statements.*

## 4.9 CP-10 System Recovery and Reconstitution

**Control:** Provide for the recovery and reconstitution of the system to a known state within [*the system's defined recovery time and recovery point objectives per its BIA*] after a disruption, compromise, or failure.

**Control Enhancements:**

(2) System Recovery and Reconstitution | Transaction Recovery. Implement transaction recovery for systems that are transaction-based.
(4) System Recovery and Reconstitution | Restore Within Time Period. Provide the capability to restore system components within [*GSA SSO or Contractor recommended and GSA CISO and AO approved time periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

**GSA Implementation Guidance:** Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

Recovered information systems must have all security related configuration settings required by FIPS 199 impact level and all security-critical patches verified or reinstalled prior to resumption of system operations.

For enhancement CP-10(2), FIPS 199 Moderate and High impact systems, all transaction-based systems, such as databases and transaction processing systems, must employ appropriate transaction recovery mechanisms.

For enhancement CP-10(4), FIPS 199 High impact systems must be capable of restoring system components to a known, operational state within an agreed upon timeframe meeting the system's specified recovery times. The restoration should be from secure, configuration controlled, and integrity-protected information. For example, restoring from a disk image to achieve a known state meets the requirement. If possible, restoring additional information and data to a last known operational state provides a better recovery and reconstitution capability.

***Additional Contractor System Considerations:*** *Vendor/contractor systems are required to comply with the control statements.*

## Appendix A: Contingency Planning Templates

The templates identified below are available on the GSA InSite IT Security Forms and Aids page and can be used to develop contingency planning documents and processes.

- Business Impact Analysis Template
- Contingency Plan Template for Low Impact System
- Contingency Plan Template for Moderate Impact System
- Contingency Plan Template for High Impact System
- Contingency Plan Test Plan Template
- Contingency Plan Test Report Template
- Contingency Plan Logistics Checklist Template

## Appendix B: Contingency Plan Sample Test Scenarios

Provided in the table below are examples of possible contingency plan test scenarios and potential expected outcomes.

| Example Contingency Test Scenario | Example Expected Outcome |
|---|---|
| System X maintained at Vendor Y is declared inoperable. The system must be restored at the alternate (Hot Site) facility where a sufficient communication network exists to support the system. Full back-up tapes from System X completed the night before are maintained at an offsite location (vault). Restore operations at the Alternate Facility (Hot Site) where the system can successfully be run on the recreated system. | ☐ Backup tapes can be recovered in a timely manner.<br>☐ System can be recovered successfully on an alternate platform from backup media. The alternate production site assumes all functions of the system.<br>☐ Telecommunications can be switched and reconfigured to the alternate production site.<br>☐ Vendor, agency, and recovery team are able to coordinate recovery actions between teams.<br>☐ The system is functional on the alternate equipment.<br>☐ Procedures for restoring to normal operations are effective.<br>☐ Notification procedures are effective. |
| System X experiences multiple component failures and is declared inoperable. Failures include:<br>☐ Power failure (as if, short circuit, malfunction, etc.)<br>☐ Hard drive/disk failure as a result of power surge/short circuit and/or malfunction<br><br>The following controls are in place:<br>☐ System Contingency Plan procedures for recovery action are established<br>☐ Redundant/ back-up power supply exist and available to maintain system operations<br>☐ Back-up Systems data is available and current<br>☐ Applications can be re-established on the System without losing operational status | ☐ System contacts, vendors, and recovery teams are able to coordinate recovery actions.<br>☐ Procedures to address system component failures are contained in the system contingency plan.<br>☐ Procedures for restoring to normal operations are effective.<br>☐ Notification procedures are effective.<br>☐ Redundant power supply is available, and system works as intended.<br>☐ System back-up/mirror image is current and available.<br>☐ System is recovered in the scheduled time window specified in the contingency plan. |
| System X maintains two sites that are replicas of one another. Only one is the production system. The production site is brought down for routine maintenance. The remaining site must assume all functions of the system. Telecommunications to the alternate are switched and/or reconfigured. | ☐ System recovery at the alternate site is successful. The alternate production site assumes all functions of the system.<br>☐ Coordination among recovery teams is effective.<br>☐ Procedures for migration to replicate site is effective.<br>☐ Notification procedures are effective.<br>☐ Telecommunications are switched to the alternate production site.<br>☐ Users continue to post transactions to the system.<br>☐ System application back-ups are routinely accomplished.<br>☐ System back-up/mirror image is current and available.<br>☐ Operational status of the system is maintained. |