



NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.08-01 v2024-02

Published: 2024-02-23

**Contingency Planning
TECHNICAL HANDBOOK**

TABLE OF CONTENTS

Document Properties	5
Document History Log	5
Approval	5
1. Introduction	6
1.1. Purpose	6
1.2. Scope	7
1.3. Point of Contact(s)	7
1.4. Applicability	7
1.5. Applicable Documents	7
1.5.1. Federal Information Processing Standards (FIPS)	7
1.5.2. National Institute of Standards and Technology (NIST)	7
1.5.3. Other Government Agencies	8
1.5.4. National Aeronautics and Space Administration (NASA)	8
1.5.5. Cancellations, Updates, Consolidations	8
2. Roles and Responsibilities Overview	8
2.1. In-Depth Roles and Responsibilities Description	8
2.1.1. Office of Protective Services (OPS)	8
2.1.2. Authorizing Official (AO)	8
2.1.3. Information System Owner (ISO)	8
2.1.4. Chief Information Officer (CIO)	9
2.1.5. Senior Agency Information Security Officer (SAISO)	9
2.1.6. Center Chief Information Security Officer (CISO)	9
2.1.7. Information System Security Officer (ISSO)	9
2.1.8. Contingency Planning (CP) Coordinator	9
2.1.9. Key Contingency Personnel	10
3. Security Controls and Corresponding Roles and Responsibilities	10
3.1. Contingency Plan (CP-2)	10
3.1.1. Authorizing Official (AO)	10
3.1.2. Information System Owner (ISO)	10
3.2. Contingency Training (CP-3)	10
3.2.1. Information System Owner (ISO)	10
3.3. Contingency Plan Testing (CP-4)	11
3.3.1. Information System Owner (ISO)	11
3.4. Alternate Storage Site (CP-6)	11
3.4.1. Information System Owner (ISO)	11
3.4.2. Information System Security Officer (ISSO)	11
3.5. Alternate Processing Site (CP-7)	12
3.5.1. Information System Owner (ISO)	12
3.5.2. Information System Security Officer (ISSO)	12
3.6. Telecommunications Services (CP-8)	12
3.6.1. Information System Owner (ISO)	12
3.7. System Backup (CP-9)	12
3.7.1. Information System Owner (ISO)	12
3.8. System Recovery and Reconstitution (CP-10)	13
3.8.1. Information System Owner (ISO)	13

3.9. Alternate Communications Protocols (CP-11)	13
3.10. Safe Mode (CP-12)	13
3.11. Alternative Security Mechanisms (CP-13)	13
4. Contingency Planning Guidance	13
4.1. Overview of Contingency Planning Steps	14
4.2. Risk Management	14
4.3. System Development Lifecycle	15
5. Contingency Planning Process	16
5.1. General	16
5.2. Develop Contingency Planning Policy	16
5.3. Conduct Business Impact Analysis (BIA)	17
5.3.1. BIA Guidelines	17
5.3.2. Determine Business Processes and Recovery Criticality	17
5.3.3. Identify Resource Requirements	18
5.3.4. Identify System Resource Recovery Priorities	18
5.4. Identify Preventative Controls	19
5.5. Create Contingency Strategies	19
5.5.1. Strategy Development/Selection	19
5.5.2. Backup and Recovery Methods and Offsite Storage	20
5.5.3. Alternate Sites	20
5.5.4. Equipment Replacement	21
5.5.5. Cost Considerations	22
5.5.6. Strategy Implementation	22
5.6. Develop Contingency Plan	23
5.6.1. Supporting Information	24
5.6.2. Activation and Notification Phase	26
5.6.3. Recovery Phase	27
5.6.4. Reconstitution Phase	30
5.6.5. Plan Appendices	31
5.7. Ensure Plan Testing, Training, and Exercises	32
5.8. Ensure Plan Maintenance	33
Appendix A: Acronyms	34
Appendix B: Definitions	35
Appendix C: BIA Data Collection Template	41
Appendix D: CP Template and Quality Control Checklist	41
D.1. CP Template	41
D.2. Quality Control Checklist	41
Appendix E: Test, Training, and Exercise (TT&E) Program Plan	41
E.1. Introduction	41
E.1.1. Purpose	42
E.1.2. Objectives	43
E.1.3. Applicability	43
E.2. TT&E Activities	43
E.2.1. Scope of Activities	43
E.2.2. Types of TT&E Activities	44
E.2.3. Recommended TT&E Schedule	47
E.2.4. TT&E Documentation and Maintenance	50

E.3. TT&E Development Process	51
E.3.1. Phase I: Planning Process	51
E.3.2. Phase II: Execution Process	52
E.3.3. Phase III: Evaluation Mechanisms	53

DOCUMENT PROPERTIES

Document History Log

Document Version	Published Date	Description
1.0	2011-05-06	Initial Draft
1.1	2012-04-26	Clarify Organizational value for CP-2. Updating to state “The NASA SOC Operations Manager (access the plan via NSAAR).”
1.2	2013-04-30	Extended for 1 year.
1.3	2014-04-24	Extended while revision 4 updates are rolled into the Handbook.
1.4	2014-12-01	Revised for Rev 4 controls, ODVs and updated TOC
1.5	2015-02-23	Revisions to 2.1.2.1 and Section 6
1.6	2017-02-14	Extended due to updates
1.7	2017-04-12	Updated to reflect new tools and maintain consistency with referenced documents/standards
1.8	2017-11-15	Updated to new template
1.9	2019-01-30	Consolidated with ITS-HBK 2810.08-02, <i>Contingency Planning: Guidance and Templates for Plan Development, Maintenance, and Test</i> and updated to new template. Updated content to meet current NIST SP 800-34 Rev. 1 standards, updated BIA data call template, CP template, and TT&E Program Plan.
2.0	2019-05-03	Updated with input from first round of reviews.
2.1	2021-09-30	Updated to account for SP 800-53 Rev. 5
2.2	2023-01-31	Annual update.
v2023-06	2023-06-16	Updated to new format
v2024-02	2024-02-23	Annual update

Approval

Associate Chief Information Officer for
Cybersecurity & Privacy

1. INTRODUCTION

NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance to determine the proper security categorization (Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization for Federal Information and Information Systems), and in the selection and implementation of information security controls ([FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*](#) and [NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*](#), in a manner consistent with the Risk Management Framework ([NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*](#)). [NPD 2810.1, *NASA Information Security Policy*](#), [NPR 2810.1, *Security of Information and Information Systems*](#), and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of [SP 800-53](#).

[NPR 2810.1](#) designates this Handbook as a guide for NASA's Contingency Planning information security controls (CP-controls) and for developing contingency plans (CP) for NASA information systems in accordance with [NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*](#).

This Handbook supports the implementation of requirements in [NPR 2810.1](#) and [NPD 2810.1](#). It also augments NIST guidance with NASA-specific requirements, procedures, and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance unless explicitly stated. The Agency's organizationally defined values are integrated into the control requirements within RSA ARCHER in the Risk Information Security Compliance System (RISCS) system.

The [SP 800-53](#) CP-control family relates to the preparation of information security response, recovery, and continuity activities to avoid disruptions to critical business processes. Successful contingency planning increases the likelihood that essential information and information systems will be available and assists an organization with maintaining continuity of operations in emergency situations. Effective contingency planning, training, testing, and execution are essential to mitigating the impacts resulting from system and service disruptions. The content of this document, in conjunction with [NPD/R 2810.1](#), defines NASA policy and procedures to address [CP-1](#).

1.1. Purpose

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.

The purpose of this Handbook is to provide a framework for consistent and effective CP practices and controls across the NASA organization. This Handbook provides ISOs with a guide for developing CPs and defines the process necessary to develop and maintain contingency capabilities and implement the requirements of [SP 800-34](#) and [NPR 2810.1](#). The development of viable CPs will mitigate the risk of system unavailability by providing effective and efficient solutions that facilitate a timely response to an information system disruption, provide effective and efficient solutions to enhance system availability, and enable quick and effective system recovery and reestablishment of normal operations. In an emergency, conditions may exist where personnel who are not in technical positions or who are new to technical positions must assume the duties of experienced technical personnel; therefore, CPs must have sufficient detail so recovery procedures can be carried out by any assigned personnel or team. CPs fit into a much broader emergency preparedness environment, which includes organizational and business process continuity and recovery planning.

As a fundamental aspect of the reestablishment of normal business operations, ISOs must ensure that critical information systems can resume normal functions within a reasonable timeframe; therefore, the contingency planning process is focused on minimizing the duration of a serious disruption, facilitating the effective coordination of recovery tasks, and reducing the complexity of the restoration effort.

1.2. Scope

This Handbook applies to all systems owned and/or operated by NASA, except for national security systems.

Although NASA Handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. However, pursuant to NPR 1400.1, portions of NASA Handbooks containing procedural or process guidance may be cited in contract, program, and other Agency documents, and may become requirements when a NASA directive specifies their use by citing the document title, revision letter/number, and date; or, when a NASA manager with authority over a NASA program, project, or other activity, identifies it as a requirement.

This Handbook and the procedural guidance contained within remains in full force and effect until such time that the Handbook is formally canceled, rescinded or superseded by an updated document.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the procedural guidance set forth in this Handbook to support such decision. The documented rationale/justification shall be provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this Handbook, in coordination with Center Information Security Officers (CISO), to review and validate for the record.

1.3. Point of Contact(s)

For any questions or comments regarding the contents of this Handbook, contact:

- CSPD Policy Group (hq-dl-cspd-policy@mail.nasa.gov)

1.4. Applicability

This Handbook is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory, a Federally Funded Research and Development Center, other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements

1.5. Applicable Documents

1.5.1. Federal Information Processing Standards (FIPS)

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

1.5.2. National Institute of Standards and Technology (NIST)

- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*

- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*

1.5.3. Other Government Agencies

- Federal Continuity Directive (FCD) 1, *Federal Executive Branch National Continuity Program and Requirements*

1.5.4. National Aeronautics and Space Administration (NASA)

- NPD 2810.1, *NASA Information Security Policy*
- NPR 1040.1, *NASA Continuity of Operations (COOP) Planning Procedural Requirements*
- NPR 1600.1, *NASA Security Program Procedural Requirements*
- NPR 2810.1, *Security of Information and Information Systems*
- ITS-HBK-2810.11-02, *Media Protection and Sanitization*

1.5.5. Cancellations, Updates, Consolidations

- ITS-HBK-2810.08-01, Contingency Planning
- ITS-HBK 2810.08-02, Contingency Planning: Guidance and Templates for Plan Development, Maintenance, and Test

2. ROLES AND RESPONSIBILITIES OVERVIEW

2.1. In-Depth Roles and Responsibilities Description

2.1.1. Office of Protective Services (OPS)

OPS is responsible for the physical and environmental security controls that protect the Agency information system assets. This responsibility includes facility security and access, Continuity of Operations (COOP) Plan requirements, and personnel security management.

2.1.2. Authorizing Official (AO)

The AO has the authority to formally assume responsibility for operating an information system at an acceptable level of risk to Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals. This includes contingency planning, including the CP, to meet an acceptable level of risk as part of the system accreditation and the decision for awarding an Authorization to Operate. The AO may appoint in writing a Contingency Plan (CP) Coordinator for specific individual or multiple systems for which they have AO responsibility and may be requested to assist in obtaining resources to develop, implement, maintain, and test/exercise contingency plans.

2.1.3. Information System Owner (ISO)

The Agency depends upon the ISO to fulfill the business requirements necessary to achieve their program area's mission. The ISOs are responsible for the successful operation of those systems and ultimately accountable for the security of their information systems. They are also responsible for executing crucial steps to implement appropriate and effective controls in protecting the information and information systems under their purview; this includes the development of current assessment, recovery, and restoration procedures in a CP that meet business requirements. The ISOs are responsible for ensuring that CPs are prepared and coordinated with other Agency offices/organizations; key contingency personnel receive the training required to fulfill their responsibilities; the CP is tested, evalu-

ated, and documented annually, and the CP is maintained in a ready state and updated when modifications are made to the system.

2.1.4. Chief Information Officer (CIO)

The Agency CIO has the ultimate responsibility to ensure that the Agency has appropriate, comprehensive, and tested contingency plans in place to continue fulfilling its mission. During a major disaster or disruption of service, the Agency CIO has the authority to activate the Agency Disaster Recovery Plan (DRP), as applicable, and initiate the activation of individual system CPs.

For Center information systems, this authority is delegated to the Center CIOs for the coordination of Center-wide contingency planning efforts.

2.1.5. Senior Agency Information Security Officer (SAISO)

The SAISO directs the management of the Agency's IT Security program and develops policies and procedures including contingency planning, and established recovery metrics and objectives for information systems. The SAISO interacts with internal and external resources, and coordinates security compliance (including CP testing requirements) across Agency Centers and other organizational elements. The SAISO and the Center Chief Information Security Officer (CISO) establish a strong foundation in providing oversight to all IT security activities, including contingency planning requirements.

2.1.6. Center Chief Information Security Officer (CISO)

The Center CISO issues IT security policy, procedures, and guidance for all Center information systems. The Center CISO is responsible for providing oversight to ensure Agency and Center policies are implemented. The Center CISO reviews and approves the processes, techniques, and methodologies planned for securing Center information system assets, including contingency planning and associated tests, training, and exercises activities.

2.1.7. Information System Security Officer (ISSO)

The Information System Security Officer (ISSO) is responsible for ensuring that management, operational, and technical controls for securing Program Office information systems are in place and are effective. The ISSO is the principal Point of Contact (POC) for information systems security and is responsible for ensuring an appropriate operational security posture is maintained for all assigned systems from inception until disposal, including contingency planning.

2.1.8. Contingency Planning (CP) Coordinator

The CP Coordinator is appointed in writing by the ISO or the Authorizing Official (AO) to coordinate and approve contingency planning activities for an individual system or multiple systems within the Program Office. The CP Coordinator may be the ISO. The ISO retains the responsibility to assure the accomplishment, quality, and implementation of the contingency planning and contingency planning activities.^[1] The CP Coordinator is responsible for carrying out duties as assigned by the ISO, which may include:

- Developing the strategy in cooperation with the functional and resource managers.
- Preparing the Business Impact Analysis (BIA);
- Developing the CP for the ISO in conjunction with senior managers within the Program Office, as well as other Agency offices and organizations;
- Coordinating training for individuals with key contingency roles;
- Testing, exercising, and maintaining the CP;

- Distributing the contingency plan to all relevant parties according to a list of authorized individuals/organizations; and
- Directing key contingency personnel or teams responsible for the information system(s) and coordinating their actions with other relevant Agency personnel or organizations when the contingency plan is executed.

2.1.9. Key Contingency Personnel

Key contingency personnel are responsible for the execution and implementation of activities as specified in the information system contingency plan.

3. SECURITY CONTROLS AND CORRESPONDING ROLES AND RESPONSIBILITIES

3.1. Contingency Plan (CP-2)

3.1.1. Authorizing Official (AO)

The AO reviews and approves proposed contingency plans as a part of the security authorization package.

3.1.2. Information System Owner (ISO)

The ISO:

- Develops and maintains a contingency plan for all information systems, as a part of the security authorization package, which includes the following:
 - Identification and continuation of mission essential and business functions and associated contingency requirements;
 - Recovery objectives, restoration priorities, and metrics;
 - Contingency roles, responsibilities, assigned individuals with contact information and activities associated with restoring the system;
 - Continuation of essential mission and business functions despite the information system disruption, compromise, or failure; and
 - A BIA for information systems under their purview in accordance with this Handbook, [SP 800-34](#), and [NPR 1040.1](#).
- Coordinates contingency planning activities with the Security Operations Center (SOC).
- Incorporates lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training.
- Ensure copies of the approved contingency plan are distributed when updates are made and in a manner that is consistent with organizationally defined values.

3.2. Contingency Training (CP-3)

3.2.1. Information System Owner (ISO)

The ISO:

- Ensures that all personnel involved in information system contingency planning efforts are identified and trained in the procedures and logistics of information system contingency planning and implementation, in compliance with this Handbook, [SP 800-34](#), and [SP 800-84](#).
- Reviews and updates contingency plan training content.
- Provides refresher training focusing on any changes implemented to the contingency plan.
- Maintains contingency planning training records.
- Documents refresher training completion in RISCs.

3.3. Contingency Plan Testing (CP-4)

3.3.1. Information System Owner (ISO)

The ISO:

- Conducts controlled tests and/or exercises to gauge the effectiveness of the CPs and training, and to identify and correct weaknesses, in compliance with this Handbook, [SP 800-34](#), and [SP 800-84](#).
 - Execution of contingency plan testing shall follow the schedule laid out in [Table 1, “Recommended Methods and Frequency of Occurrence for TT&E Activities”](#).
 - The Test type identified shall represent the minimum level of testing at the defined interval, but the ISO may impose additional testing as appropriate.
- Reviews the results of the contingency plan test/exercise, initiates corrective action, and updates the contingency plan to reflect changes.
- Documents completion of the annual contingency plan test/exercise in RISCs.

3.4. Alternate Storage Site (CP-6)

3.4.1. Information System Owner (ISO)

The ISO:

- Establishes an alternate storage site, if required.
- Includes necessary agreements, to permit storage and retrieval of information system backup information.
- Ensures the alternate storage site is separated from the primary storage site so as not to be susceptible to the same hazards.
- Ensures mitigation actions are outlined to address potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.
- Ensures the alternate storage site is fully configured to facilitate recovery operations in accordance with recovery time and recovery point objectives.

3.4.2. Information System Security Officer (ISSO)

The ISSO:

- Ensures the alternate storage site has information security measures equivalent to that of the primary storage site.

3.5. Alternate Processing Site (CP-7)

3.5.1. Information System Owner (ISO)

The ISO:

- Establishes an alternate processing site, if required.
- Includes necessary agreements, to permit resumption of information system essential mission and business functions within the timelines of the system recovery objectives when the primary processing capabilities are unavailable, in a manner consistent with organizationally defined values.
- Ensures the availability of equipment and supplies to support the resumption of operations within the time period required.
- Ensures the alternate processing site is separated from the primary processing site so as not to be susceptible to the same hazards.
- Ensures mitigation actions are outlined to address potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster.
- Ensures alternate processing site agreements are developed/established that contain priority-of-service provisions to meet the information system availability requirements.
- Ensures the alternate processing site is fully configured so that it is ready to use as an operational site supporting essential mission and business functions.

3.5.2. Information System Security Officer (ISSO)

The ISSO:

- Ensures the alternate processing site has information security measures equivalent to that of the primary site.

3.6. Telecommunications Services (CP-8)

3.6.1. Information System Owner (ISO)

The ISO:

- Establishes primary and alternate telecommunication service agreements that contain priority-of-service provisions in accordance with the information system availability requirements, and in a manner consistent with organizationally defined values.
- Requests priority of services for the primary and alternate telecommunications services provided by a common carrier that are used for national security emergency preparedness.
- Obtains alternate communications services with consideration for reducing the likelihood of sharing a single point of failure with the primary communication services.
- Obtains alternate telecommunication services that are geographically separated from the primary service provider to reduce susceptibility to the same hazards.
- Ensures service providers of primary and alternate telecommunication services have contingency plans.

3.7. System Backup (CP-9)

3.7.1. Information System Owner (ISO)

The ISO:

- Ensures backup of user-level and system-level information consistent with recovery time and recovery point objectives.
- Ensures backup of information system documentation, including security-related documentation.
- Ensures the security of system backup information at the storage site.
- Ensures backup information is tested to verify media reliability and information integrity.
- Maintains a record of the results from testing of the backup information in RISCs.
- Ensures backup copies of the operating system and other critical information systems inventory (including hardware, software, and firmware components) are stored in a separate facility or in a fire-rated container that is not collocated with the operational system.

3.8. System Recovery and Reconstitution (CP-10)

3.8.1. Information System Owner (ISO)

The ISO:

- Ensures that the recovery and reconstitution of the information system are to a known state after a disruption, compromise, or failure of the information system.
- Ensures transaction-based recovery is implemented for information systems that are transaction-based.^[2]
- Ensures compensating security controls are defined and provided for the following circumstances that may inhibit recovery to a known state:
 - failure of the system backup capability;
 - loss and/or corruption of backup files;
 - system information integrity has been compromised by unauthorized access or malware; and
 - a hardware component failure, (e.g., server or storage device).
- Ensures the capability to reimage information system components within the recovery time objectives of the system using configuration controlled and integrity protected disk images that represent a secure, operational state for the components.

3.9. Alternate Communications Protocols (CP-11)

This control is not required or applicable to NASA systems, therefore responsibilities are not assigned.

3.10. Safe Mode (CP-12)

This control is not required or applicable to NASA systems, therefore responsibilities are not assigned.

3.11. Alternative Security Mechanisms (CP-13)

This control is not required or applicable to NASA systems, therefore responsibilities are not assigned.

4. CONTINGENCY PLANNING GUIDANCE

4.1. Overview of Contingency Planning Steps

There are seven key steps in the Agency's comprehensive information system contingency planning process, which is aligned with [SP 800-34](#). Seven steps:

1. Develop Contingency Planning Policy to provide the authority and guidance necessary to develop an effective CP that includes the identification of existing requirements, associated plans, programs, and management support.
2. Conduct BIA to identify and prioritize information system critical business processes and resources.
3. Identify Preventive Controls implemented to reduce the effects of system disruptions (e.g., uninterruptible power supplies (UPS), gas-or diesel-powered generators, smoke detectors, fire suppressors, and water sensors).
4. Create Contingency Strategies to ensure quick and effective recovery following a disruption.
5. Develop Contingency Plan containing detailed guidance and procedures to recover and restore the system (e.g., backup tapes) to meet business requirements.
6. Ensure Plan Testing, Training, and Exercises to validate recovery capabilities, prepare recovery personnel, and identify planning gaps for continuous plan improvement and organizational preparedness.
7. Ensure Plan Maintenance to regularly review and update the plan, control plan distribution, and document plan changes. These planning process guidance steps are covered in more detail in Section 5 of this Handbook.

4.2. Risk Management

Risk management activities from the contingency planning perspective have two primary functions:

- First, risk management shall identify threats and vulnerabilities so appropriate controls can be put into place to either prevent incidents from happening or to limit the effects of an incident. These security controls protect an information system against three categories of threats:
 - Natural—hurricanes, tornados, floods, or fires.
 - Human—operator error, sabotage, malicious code implant, and terrorist attacks.
 - Environmental—equipment failure, software error, telecommunications network outage, and electric power failures.
- Second, risk management shall identify risks for which contingency plans must be put into place. The contingency plan, therefore, is closely tied to the results of the risk assessment and its mitigation process.

To effectively determine the specific risks to an information system during service interruption, a risk assessment of the information system environment is required.^[3] Since risks can vary over time and new risks may replace old ones as a system evolves, the risk management process must be ongoing and dynamic. The ISO must be aware of system risks and develop contingency plan strategies to address risks as completely and effectively as possible.

[FIPS 199](#) security impact categories are used in conjunction with vulnerability and threat information in assessing the risk to an organization. This categorization is based on the potential impact to an organization should certain events occur that jeopardize their information and information systems, which are needed to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. The system security impact category of Low, Moderate, or High determines the [SP 800-53](#) security controls that must be implemented for the information system, which includes contingency planning controls.

The contingency planning security controls determine the degree of rigor necessary to prepare the contingency plan; coordinate the plan with other Agency organizations; and determine the frequency of system backups, types of alternate sites selected, training type and frequency, testing type and frequency, and recovery procedure requirements. The risk assessment process facilitates the tailoring of security controls to address organizational needs and risk tol-

erance.

4.3. System Development Lifecycle

System Development Lifecycle (SDLC) refers to the full scope of activities conducted by ISOs associated with a system during its lifespan. The lifecycle begins with the project initiation phase and ends with the system disposal phase. Contingency measures shall be identified and integrated into all phases of the lifecycle—an approach that reduces overall contingency planning costs, enhances contingency capabilities, and reduces the impacts to system operations when the contingency plan is implemented. Contingency Planning considerations during the SDLC phases are as follows:

Initiation Phase

Contingency planning requirements shall be considered when a new information system is being conceived. In the initiation phase, system requirements are identified and matched to their operational processes. Business processes that the new information system will support are evaluated to determine initial contingency requirements, including policy, alternate storage, alternate processing, telecommunications, and backup. During this phase, the new information system shall be evaluated against all other existing and planned information systems to determine its appropriate recovery priority.

Development/Acquisition Phase

As initial concepts evolve into system development, specific contingency solutions may be determined. Contingency measures shall continue to reflect system and operational requirements. The design shall incorporate redundancy and robustness directly into the system architecture to optimize reliability, maintainability, and availability during the operations/maintenance phase. Recovery priorities are sequenced, and backup procedures and timeframes are also defined to meet business requirements. By including these in the initial design, costs, as well as problems associated with retrofitting or modifying the system during later phases, are reduced.

Implementation Phase

The contingency strategies are formally documented in the CP in coordination with security control assessments. While the system is undergoing initial testing, contingency strategies shall be exercised to ensure that recovery procedures are accurate and effective. Exercise results may prompt modification to the procedures in the CP.

Operation/Maintenance Phase

When the system is operational, users, administrators, and managers shall maintain a test, training, and exercise program that continually validates CP procedures and strategies. Exercises and tests are conducted to ensure the procedures remain effective. Regular backups shall be conducted, stored offsite, rotated, and periodically validated. The CP is 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 (e.g., changes to external interfaces), these modifications are reflected in the CP. Coordinating and documenting changes in the plan should be performed in a timely manner to maintain an effective plan.

Disposal Phase

Contingency considerations shall not be neglected because an information system is retired, and another system replaces it. As legacy systems are replaced, they may provide a valuable backup capability if a loss or failure of the new system occurs. In some cases, equipment parts (e.g., hard drives, power supplies, memory chips, or network cards) from hardware that has been replaced by new systems can be used as spare parts for new, operational equipment.^[4] In addition, legacy systems can be used as test systems for new applications, allowing potentially disruptive system flaws to be identified and corrected on non-operational systems. During a system's disposal phase, it may be necessary to develop and implement plans to maintain the availability of data and/or software stored on that system (for regulatory or other reasons). If the data is not incorporated into the replacement system, it may need to be transferred elsewhere and stored in an accessible format. During the disposal phase ensure that all information and information platforms are properly handled and/or disposed of.

5. CONTINGENCY PLANNING PROCESS

5.1. General

This section provides guidance on developing, testing, and maintaining information system CPs. Ultimately, the Agency, individual Program Offices, and ISOs will have a suite of plans to prepare proper response, recovery, and continuity activities for disruptions affecting Agency information systems, business processes, and facilities. Because there is an inherent relationship between an information system and the business processes it supports, there must be coordination between the development and updates of each plan to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts. These plans are described below.

- The Business Continuity Plan (BCP) focuses on sustaining an organization's business functions during and after a disruption (e.g., payroll process or consumer information process). A BCP may be written for business processes within a single Office or may address the entire Agency's processes. The BCP considers information systems in terms of their support to business processes, and must coordinate with ISOs to ensure that the BCP expectations and IS capabilities are matched. In some cases, the BCP may not address long-term recovery and return to normal operations, but solely cover interim business continuity requirements. To eliminate possible conflicts, the responsibilities and priorities set in the BCP must be coordinated with those responsible for COOP Planning Procedural Requirements ([NPR 1040.1](#)). Most Agency designated Mission Essential Infrastructure (MEI) systems will include a formal COOP. This coordination is particularly critical if the information system is a designated MEI or an integral element of a designated MEI.
- The COOP plan focuses on restoring an organization's mission essential functions at an alternate site and performing those functions for a minimum of 30 days or until normal operations are resumed. The COOP plan usually addresses Agency issues and is developed and executed independently from the BCP. Because the COOP plan emphasizes the recovery of an organization's operational capability at an alternate site, the plan does not necessarily include IT operations. In addition, the plan does not typically address minor disruptions that do not require relocation to an alternate site.
- The Disaster Recovery Plan (DRP) applies to major, usually physical disruptions that deny access to the primary facility infrastructure for an extended period. A DRP is an IS-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 CPs 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 MEFs at an alternate location. The DRP scope may overlap that of a CP; however, the DRP is narrower in scope, site-specific, and only addresses disruptions that require relocation of system operations to an alternate site.
- A CP provides established procedures for the assessment and recovery of an information system following a system disruption. The CP provides key information to assist with system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. The CP differs from a DRP primarily in that the CP procedures are developed for recovery of the system regardless of site or location. A CP can be activated at the system's current location or at an alternate site depending on the extent of the system disruption and resources available.

The following subsections describe the process to develop and maintain an effective CP. These steps represent key elements in a comprehensive CP capability, to collect and gather logically grouped system information, strategies, and procedures that will be used to populate the CP document.

5.2. Develop Contingency Planning Policy

The development and maintenance of the Agency contingency planning policy and guidance is the responsibility of the SAISO. The Agency's contingency planning policy was developed and is addressed in [NPR 2810.1](#), and identifies the objectives, regulatory requirements, and roles and responsibilities for contingency planning to meet security

control compliance commensurate with each system's [FIPS 199](#) security categorization. According to the policy, the ISOs have the responsibility for developing, testing, and maintaining CPs for the systems under their purview. This Handbook guides ISOs on how to implement the Agency contingency planning requirements defined in [NPR 2810.1](#). This guidance must be implemented in coordination with related Agency activities (e.g., physical security, human resources, incident response, system operations, and emergency preparedness functions). Contingency planning personnel must coordinate activities from each area to remain aware of new or evolving policies, programs, or capabilities. Contingency planning shall be integrated into all phases of the SDLC to ensure contingency planning requirements are developed and updated throughout the system's lifecycle.

5.3. Conduct Business Impact Analysis (BIA)

5.3.1. BIA Guidelines

The BIA is a key step in the contingency planning process that collects the information to fully characterize system components, business processes, and interdependencies to determine contingency requirements and priorities. The purpose of the BIA is to correlate the system components with the critical business processes (CBP) they provide and, based on that information, characterize the consequences of a disruption. Results from the BIA are incorporated into the analysis and strategy development efforts for the information system CP^[5] and will be included in the contingency plan as an appendix.

The BIA is initially conducted during the Initiation phase of the SDLC, and periodically reviewed and updated (e.g., during Development/Acquisition and Operations/Maintenance phases) to identify new contingency requirements and/or priorities and account for the appropriate level of risk. As new technologies become available, preventive measures may be enhanced and recovery strategies may be modified. The BIA is a critical tool that, when developed and updated throughout a system's lifecycle, guides and supports the development and maintenance of appropriate recovery strategies that will ensure system availability and meet the Agency's evolving business needs and requirements. The BIA template is in Appendix C.

5.3.2. Determine Business Processes and Recovery Criticality

The first step in the BIA is to identify and validate business processes performed by the system and any processes that depend on or support the system, evaluate the impacts of a system disruption on those business processes, and estimated downtime that reflects the maximum downtime the organization can tolerate while still maintaining the mission/business processes. This is a multi-step process that will identify the mission/business processes, identify the impact of a disruption to each business process across several impact categories, and determine the acceptable downtime if a specific process is unavailable.

This activity should be performed with internal and external POCs/stakeholders associated with the system. When identifying POCs/stakeholders, it is important to include organizations that provide or receive information from the system, as well as POCs supporting any interconnected systems. This coordination should enable the ISO to characterize the full range of support provided by, and capture the unique purpose of, the system.

Working with input from the POCs/stakeholders, identify the specific business processes that depend on or support the information system. This will ultimately characterize the full-range of operation and support provided by the system. Depending on system complexity, business processes may be mapped to one or more system modules.

Each identified business process is then evaluated and measured against several impact categories to determine the impact severity to the Division/Office/Agency if the process could not be performed. The outage impact evaluation shall incorporate any cascading effects that may occur, as a disrupted system affects other systems/processes that rely on it. The impact rating should consider the information types and the [FIPS 199](#) security categorization, as these could affect business process criticality.^[6]

To further evaluate the criticality of each business process, the ISO (in conjunction with POCs/stakeholders) must determine the acceptable downtime if a given process (or its data) were disrupted, based on the outage impacts to

the business and the Agency's mission. The analysis shall evaluate the downtime thresholds based on the effects of the outage over time and the impact to the mission, with respect to the outage impacts ratings, using the following factors:

Maximum Tolerable Downtime (MTD)

the total amount of time the AO/ISO is willing to accept for a business process outage before irreparable harm comes to the organization, and includes all impact considerations. Determining MTD is important for (1) the 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.^[7] Identify the effect of the outage on each business process over time, from the point of disruption to the time the outage impact ratings are realized.

Recovery Time Objective (RTO)

the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on supported business processes, other system resources, and the MTD. Determining the RTO is important for selecting appropriate technologies/strategies that are best suited for meeting the MTD. As the RTO must ensure that the MTD is not exceeded, the RTO must normally be shorter than the MTD. Any additional time to reprocess the data must be added to the RTO (but not part of the RTO) to stay within the time limit established by the MTD. For each business process, determine the target timeframe for the recovery of all of its supporting resources.

Recovery Point Objective (RPO)

represents the point in time, prior to a disruption or system outage, to which 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 measure of the data loss tolerance during the recovery process. Based on time, determine how much data that supports the business process that the Agency/Division can afford to lose; this will guide and determines the minimum frequency with which backups must be conducted.

It is also vital to develop an explanation of the rationale or justification for the timeframes selected, which may include mandates and legal parameters, workload, performance measures, etc. This information will be utilized to support the selection of potential recovery strategies, and should be utilized to determine the MTD, RTO, and RPO.

The ISO shall balance the cost of system inoperability against the cost of resources required for restoring the system and its overall support for critical business processes. 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. Plotting the cost balance points will show an optimal point between disruption and recovery costs.

5.3.3. Identify Resource Requirements

Realistic recovery efforts require a thorough identification and evaluation of the resources required to resume business processes as quickly as possible. Working with POCs/stakeholders, the ISO should ensure that the complete information system resources are identified. To avoid duplication of effort, this information may be obtained from the system component inventory and the system software inventory. Ensure each system module supported by each resource is identified to ensure that the business processes are mapped to the appropriate system resources.

Once all resources are identified, it is vital to identify a Recovery Time Capability (RTC) which identifies the time to actually recover each resource, taking into account any dependencies between resources. This is different from the RTO, which is linked to the recovery goals for supported business process. Used together, the RTO and RTC can identify operational gaps and guide the development of appropriate recovery strategies.

5.3.4. 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 business process criticality, outage impacts, tolerable downtime, and system resources.

This analysis usually will identify infrastructure requirements, such as electric power, telecommunication connections, and environmental controls. Specific equipment (e.g., routers, application servers, and authentication servers) is usually considered critical; however, the analysis may determine that certain components (e.g., printer or print server) are not needed to support critical services. The result is an information system recovery priority hierarchy, and will enable the ISO to develop and prioritize recovery strategies to meet the recovery priorities.

5.4. Identify Preventative Controls

The outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, 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. A wide variety of preventive controls are available, depending on system type and configuration. Some common measures include:

- Appropriately sized universal power supplies (UPS);
- Gasoline- or diesel-powered generators to provide long-term backup power;
- Air-conditioning systems with adequate excess capacity to prevent the 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.

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

5.5. Create Contingency Strategies

5.5.1. Strategy Development/Selection

Organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of business processes. The challenge for organizations is in implementing the right set of security controls. Contingency strategies are created to mitigate the risks for the contingency planning family of controls (per NIST [SP 800-53](#)) and cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance.

Contingency strategies shall address outage impacts and tolerable downtimes identified in the BIA. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level recovery plans. Contingency strategies shall be integrated into the system architecture during the design and implementation phases of the information system life cycle. The strategies should include a combination of methods that complement each other to provide recovery capability over the full spectrum of incidents.

The following subsections represent key activities in the CP Recovery Phase, which details a suggested course of

action for recovery teams to restore system operations at an alternate site or using contingency capabilities.

5.5.2. Backup and Recovery Methods and Offsite Storage

Backup and recovery 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, including the RPOs, and should be integrated into the system architecture during the Development/Acquisition phase of the SDLC.

When developing and comparing strategies to regularly back up data, several approaches should be considered, including cost, maximum downtimes, security, recovery priorities, and integration with larger, organization-level CPs. Backup frequency and scope of backups (e.g., daily or weekly, incremental or full) shall be based on Agency policy (refer to [SP 800-53](#) control [CP-9](#)), data criticality, and the frequency that new information is introduced. The location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite should be documented in the CP. The specific method chosen for conducting backups should be based on system and data availability and integrity requirements.

It is good business practice to store backed-up data offsite. 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. Offsite storage addresses [SP 800-53](#) control [CP-6](#). 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, activation fees, and disaster response/recovery services.

Backups and offsite storage processes and mitigations address [SP 800-53](#) controls [CP-6](#) and [CP-9](#).

5.5.3. Alternate Sites

Although major disruptions with long-term effects may be rare, they shall be documented in the CP, as required based on the [FIPS 199](#) security categorization. The plan must include a strategy to recover and perform system operations at an alternate site for an extended period to meet [SP 800-53](#) control [CP-7](#). The alternate site must be able to support system operations as defined in the CP, including considerations given to business impacts and downtime defined in the BIA. The three alternate site types may be categorized in terms of their operational readiness, in addition to two hybrid variations that may combine features from the three baseline site types. Sites may be identified as cold, warm, hot, mobile, or mirrored. Progressing from basic to advanced, the five types of sites are described as follows:

Cold Sites

typically consist of a facility with adequate space and infrastructure (e.g., electric power, telecommunications connections, and environmental controls) to support the information system recovery activities. The site does not contain equipment and usually does not contain office automation equipment (e.g., telephones, facsimile machines, or copiers). The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities.

Warm Sites

partially equipped office spaces that contain some or all system hardware, software, telecommunications, and power sources. The warm site is maintained in an operational status ready to receive the relocated system, but may not be loaded with the current data. The site may need preparation before receiving the system and recovery personnel. In many cases, a warm site may serve as a normal, operational facility for another system or function, and in the event of contingency plan activation, the normal activities are displaced temporarily to accommodate the disrupted system.

Hot Sites

facilities appropriately sized to support system requirements and configured with necessary system hardware, supporting infrastructure, and support personnel. 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 are typically staffed 24 hours a day, 7 days a week. Hot site personnel begin preparations for system arrival as soon as they are notified that the contingency plan has been activated.

Mobile Sites

self-contained, transportable shells that are custom-fitted with specific telecommunications and information system equipment necessary to meet system requirements. The facility is often contained in a tractor-trailer and may be driven to and set up at the desired alternate location. In most cases, to be a viable recovery solution, mobile sites shall be designed in advance with the vendor and a Service Level Agreement (SLA) must be signed between the two parties.

Mirrored Sites

fully redundant facilities with automated, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data is processed and stored at the primary and alternate site simultaneously.

There are obvious cost and ready-time differences among the five options. 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 the necessary equipment. Partially equipped sites (e.g., warm sites) fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours. The selection of fixed site locations should account for the time and mode of transportation necessary to move personnel and/or equipment to the site. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event as the organization's primary site. As the sites are evaluated, the ISO shall ensure that the system's security controls are compatible with the prospective site. Such controls may include firewalls and physical access controls, and personnel security requirements of the staff supporting the site.

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 (including alternate telecommunications, per [SP 800-53](#) control [CP-8](#)), 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. An MOU or an SLA for an alternate site should be developed based on the organization's needs and the partner organization's capabilities. Consideration should also be given to system interconnections and possible interconnection security agreements (ISAs).

5.5.4. Equipment Replacement

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

described as follows:

Vendor Agreements

as the contingency plan is being developed, SLAs for 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's 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 (i.e., warm or mobile site) or at another location where it will be stored and then shipped to the alternate site. This solution has certain drawbacks since the 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 Office/Division within the Agency. 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 ISO should consider that purchasing equipment when needed is cost-effective, but can add significant overhead time to the recovery process while waiting for shipment and setup. Conversely, storing unused equipment is costly, but allows recovery operations to begin sooner. Based on the impacts discovered through the risk management process and BIA, consideration should be given to the possibility of a widespread disaster requiring 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 CP.

5.5.5. Cost Considerations

The ISOs must ensure that the strategy chosen can be implemented effectively with the 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 ISO shall determine known contingency planning expenses (e.g., alternate site contract fees) and those less obvious (e.g., cost of implementing an agency-wide contingency awareness program and contractor support). The budget must be sufficient to encompass software, hardware, travel, 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 Program Office shall perform a Cost Benefit Analysis (CBA) to identify the optimum recovery strategy.

5.5.6. Strategy Implementation

Having selected the system recovery strategy, the ISO must designate appropriate personnel or teams to implement the system recovery strategy. Each individual shall 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 who will respond to the event, recover capabilities, and return the system to normal operations. To accomplish this, recovery team members need to clearly understand the team's goal in the recovery effort, individual procedures the team will execute, and how their team relates to other teams.

Personnel should be chosen to staff these teams based on their skills and knowledge. Ideally, teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. Team members

must not only understand the contingency plan's purpose, but also need to know the procedures necessary to execute 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 ISO should also consider that a disruption could render some personnel unavailable to respond. In this situation, executing the plan may only be possible 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 and 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 is unavailable.

For most systems, a leadership team is necessary for providing overall guidance following a major system disruption or emergency. The leadership team is responsible for activating the contingency plan and supervising the execution of contingency operations. The leadership team also facilitates communications among other teams and supervises CP tests and exercises. Some or all of the leadership team may manage specialized recovery teams. One or more members of the leadership team have the authority to activate the plan and to make decisions regarding spending levels, acceptable risk, and interagency coordination.

5.6. Develop Contingency Plan

Documenting information in the contingency plan is a critical step in the process of implementing a comprehensive Contingency Planning Program. The plan shall contain detailed roles and responsibilities and procedures associated with restoring the information system following a disruption. The contingency plan documents the technical capabilities designed to support contingency operations and is tailored to the organization and its requirements.

Contingency plans should be formatted to provide clear and concise directions in the event that personnel not familiar with the plan or the systems are called upon to perform recovery operations. Plans should be comprehensive and easy to implement in an emergency. Where possible, checklists and step-by-step procedures should be used. A simple and well-formatted plan reduces the likelihood of unnecessary complexity and confusion at the time of implementation. There are five main components of the contingency plan:

Supporting Information

This includes introductory information providing essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain. This information assists in making decision on how to use the plan and provides information on where associated plans and information outside the scope of the plan may be found. It also includes additional details about the information system, including architecture, interconnections, teams, and other relevant system information.

Activation and Notification Phase

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

Recovery Phase

This phase documents the activities that take place after the plan has been activated, outage assessments completed (if possible), personnel notified, and teams mobilized. It focuses 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.

Reconstitution Phase

This phase defines the actions taken to test and validate system capability and functionality. Recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can be applied to preparing a new permanent location to support information system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan.

Plan Appendices

Contingency plan appendices provide key details not contained in the main body of the plan. The main body typically contains high-level information for the above four plan components, while the appendices make up the majority of the plan and include significant, specific details for the four plan components. These details enable CP execution, including keystroke-level recovery procedures, detailed contact information, service level agreements. Appendix information is collected typically in conjunction with the above phases, but also contains additional information to support contingency operations.

The following subsections utilize a methodology to collect the BIA information and contingency strategies previously identified, and gather additional, logically organized information across the five main CP components that will be used to populate the CP. The CP template is provided in Appendix D, and outlines the recommended layout for high-level information and detailed appendices.

5.6.1. Supporting Information

CP supporting information describes the purpose of a CP and lays the initial foundation on the location of information contained in the plan. Supporting information may address one or more [SP 800-53](#) CP-controls. Each of the key plan areas that comprise the supporting information section is outlined below and range from system information to information about the plan itself

5.6.1.1. Change History

The change history section provides a history of updates to the CP, typically capturing the date, version, and modifications made to the previous version. This may track drafts or final approved versions, as required by Agency policy. The change history also provides evidence to support regular (e.g., annual) plan reviews and updates, meeting compliance requirements defined in Agency policy.

5.6.1.2. Plan Approval

CPs must be approved and signed by the designated authorities outlined in the Agency contingency planning policy. Approvers attest that the plan addresses the system criticality, contains current information to maintain critical functions, has been tested/exercised, and is complete.

5.6.1.3. Introductory Information

The introduction section orients the reader to the type of information contained in the plan and is mostly boilerplate text with some system-specific information. This section includes the following subsections:

Background

This subsection establishes the reason for developing the CP and defines the plan objectives.

Scope

The scope identifies the [FIPS 199](#) impact level and associated RTOs. It also contains a mapping of the [SP 800-53](#) CP controls to the relevant sections of the CP, providing a means of reference for documenting security control elements, as required by the system's security categorization.

Assumptions

This section includes the list of assumptions that were used in developing the CP as well as a list of constraints/situations that are not applicable.

References/Requirements

This section outlines both the Federal and Agency policies and guidelines that the CP is compliant with.

5.6.1.4. Concept of Operations/System Information

The concept of operations provides an overview of the system, its architecture, and other information about its implementation. Many of the concept of operations information is not typically developed specifically for the CP, but are elements developed during the SDLC phases or for other security documentation; this information may be leveraged for use in the CP. The following system information is typically included in the CP:

BIA

The BIA was previously completed as part of the CP process and is included as an appendix. As the foundation for the development of the contingency strategies, this is a vital component of the CP.

System Description

This is a general description of the system, including each module, and its purpose in support of the organization's mission/business processes. It is typically a narrative format based on the business processes outlined in the BIA.

System Environment

This is a technical description of the system architecture, operating environment, physical location(s), general information about system users, and partnerships with external organizations/systems.

System Diagrams

Diagrams provide a visual representation of the system environment, and may include system architecture, input/output, and/or other technical or logical diagrams that may be useful in recovering the system. System diagrams are typically included in an appendix.

System Inventory

Inventory information should include specific hardware and software information with the system boundary, as well as alternate or replacement equipment used in contingency operations. System inventory may have been collected as part of the Equipment Replacement step in the CP process and is typically included in an appendix.

Dependencies and Interconnections

This section includes information on other systems that directly interconnect or exchange information with the system, including type of connection, information transferred/shared, and point of contact for that system. Some of this information may have been identified during the BIA, and is formally outlined in this section. These interconnections are typically included in an appendix.

Associated Plans

Related documentation that supports the system, including other interconnecting or support systems, business continuity plans, or other key supporting documentation outside the system boundary. These are plans that may be executed in parallel with or directly support the CP. Associated plans are typically included in an appendix.

5.6.1.5. Roles and Responsibilities

The roles and responsibilities section presents the overall structure of contingency teams, and was previously completed as part of the CP process. Many of these roles and individuals were also identified as POCs/Stakeholders during the BIA process. The CP organizes the roles and responsibility information in three areas:

Leadership Roles

Typically included in the main body of the document, each key leadership role is identified, and their responsibilities are defined. Leadership roles are specific to contingency planning and provide overall guidance following a major system disruption or emergency, provide communications, and supervise the execution of contingency operations. Specific CP roles include the CP Coordinator appointed by the ISO or AO, and a CP Director with overall management responsibility for the contingency plan and directs its implementation to meet relevant IT security and contingency planning policies.

Contingency Teams

Typically included in the main body of the document, each key team is identified, and their responsibilities are defined. Teams are responsible for the execution and implementation of CP activities, including responding to the event, recovering capabilities, and returning the system to normal operations. Specific vendor support, incident response, or teams responsible for interconnected systems may also be included.

Personnel Roster

Typically contained in an appendix, this section identifies the specific individuals assigned to each leadership role and contingency team, their work location, and at least two pieces of contact information to avoid a single point of failure. The personnel roster also serves as a formal listing of key personnel that should receive a copy of the CP, per [SP 800-53](#) control requirements.

CP Organizational Chart

Typically provided in an appendix, the organizational chart provides a graphical depiction of the overall structure of contingency teams, including the hierarchy and coordination among the teams.

Vendors

Typically provided in an appendix, key third part support vendors that provide emergency or contingency support should be identified, including the type of support and contact information. Contract and other service level agreement (SLA) information may also be collected for inclusion in the appropriate SLA appendix.

5.6.2. 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 activate the CP, notify recovery personnel, and conduct an outage assessment. At the completion of the Activation and Notification Phase, CP staff will be prepared to perform recovery measures. This phase consists of three main focus areas whose activities may be sequential or conducted in parallel. They are outlined in the following subsections.

5.6.2.1. Activation Criteria

Activation criteria are the conditions that must be met for the designated authorities to activate the CP. These include the RTOs identified during the BIA (and evaluated during outage assessment), plus other criteria specific to the Agency, Center, or Office, including COOP and business continuity criteria. It is important to identify any criteria that will trigger CP activation as utilized by leadership; criteria may be in the form of a decision tree or a basic listing.

In addition, all designated roles with authority to activate the CP should be identified, including the CP Coordinator, CP Director, or other designee.

5.6.2.2. Notification Procedures

As outages or disruption may occur with or without prior notice, 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. Upon plan activation or following the outage, notification should be sent to the appropriate roles/teams so that the status of the situation (e.g., outage assessment) and next steps may be determined.

Notification procedures should outline who makes the initial notifications, the sequence in which personnel are notified (e.g., system owner, technical POC, CP Coordinator, business unit POC, or recovery team POC), and the method of notification (e.g., email blast, call tree, automated notification system, etc.). Procedures should follow a logical sequence based on the system's unique communication procedures, including ticket routing, contacting vendors, or mobilizing recovery teams for outage assessment and response. Notifications should be coordinated with incident response, POCs of external organizations, or interconnected system partners, as required. The notification strategy should also define procedures to be followed in the event that specific personnel cannot be contacted. The notification process may follow the organizational chart or a similar call tree, and should account for business and non-business hours, as appropriate.

5.6.2.3. Outage Assessment

To determine how the CP 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. Personnel with outage assessment responsibilities should understand and 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.

High-level outage assessment procedures may be included in the main body of the CP, with specific details and/or outage assessment report template contained in an appendix. 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.

5.6.3. Recovery Phase

Formal recovery operations begin at the conclusion of the Activation and Notification Phase: after the CP 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 should be functional and capable of performing the functions identified in the plan.

This phase incorporates the contingency strategy information developed during previous steps in the CP process, along with the development of specific detailed procedures to restore business and system processing. It builds upon information derived from the BIA, Backup Strategies, Alternate Sites, and implementation of the contingency strategies.

5.6.3.1. Sequence of Recovery Activities

When recovering a complex system involving multiple independent and/or interrelated 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. A high-level sequence of recovery activities with outline the order of operations, including the selection of the appropriate recovery strategy and location, failover of the most crit-

ical modules/components, retrieval of backup data, and modules/components restoration priority. This sequence of recovery activities serves as the baseline for all subsequent recovery sections.

It should be noted that this listing of activities is not the list of procedures followed to execute those activities. Those procedures are developed in other sections.

5.6.3.2. Recovery Procedures

To facilitate Recovery Phase operations, the CP should provide detailed procedures to restore the information system or components to a known state. 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.

A high-level summary of the various recovery procedures in the main body of the CP is useful in understanding what must occur from a narrative and layperson perspective, and should also indicate the roles/teams that perform the procedures. The detailed, step-by-step keystroke-level procedures should be included in the appendices. 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. Detailed procedures may include:

- Keystroke-level recovery steps/standard operating procedures (SOP);
- Obtaining and installing necessary hardware components;
- Obtaining and loading backup media;
- Restoring critical operating system and application software;
- Required configuration settings or changes;
- Restoring system data to a known state;
- Failover/transfer of processing to the APS (and failback to original/primary site)
- Connecting system to network or other external systems; and
- Other system recovery procedures, as appropriate.

Procedures may be divided and segmented by activity, module, component, or team as desired by the CP Coordinator and recovery personnel, and in a manner that enables recovery in accordance with the BIA and sequence of recovery activities.

5.6.3.3. Data Backup Details

Backup strategies are a means to restore system operations quickly and effectively following a service disruption. This strategies may have been completed as part of the Backup and Recovery step in the CP process. The data backup strategies are typically documented in an appendix, and outline each type of backup, frequency/schedule, backup procedures, backup utility/method, and includes considerations to address control [CP-9](#), which sets requirements to conduct backups of user-level information, system-level information, and system documentation (including security-related documentation).

This section may also include procedures to restore data as part of recovery, if it is not included in the detailed recovery procedures appendix.

5.6.3.4. Alternate Storage Site

This appendix contains the information for offsite storage, as determined during earlier steps in the CP process to identify the alternate location to store backup data. Detailed information about the alternate storage site should pro-

vide personnel with enough information to obtain and retrieve backup data during a contingency event. Information includes offsite storage location, storage site POC, data stored offsite, the delivery and rotation schedule, retrieval procedures, and other information to meet [CP-6](#) security control requirements.

5.6.3.5. Alternate Processing Site

This appendix contains the information for the alternate processing site, as determined during earlier steps in the CP process. Detailed information about the alternate processing site should provide personnel with enough information to obtain and retrieve backup data during a contingency event. Information includes site location, type of site, alternate site POC, system modules supported, any key information on using the site, and other information to meet [CP-7](#) security control requirements.

As more than one alternate processing site may be identified, it is important to clearly indicate which system modules are supported by which site.

5.6.3.6. Alternate Telecommunications

Telecommunications services (data and voice) are required by [SP 800-53](#) control [CP-8](#) to permit the resumption of prioritized operations and timeframes defined in the BIA when primary telecommunications capabilities are unavailable at either the primary site, APS, or alternate storage sites. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential missions/business functions despite the loss of primary telecommunications services. Information for this section include the vendor/provider, points of contact, the bandwidth/throughput or other capacity provided by the vendor, SLAs, and other support information as required.

For many systems, this control is inherited from an infrastructure system (LAN or WAN), however it is important to indicate this inheritance. This information should be consistent with the Dependencies and Interconnecting Systems appendix.

5.6.3.7. Alternate/Manual Processing Procedures

Alternate manual or technical processing procedures may be utilized by users 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. This information is typically included in an appendix, and should indicate what business processes/modules are being performed, by whom, and include the relevant SOPs to perform the processes.

5.6.3.8. Service Level Agreements (SLA)

SLAs, memorandums of understanding (MOU), interconnection service agreements (ISA), or other contracts with third parties/vendors should be identified and included in an appendix. Vendor SLAs, reciprocal agreements with other organizations, and other essential records ensure that the system receives the appropriate priority support that guarantee the desired network availability, priority of service at an alternate processing site, replacement equipment delivery, or other contractual requirements that support the resumption of business processes.

This information may have been gathered during previous steps in the CP process, but it is beneficial to consolidate the SLA listing into one appendix, identifying basic information such as contract number, contact information for document custodian, level of support provided, and timeframe. If desired, a copy of each SLA can be included in the plan.

5.6.3.9. 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. During the Recovery Phase, 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.

These procedures are typically included in the main body of the document.

5.6.4. Reconstitution Phase

The Reconstitution Phase is the third and final phase of CP 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.

5.6.4.1. Concurrent Processing

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. Although not required for information systems per [SP 800-53](#), 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. This information may be included in the main body at a high-level, with detailed procedures in an appendix.

5.6.4.2. Validation Testing

During validation, the system is tested and validated as operational prior to returning operation to its normal state and typically comprises data validation and functionality validation. 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. Functionality testing is a process for verifying that all system functionality has been tested, ensuring the migration of systems, interfaces, and data has been correctly restored and verified, and the system is ready to return to normal operations.

Data validation and functionality validation information may be included as a summary of activities in the main body of the document. Detailed validation test procedures should be included in an appendix. Test procedures typically include a list of procedures and expected results, which are compared against the actual results to validate successful recovery.

5.6.4.3. Recovery Declaration

At the successful completion of the validation testing, CP personnel will be prepared to declare that recovery efforts are complete and that the system is operating normally. This declaration is made by an appropriate designated authority, and includes the deactivation of any interim processes. The plan deactivation process then begins.^[8]

5.6.4.4. Notifications

Upon return to normal operations, users should be notified by a designated role using predefined notification procedures. These procedures and the notification method are typically included in the main body of the plan.

5.6.4.5. 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. Specific cleanup procedures are typically included in the main body of the document.

5.6.4.6. Offsite Data Storage

It is important that all backup and installation media used during recovery be returned to the offsite data storage location. Procedures should be documented for returning retrieved backup or installation media to its offsite data storage location. This information is typically including as a high-level summary in the main body of the document, identifying any exceptions to the standard offsite storage delivery schedule.

5.6.4.7. 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. Procedures should be documented for conducting the next backup, and is typically including as a high-level summary in the main body of the document. If the backup is conducted outside of the normal backup schedule, this and other exceptions should also be documented, but may be referenced in the appropriate data backup appendix.

5.6.4.8. 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 CP, and a report template is typically included in an appendix.

5.6.4.9. Deactivation

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

5.6.5. Plan Appendices

Plan appendices make up the majority of the plan and include significant, specific details that enable CP execution, including keystroke-level recovery procedures, detailed contact information, service level agreements. Appendices may include the following as individual or grouped subsections, and contain the details necessary to execute contingency operations:

- Personnel and Vendor Contact Information
- Vendor Contact List
- Detailed Recovery Procedures
- Validation Test Plans
- Alternate Storage Site
- Alternate Processing Site
- Alternate Telecommunications
- Alternate Processing Procedures
- Backup Details
- Outage Assessment Report
- After Action Report
- System Inventory
- Dependencies and Interconnections

- Associated Plans
- System Diagrams
- Service Level Agreements (SLA)
- Business Impact Analysis
- TT&E Schedule

5.7. Ensure Plan Testing, Training, and Exercises

A CP 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 CP. In addition, the effectiveness of the information system controls should be assessed by using the procedures documented in [SP 800-53](#). [SP 800-84](#) 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 CP 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 their roles in the conduct of each information system plan. TT&E event schedules are often dictated in part by organizational requirements. For each TT&E event conducted, results are documented in an after-action report, and Lessons Learned corrective actions are captured for updating information in the CP.

CP 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.

To derive the most value from the test, the ISO shall 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 shall include a schedule detailing the timeframes 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 that is most likely to occur, and mimic reality as closely as possible.

Training for personnel with CP responsibilities should focus on familiarizing them with CP 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. Personnel newly appointed to CP roles should receive training shortly after assignment, and all personnel training should be provided annually thereafter. Ultimately, CP personnel should be trained to the extent that they can execute their respective recovery roles and responsibilities without aid of the actual CP 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.

There are two types of exercises widely used in information system TT&E programs by single organizations:

Tabletop exercises

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

exercises that 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 Agency's security policy states that testing for all systems shall be done annually (fiscal year).^[9] The contingency plan testing should be done at approximately the same time each year but completed no later than July 31st. If major changes have been made to the system, the contingency plan shall be updated, distributed, and tested prior to implementation.

Participants in the exercises and tests should include key personnel identified in the contingency plan, operational personnel, recovery and restoration personnel and the ISO.

For more information, including a baseline schedule of TT&E activities, refer to the TT&E Program Plan in Appendix E.

5.8. Ensure Plan Maintenance

To be effective, the CP must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operations/Maintenance phase of the SDLC, information systems undergo frequent changes due to shift of business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the contingency plan be reviewed and updated regularly as part of the organization's change management process to ensure that new information is documented and contingency measures revised, if required. [NPR 2810.1](#) requires ISOs to review the contingency plans for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists. Based on the system type and criticality, it may be necessary to evaluate contingency plan content and procedures more frequently. At a minimum, plan reviews should focus on the following elements:

- Operational requirements;
- Security requirements;
- Technical procedures;
- Hardware, software, and other equipment (e.g., 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 (e.g., electronic and hardcopy).

Because the CP contains 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. Additionally, a copy shall also be stored at the alternate site and with the backup media to ensure its availability and good condition in the event local plan copies cannot be accessed. Other information that should be stored with the contingency plan includes contracts with vendors (e.g., 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 ISO, who should communicate changes to the representatives of associated plans or programs, as necessary. The ISO should record plan modifications using a record of changes, and distribute plan updates to all relevant parties.

The ISO 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 CP. The ISO also should evaluate supporting information to ensure that the information is current and continues to meet system requirements adequately.

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.

APPENDIX A: ACRONYMS

AO	Authorizing Official
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BRP	Business Recovery-Resumption Plan
CBA	Cost Benefit Analysis
CIO	Chief Information Officer
COOP	Continuity of Operations
CP	Contingency Plan
DRP	Disaster Recovery Plan
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
HBK	Handbook
HSPD	Homeland Security Presidential Directive
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITS	Information Technology Security
MEI	Mission Essential Infrastructure

MTD	Maximum Tolerable Downtime
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OMB	Office of Management and Budget
OPS	Office of Protective Services
POC	Point of Contact
RISCS	Risk Information Security Compliance System
RTC	Recovery Time Capability
RTO	Recovery Time Objective
SAISO	Senior Agency Information Security Official
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SOC	Security Operations Center
SOP	Standard Operating Procedures
SP	Special Publication
SSP	System Security Plan
TT&E	Test, Training, and Exercise
UPS	Uninterruptible Power Supply

APPENDIX B: DEFINITIONS

Alternate Processing Procedures

Procedures that can be initiated in lieu of the system to maintain business operations during an outage.

Alternate Processing Site (APS)

A location, other than the systems primary location, used to continue operational capabilities during a significant system disruption.

Availability

Ensuring timely and reliable access to and use of information, [44 U.S.C., SEC. 3542].

A loss of availability is the disruption of access to or use of information or an information system.

Backup

A copy of files and programs made to facilitate recovery.

Business Continuity

Is a collection of strategies and specialized pre-conceived plans ensuring a local site can continue to manage efficiently and operate optimally in response to an impending/actual incident without significant impact to client services.

Business Continuity Plan (BCP)

The documentation of a predetermined set of instructions and 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, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. [[SP 800-34](#)]

Chief Information Security Officer (CISO)

NASA Center Senior Information Security Officer responsible for assisting the Center CIO in implementing this directive, NASA information security policies and procedures, and the Federal information security laws, directives, policies, standards, and guidelines and compliance with the FISMA section 3541 et seq..

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information, [44 U.S.C., Sec. 3542].

A loss of confidentiality is the unauthorized disclosure of information. [[FIPS 199](#)]

Contingency Plan

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 disaster. Contingency plans assist managers to ensure that data owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.

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 a minimum of 30 days as a result of a disaster event before returning to normal operations. [FCD 1, Adapted; [SP 800-34](#), Adapted]

Cost Benefit Analysis (CBA)

When considering security, cost-benefit analysis is done through risk assessment, which examines the assets, threats, and vulnerabilities of the system in order to determine the most appropriate, cost-effective safeguards (that comply with applicable laws, policy, standards, and the functional needs of the system). Appropriate safeguards are normally those whose anticipated benefits outweigh their costs. Benefits and costs include monetary and non-monetary issues such as prevented losses, maintaining an organization's reputation, decreased user friendliness, or increased system administration.

Critical Business Process (CBP)

The operational and/or business support functions that could not be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing the organization.

Data

A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means.

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 an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Failover

The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

Functional Exercise

An exercise that allows personnel to validate their operational readiness for emergencies 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 CP.

Hardware

The mechanical, magnetic, electrical, and electronic devices or components of an information system.

High-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a [FIPS 199](#) potential impact value of high. [[FIPS 200](#)]

Impact

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.

Information

An instance of an information type. [[FIPS 199](#)]

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]

Information System (Also referred to as IT System)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., Sec. 3502]

An information system will consist of automated data processing system hardware, operating system and application software, peripheral devices, and associated data communications equipment.



Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.) [NIST]

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.

Information System Owner (ISO) (or Program Manager)

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

nance of an information system. (NIST; CNSS 4009, Adapted)

Information System Security Official (ISSO)

Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. [CNSS Inst. 4009, Adapted]

Information Technology

Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product. IT Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract.



For additional guidance/clarification on meaning or scope of IT, please refer to the definition for “Information System” which is a “discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.”

Information Type

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation. [FIPS 199]

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]

A loss of integrity is the unauthorized modification or destruction of information. [FIPS 199]

IS Contingency Plan (CP)

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.

Low-Impact System

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a [FIPS 199](#) potential impact value of low. [FIPS 200]

Maximum Tolerable Downtime (MTD)

The MTD represents the total amount of time leaders/managers are willing to accept for a business process outage or disruption and includes all impact considerations.

Mission Essential Infrastructure (MEI)

Critical infrastructures, physical, Cyber-based systems, or a combination, whose diminished capabilities would significantly impact the Federal Government’s ability to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and to deliver minimum essential public services; and the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. (Reference Presidential Decision Directive (PDD) 63, May 22, 1998.)

Moderate-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a [FIPS 199](#) potential impact value of moderate and no security objective is assigned a [FIPS 199](#) potential impact value of high. [[FIPS 200](#)]

NASA Information

Any knowledge that that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for, or is under the control of NASA. [NPD 2810.1]

Operating System (OS)

An organized collection of techniques, procedures, programs, or routines for operating an information system, usually supplied by the system hardware vendor.

Potential Impact

The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect ([FIPS 199](#) low); (ii) a serious adverse effect ([FIPS 199](#) moderate); or (iii) a severe or catastrophic adverse effect ([FIPS 199](#) high) on organizational operations, organizational assets, or individuals. [[FIPS 199](#)]

Recovery Point Objective (RPO)

The point in time to which data must be recovered after an outage. RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that may need to be recreated after the system or functions have been recovered.

Recovery Time Objective (RTO)

The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported 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.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [[FIPS 200](#), Adapted]

Risk Analysis

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

Risk Assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.

Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Security

Security is a system property. Security is much more than a set of functions and mechanisms. Information technology security is a system characteristic as well as a set of mechanisms, which span the system both logically and physically.

Security Category

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operation, organizational assets, individuals, other organizations, and the Nation. [FIPS 199]

Security Objectives

Confidentiality, integrity, or availability. [FIPS 199].

Security Requirements

Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted. [FIPS 200]

Senior Agency Information Security Officer (SAISO)

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544]

Synonymous with Chief Information Security Officer (CISO)

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.

System Security Plan

Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. [NIST]

Tabletop Exercise

A discussion-based exercise 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 scenario.

Test

An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in a CP.

Test Plan

A document that outlines the specific steps that will be performed for a particular test, including the required logistical items and expected outcome or response for each step.

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [CNSS Inst. 4009, Adapted]

User

A person who accesses information systems to use programs or applications in order to perform an organizational task.

APPENDIX C: BIA DATA COLLECTION TEMPLATE

The attached BIA Data Collection Template may be utilized for all NASA information systems. If this template is utilized, it may be attached to the CP in the appropriate appendix, or the information may be entered directly into the CP in sections provided.

[CP_BIA_Template_20190130.xlsx](#)

APPENDIX D: CP TEMPLATE AND QUALITY CONTROL CHECKLIST

D.1. CP Template

The attached CP Template shall be utilized for all NASA information systems and uploaded to RISCS upon signature.

[Contingency_Plan_Template_20190130.docx](#)

D.2. Quality Control Checklist

The attached quality control (QC) checklist may be utilized to review the CP for content and compliance with [SP 800-34](#).

[ISCP_QC_Checklist_Template_20190130.xlsx](#)

APPENDIX E: TEST, TRAINING, AND EXERCISE (TT&E) PROGRAM PLAN

E.1. Introduction

The Test, Training, and Exercise (TT&E) Program Plan will ensure NASA's CPs are exercised annually, contingency personnel are trained in their respective roles and responsibilities, and critical systems are tested regularly.

This program plan is a recommendation based on industry standards and best practices for consideration in the implementation and long-term sustainment of NASA CPs and in support of the Divisions, Offices, the NASA Agency, and their missions.

Training ensures that contingency personnel are knowledgeable on the continuity roles and responsibilities described within their respective CPs. Tests and exercises validate, or identify for subsequent correction, specific aspects of the plan, including plan activation and notification, decision making, leadership succession, communications, recovery and reconstitution. In addition, tests and exercises verify the availability of essential records and documents and ensure that an alternate processing site (APS) is in a constant state of readiness, as applicable. When appropriate, results of a corrective action plan or after-action hot wash will be incorporated into the TT&E program after exercises and/or real-time emergencies.

The TT&E Program Plan includes information on the following:

- CP orientation for new employees (conducted within 30 days of assignment or as needed)
- CP refresher training for identified contingency personnel (conducted annually), which addresses alerting/notification procedures, CP plan activation, primary processing site (PPS) and APS activities, recovery, reconstitution, and other key CP issues
- Testing of CP alert, notification, and activation procedures (conducted quarterly)
- Testing of plans for the recovery of critical information systems, services, and data (conducted semiannually)
- Testing of CP communications capabilities (conducted quarterly)
- Testing of primary and backup infrastructure systems and services at the PPS and APS (conducted annually)
- Tabletop exercises for senior and/or technical staff (conducted annually)
- Relocation exercise (if necessary via the respective CP and/or local business continuity procedures), including a real-time emergency simulation and a mock deployment to the alternate operating facility (conducted annually)
- Interagency CP plan exercises (conducted annually)
- Development of a comprehensive corrective action program (CAP) to enable identification of weaknesses in plans and procedures and to make recommendations for CP plan revisions. This incorporates after action reports from exercises, after action reports from real-time events, feedback from training sessions, and on-going plan review and updates required by Federal guidance for continuity programs.

E.1.1. Purpose

The goal of the TT&E Program Plan is to ensure, as a baseline of preparedness, NASA information systems have in place a viable CP capability to ensure the performance of each system's critical business processes (CBP) during any emergency that disrupts normal operations. This TT&E plan is intended to assist CP leadership in determining if its contingency-related plans, policies, procedures, systems, and facilities are meeting expectations and requirements. It also serves as a supporting plan to any local/Center business continuity/COOP TT&E Program Plans.

This plan is developed in accordance with the following guidance, policy and standards:

- Executive Order 12656, Assignment of Emergency Preparedness Responsibilities
- Homeland Security Evaluation and Exercise Program (HSEEP)
- National Security Presidential Directive-51 Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20), National Continuity Policy
- National Continuity Policy Implementation Plan (NCPIP)
- Federal Continuity Directive (FCD) 1, Federal Executive Branch National Continuity Program and Requirements
- FCD 2, Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations
- NASA IT Security Handbook (ITS-HBK- 2810.08-01A)

This TT&E plan ensures overall viability of each system's CP procedures as well as organizational capability to respond to emergency incidents through validating the following CP elements on a regular basis:

- Alert/Notification Procedures * Access to essential records/databases/systems
- System recovery * Execution of identified CBPs
- Internal and external connectivity * System performance using alternate equipment
- Reporting and communication capabilities (i.e., telework locations, other alternate operating sites) * Reconstitution/Restoration of normal operations
- Redundant processing site operations * Related plan testing (i.e., Continuity of Operations (COOP), BCP)

Performing TT&E activities at regular intervals throughout the year ensures personnel awareness and ability to perform each system's CBPs during continuity conditions. Training and exercises provide contingency personnel opportunities to enhance their familiarity with respective continuity roles and responsibilities, ensures viable procedures to transition operability to an APS (as applicable) within the timeframe required, and that the APS is capable of supporting CP requirements. Regular system and application tests ensure the functionality and accessibility of critical equipment and interoperable communications as well as validates the currency of data/back-up data.

E.1.2. Objectives

The TT&E program plan is intended to assist contingency personnel effectively manage and execute respective CP tasks. The plan incorporates the three functional areas of:

- Testing systems and equipment;
- Training personnel; and
- Exercising CP procedures.

Specific objectives of the TT&E Program Plan are to:

- Validate CP policies and procedures;
- Ensure all identified contingency personnel are sufficiently trained to execute minimum essential operations and functions;
- Ensure that backup data and essential records required for supporting identified CBPs at an APS are sufficient, complete, and current;
- Test and validate equipment essential to CP operations to ensure both internal and external interoperability; and
- Ensure that all contingency personnel understand the procedures to phase down CP operations and transition to normal activities when appropriate.

Achieving the objectives of continuity readiness is possible only if training is conducted on a regular basis and each event builds on preceding ones (i.e., the number and types of TT&E events increase over time, as does the degree of complexity). The underlying assumption of the TT&E plan is that the capabilities and knowledge of contingency personnel will increase as they cycle through a formal TT&E program.

E.1.3. Applicability

This TT&E Program Plan applies to all roles identified under ITS-HBK- 2810.08-01A Section 2.1 and as defined in each system's CP.

E.2. TT&E Activities

E.2.1. Scope of Activities

An effective TT&E Program Plan prepares contingency personnel to perform cohesively and efficiently under condi-

tions they would encounter in an actual disruption to normal operations. Additionally, exercises reinforce and test the results of other TT&E activities. The CP TT&E Program Plan aligns with NASA security control testing requirements and COOP/BCP TT&E activities, and are designed under three major classifications —

Internal, within an individual system's CP TT&E Activities

CP TT&E activities that are considered Internal TT&E activities are planned, organized, executed, and evaluated by the ISO or designee. These events support testing and validation of CP procedures and capabilities to ensure the ability of CP personnel to perform its CBPs. Internal TT&E activities also include awareness training for NASA non-contingency personnel to ensure the availability and capability to provide supplement support.

Joint Internal, NASA Office, system Hosting location(s), and supporting NASA Centers/Missions

Exercises and events that support the testing and exercising of CP procedures in coordination with its parent Office and other NASA Centers/Missions in the implementation of other NASA continuity/contingency plans, or with support of other NASA locations.

Joint External, NASA system with Stakeholder or National-Level COOP/BCP TT&E Activities

Exercises and events that support the testing and exercising of the CP procedures in coordination with participation from non-NASA individuals or organizations or as a participant with the COOP/BCP community are considered Joint External TT&E activities. Joint External events are conducted with stakeholders and with National-Level COOP community participation.

- NASA system, parent Office, NASA Center(s), and Stakeholders. Such activities may include non-NASA individuals and organizations whose participation is necessary for full COOP implementation (e.g., Department of Homeland Security/local vendors).
- National-Level Exercises. Exercises developed and conducted for the benefit of the COOP community as a whole (joint Federal Department/Agency COOP TT&E activities), and exercises developed by entities outside of the COOP community (National-level exercises) in which the COOP community is one of several participants. NASA system and NASA Center participation in these activities will vary based on National-level or Department invitation.

E.2.2. Types of TT&E Activities

The TT&E Program Plan is a deliberate blending of hands-on training, computer based training, seminars, briefings, tests, and exercises. The method of presentation and the media used are selected based on the objectives of the event, topic (e.g., concept, procedure, and skill), and the intended audience. Many of the TT&E activities, such as training, are conducted on a consistent, recurring schedule, some of which may dovetail or coincide with security authorizations, COOP/BCP TT&E activities, or other local TT&E activities. Some recurrent activities are designed for newly assigned CP personnel, or to provide refresher training for existing CP personnel to ensure they are aware of current procedures or technologies. The content for all TT&E activities is updated as new information becomes available, as new policies or procedures are developed, or as technology changes. Functional and full-scale exercises are conducted on a less frequent basis and provide opportunities to push the limits of the TT&E program to ensure that continuity elements are viable when operating under more complex conditions.

E.2.2.1. Tests

Tests are conducted to demonstrate the effective operation of equipment, systems, and applications that support CP CBPs. Tests are based on procedures and processes identified in the system's CP. Tests validate or identify for subsequent correction, specific aspects of the CP, policies, procedures, systems, and facilities used in response to a continuity/contingency event. CP Testing activities are specific to the operability of technical systems and procedures, as well as communications equipment and networks, alert systems, information and processing systems, and operational and logistics capabilities of the alternate processing facility. Periodic testing ensures equipment and operating procedures are maintained in a constant state of readiness. Tests also provide CP personnel an opportunity to familiarize themselves with the equipment. The TT&E Program plan recommends tests (i.e., alert notification

drills) to be conducted on a quarterly or bi-annual basis, based on industry best practices.

Tests conducted during the initial stages of the TT&E Program are designed to isolate individual systems or equipment and ensure proper operation. As the TT&E Program evolves, systems and equipment may be tested to validate interoperability of supporting or complimentary systems and equipment.

Alert and Notification Drills

Alert and notification drills are internal CP exercises conducted to ensure the facility and/or system notification process is understood and contact information is up to date. Drills may include updating contact information, practicing the notification process using manual phone trees or other automated systems. Drills and updates should capture contact information and calling strategies for work and non-work hours. The time required to contact personnel and the percent of personnel successfully contacted should be recorded for future reference. Drills may be conducted with or without notice. These drills can also be coordinated with other interconnected systems, or local Center exercise plans.

Communication Testing

Communication testing validates the functionality of technical equipment utilized in CP situations. A communication test may include, but is not limited to, use and interoperability evaluations of cell phones, BlackBerry devices, satellite phones, fax connectivity, or secure phone connectivity. Communication tests may be conducted between CP personnel, primary site (hosting Center), other NASA Centers, and telework sites that will transmit communications during an event.

Information Technology Testing

IT testing may occur internally at the primary site or in conjunction with the APS and/or other NASA Centers. IT testing validates functionality of the IT system components and accuracy of individual recovery procedures at the primary site and the APS.

E.2.2.2. Training

CP Training and/or training on other related plans (i.e., HQ BCP, local BCP, Business Emergency Action Plans [BEAP], Occupant Emergency Plans [OEP]) includes briefings, web-based training, and informational documents (e.g., pamphlets) used to educate contingency personnel and non-contingency personnel about general CP concepts, and to raise awareness about general emergency preparedness. CP training is made up of awareness training, orientation training, and refresher training. Training events are internal activities.

A debriefing or “hot wash” conducted after each training event allows participants to recommend areas for improvement and TT&E program enhancement, as well as contingency planning or operations that may require clarification or refinement.

Awareness Training

Awareness training provides high-level information to continuity and non-contingency personnel about the information system CP and supporting NASA Office continuity/contingency planning. Briefing topics may include the CP concept of operations (i.e., implementation levels and operational phases), roles and responsibilities, and an overview of CBPs. Awareness training does not include how personnel should conduct their day-to-day operations. Awareness training can be executed via online courses or may be provided via instructor-led briefings or workshops.

Orientation/Refresher Training

Orientation training is designed for personnel recently assigned contingency personnel-related duties and as annual refresher training for existing contingency personnel. Orientation training provides introductory information on CP concept of operations, APS information and capabilities, roles and responsibilities, and system information as it relates to the identified CBPs. Orientation training can be offered in briefing and web-based formats.

APS Orientation Training

Each APS should provide a site orientation training to address support services available at the facility, including all available contingency communications and information technology systems/automated data processing. The training should also include administrative matters, such as supervision, security, support, and personnel policies. APS orientation training should be made available by site support personnel at the onset of a CP activation. APS orientation training may be provided through various formats including but not limited to a briefing, handout, online training, or video presentation. This APS orientation training may be included as part of orientation/refresher training sessions, however if future redundant processing sites or other relocation sites are identified for a particular system, this should be executed as a separate training specific to that site.

Succession Training

Annual succession training ensures that persons designated in the Line of Succession understand the authorities that may be delegated to them and the procedures for assuming and relinquishing authority. Designated successors should also receive training to familiarize themselves with the specific system components identified in the system's Business Impact Analysis (BIA) and required for making key policy decisions.

E.2.2.3. Exercises

Exercises measure the combined effectiveness of systems tests and contingency personnel training. Exercises provide an opportunity to practice CP implementation procedures and address issues associated with performing identified CBPs based on plausible scenarios. Exercises validate capabilities, identify deficiencies or shortfalls, verify availability and usability of contingency resources, and help ensure that the APS, if applicable, remains at a constant state of readiness. As the TT&E activities are planned, exercises are designed to build upon continuity objectives already tested and exercised to further expand the participants' knowledge and familiarity with the CP. These activities simulate different aspects of an emergency and can be designed to provide advance notice to participants or may be conducted without prior notice.

At the conclusion of each exercise (tabletop and/or functional), participants are to join a hot wash discussion, during which issues, concerns, and lessons learned are captured and documented. The hot wash elicits feedback from all exercise players, observers, and facilitators to identify "what went well" and "what needs improvement." The exercise developers aggregate observations and compare them against the exercise objectives to develop the After Action Report, including recommendations to address weaknesses or areas for improvement in plans and procedures.

Tabletop Exercises

Tabletop exercises are discussion-based events ideal for developing, training, and validating operational procedures, processes, issues, relationships, and functions in a no-fault environment. Tabletop exercises use a scenario to introduce a fictitious disruption of operations prompting a CP activation. Exercise participants use this opportunity to validate existing system procedures and identify areas for improvement. The success of the tabletop exercise is determined by group participation. Participant discussion is encouraged to solve or clarify a problem. Tabletop exercises are always no-fault exercises, therefore, the facilitator provides additional information or advises that further research may need to be conducted to solve the issue, but does not announce personal errors.

Following a tabletop exercise, participants should better understand their CP roles and responsibilities, understand interdependencies among organization units and the system(s) they are responsible for, and identify areas for improvement that need to be addressed before the next training, exercise, or actual real-time event. A typical Tabletop exercise design includes a facilitated meeting between a select group of individuals who have decision-making authority and/or technical staff with system responsibilities to discuss a specific emergency scenario, an identified system problem, or discuss system procedures.

Functional Exercises

Functional exercises are scenario-driven activities that provide an opportunity for participants to test their readiness in implementing the CP in a simulated operational environment. These exercises can vary in complexity and scope, from implementing specific aspects of the CP to a full-scale exercise that addresses all plan elements.

Functional exercises are designed to explore specific team member roles, procedures, and assets involved with a functional aspect of a plan (e.g., communications, emergency notifications, or system components) and include actual use of communications equipment and/or total system failover to an APS. These activities simulate different aspects of an emergency and can be designed to provide advance notice to participants or conducted without prior notice.

Full-Scale Exercises

Full-scale exercises are a complex form of a functional exercise and often are conducted in participation with Joint Department/Agency and National-level exercises. Full-scale exercising of COOP plans/BCPs should be accomplished whenever applicable and feasible. NASA participation in National-level full-scale events is by invitation from NASA HQ or the Department/Agency hosting the exercise. The full-scale exercise is an interactive activity used to evaluate the operational capabilities of emergency management systems over an extended period of time. This form of functional exercise involves testing a major portion of approved relocation facility elements and organizations in a realistic, highly stressful environment. Actual mobilization and movement of personnel and resources are required to demonstrate coordination, response, and continuity capability. Normally a designated relocation site or APS is activated and field command posts may be established. The participants actively "play out" their roles in a dynamic environment that provides the highest degree of realism possible for the simulated event. The full-scale exercise is the largest and most complex of TT&E activities and may involve participation at the Federal, regional, State, and local levels. Generally, full-scale exercises will be planned at the National or Departmental levels.

E.2.3. Recommended TT&E Schedule

The following table summarizes the recommended methods and frequency of occurrence for each of the TT&E activities to address Contingency Plan (CP)-control activities. TT&E Methods may be conducted independently or concurrently to meet stated objectives.

Table 1. Recommended Methods and Frequency of Occurrence for TT&E Activities

TT&E Method	Description	Activity Example	Frequency	FIPS 199 Availability	Participants
Orientation Training (CP-3)	Familiarize CP contingency personnel with CP concepts and general system operations.	Provide an instructor-led briefing to familiarizes CP personnel with the overall CP purpose, phases, activities, and provide in-depth instruction on roles and responsibilities. Under-score importance of personal preparedness.	Annually or within 30 days of assignment	Low Impact = Yes Mod. Impact = Yes High Impact = Yes	Internal

TT&E Method	Description	Activity Example	Frequency	FIPS 199 Avail- ability	Participants
Awareness Training (CP-3)	Provide CP contingency personnel and non-CP continuity personnel with topical information to enhance their knowledge of local BCP and the information system CP.	Provide an instructor-led briefing or online training that familiarizes all staff with the overall CP purpose, phases, and activities. Under-score importance of personal preparedness.	As needed	Low Impact = Yes Mod. Impact = Yes High Impact = Yes	Internal
Succession Training (CP-3)	Ensure that persons designated in the Line of Succession understand the authorities that may be delegated to them and the procedures for assuming and relinquishing authority. Provide an instructor-led briefing or online training to individuals identified in the CP Line of Succession. Review role and responsibilities and walk-through example scenarios where a change in the line of succession would occur.	This training could be coupled with an exercise or other CP team training.	Annual	Low Impact = Yes Mod. Impact = Yes High Impact = Yes	Internal
Alert and Notification Drills (CP-4)	Ensure personnel with alert and notification responsibilities are familiar with the process and are able to execute their responsibilities during business and non-business hours.	Initiate a call-down of CP personnel using call-trees, email alerts, and/or an automated system. Track response rate to ensure staff accountability.	Monthly to Quarterly	Low Impact = Yes Mod. Impact = Yes High Impact = Yes	Internal or Joint Internal

TT&E Method	Description	Activity Example	Frequency	FIPS 199 Availability	Participants
Tabletop Exercises (CP-4)	Facilitated, scenario-based discussions that provide CP personnel the opportunity to discuss their roles and responsibilities and identify inter-relationships in an unthreatening environment.	Provide facilitated briefing to CP leadership and technical CP personnel. Provide scenario questions to prompt exercise participant discussions about appropriate contingency responses.	Annual to Semi-annual	Low Impact = Yes Mod. Impact = Yes High Impact = Yes	Internal, Joint Internal, or Joint External
Communications and IT System Testing (CP-4)	Ensure communication tools and CP essential information systems operate effectively and users of these systems are familiar with the system processes from any operating location (i.e., telework site, other office location). Evaluate the ability to access essential records, systems, and equipment, including classified or sensitive information, from the APS. IT testing also serves to evaluate the currency and security of information systems.	Can be executed via a quarterly meeting between CP personnel and APS. Select one or more system(s) to be tested. Discuss outage assessment, test sequence of recovery activities, concurrent processing, and fail-over activities at APS.	Quarterly	Low Impact = Yes Mod. Impact = Yes High Impact = Yes	Internal or Joint Internal
Functional Exercises (CP-4)	Hands-on exercises that take place in real-time and covers all CP implementation phases.	Simulate a disruption with a system recovery component.	Annually	Mod. Impact = Yes High Impact = Yes	Internal, Joint Internal, or Joint External

TT&E Method	Description	Activity Example	Frequency	FIPS 199 Availability	Participants
APS Recovery Test or Exercise (CP-4, CP-7, CP-10)	Evaluate the services and infrastructure systems of the CP APS. Determine critical points of contact between primary site and APS, and evaluate APS capabilities to support contingency operations to include a full recovery and return to normal operations.	Provide scenario to prompt CP technical teams to initiate failover and recovery procedures in coordination with APS.	Annual	Mod. Impact = Yes High Impact = Yes	Joint Internal
Full-Scale Functional Exercises (CP-4, CP-10)	Intricately planned functional exercises requiring participation of multiple Departments/ Agencies, and may include non-government organizations (e.g., the American Red Cross). Such National-level exercises may span multiple days or longer periods.	Develop a simulation that prompts a full recovery and reconstitution of the information systems	Annually, or as invited	High Impact = Yes	Joint External
System Backup Test (CP-9)	Ensure system back-up process is functioning properly	Test back-up information and ensure that backup copies are stored in a separate facility.	Quarterly	Mod. Impact = Yes High Impact = Yes	Internal or Joint Internal

E.2.4. TT&E Documentation and Maintenance

TT&E documentation is maintained by the ISO (or designee) and stored in RISCs. Documentation is used as a record of the event and a resource for identifying event participants, tracking event activities, supporting event reviews and audits, and supporting future planning activities. All documentation should be maintained and available for audit submission if requested. Documentation should be maintained at the PPS and at the APS.

Documentation for each TT&E event should include, as appropriate, the following:

- Records of each TT&E activity executed;

- A sign-in sheet recording all participating CP contingency personnel, observers, and facilitators;
- Test/exercise plans (i.e., documentation of the objective, scope, participants, scenario, and implementer messages); and
- After Action Reports.

E.3. TT&E Development Process

The TT&E activity development process-based cycle consists of three distinct phases: Planning, Execution, and Evaluation. Feedback occurs throughout all phases to ensure that activities planned for the TT&E Program Plan are dynamic and reflects the needs of the system's CP. Within each phase, certain sequential steps occur. The ISO (or designee) manages the overall CP TT&E process. Other NASA CP personnel will assist in the development of scenarios and encourage stakeholder participation, as directed. The phases of the CP TT&E Process are depicted below:

E.3.1. Phase I: Planning Process

The first step in the development cycle is “planning,” which is performed for each TT&E activity. The same planning process is used to develop all types of TT&E events. This step consists of a thorough review of the purpose, materials, and format of each activity to identify any flaws, integrate lessons learned from previous exercises, and incorporate other necessary modifications. The planning process also requires the ISO (or designee) to:

- Determine the purpose and objectives
- Identify the target audience
- Research the topic
- Develop a plan for the event
- Manage administrative and logistical issues (selecting a date and location, scheduling guest speakers when applicable, identifying and procuring needed equipment)
- Write/create necessary materials (detailed agenda, briefings, handouts, slides, guides, handbooks, talking points, evaluation plans, participant questionnaires, etc.).

The planning step usually involves several coordination and planning meetings. The ISO (or designee) reviews the plan, makes changes as necessary, and finalizes the TT&E activity plan. Lastly, materials are developed, participants are registered, and activities are conducted.

TT&E materials may vary considerably from one event to the next, although an agenda and participant roster are required at all TT&E events. Because exercises involve detailed activity planning, additional specific types of materials are required to support tabletop, functional, and full-scale exercises effectively. In addition, the exercise planning process may require a longer period of time, particularly for joint internal or external exercises.

Scenarios are used in exercise design to frame a set of simulated events which trigger an emergency incident to which participants must respond. The scenario is integrated into the facilitator and participant guides, as appropriate. It may also be included in a briefing overview of the exercise. In order to develop an effective scenario, the TT&E planner must have a thorough understanding of the exercise objectives and build a scenario that will assist in achieving those objectives. The scenario must have an obvious impact that will prompt participants to engage in response activities designed to meet exercise objectives. The TT&E planner should consider the nature of participants (i.e., senior managers, technical staff, etc.) and craft scenarios appropriate to elicit their interest. Topical issues such as recent current events commonly generate participant interest and should be considered when developing scenarios.

Implementers are detailed exercise inputs that are injected into exercise play to cause players to engage in specific response activities. Implementers should be realistic inputs that are injected at a planned time and directed toward a

specific individual/position. Exercise controllers are responsible for putting the implementer into play and should do so in the same manner as would occur during real-life operations (i.e., phone, e-mail, face-to-face meetings, etc.). The implementers should be designed to isolate and validate exercise objectives. When designing implementers, the TT&E planner should know what actions players are expected to take in response to each inject. Each implementer introduced during the course of an exercise will therefore lead participants to achieve the desired objectives of the exercise. As implementers are developed, they are generally maintained in a Master Scenario Events List (MSEL) which provides a timetable of when the implementer is to be given, by whom, to whom, and using what specific type of communication method (e.g., phone or e-mail).

Materials that may be required for TT&E activities are identified in the table below:

	Agenda	Sign-in Sheet	Facilitator Guide	Participant Guide	Briefing	Handouts	Scenario	Implementers
Training	✓	✓	✓		✓	✓		
Tests	✓	✓			✓	✓	✓	
Tabletop Exercises	✓	✓	✓	✓	✓	✓	✓	✓
Functional/Full-Scale Exercises	✓	✓	✓	✓			✓	✓

E.3.2. Phase II: Execution Process

TT&E events are conducted according to the developed and approved plans. The ISO (or designee) usually facilitates the activity and may be assisted by the CP Coordinator (or other personnel as assigned). Trained data collectors and/or observers are also responsible for recording comments and observations (their own and those of the participants) and compiling these into After Action Reports. Facilitators, data collectors, and observers may be Federal government or contractor personnel.

The number and type of individuals involved in most TT&E activities depends on the nature of the event. Conduct of tabletop, functional, and full-scale exercises involve specially trained and directed groups, including:

Players

Players are required for all types of CP tests and exercises. The role of the player is to participate in the event as one's position would require during an actual emergency situation. Players are expected to be aware of the CP and procedures surrounding exercise activities.

Controllers

Controllers are needed for functional exercises, during which controllers are responsible for injecting implementer messages into play. Implementer messages are designed to prompt exercise play required to achieve exercise objectives. Towards this end, controllers remain in contact with data collectors during exercise play, and may modify, add, or delete scripted implementers from the MSEL as needed in order to achieve the event's objectives. However, controllers generally sit separated from the players so as not to disrupt the realism of the event.

Response Cell Staff

During a functional exercise, response cell staff will simulate the roles of outside personnel/organizations who are not participating in exercise play. For example, a staff member in the response cell may be required to respond to participant inquiries or direction by simulating the role of a NASA stakeholder or other NASA regional office representative. A response cell may only be necessary in full-scale exercises in which there is the potential for participants to simulate contact with numerous outside personnel/organizations. Controllers may be appropriate to

simulate outside entities for smaller, less complex functional exercises.

Observers

Observers participate in all types of CP TT&E activities as either data collectors or note takers.

- **Data Collectors.** Data collection staff may be required for all types of tests and exercises, particularly those activities that are of a complex nature. The role of the data collector is to observe play and record exercise activity. Data collectors should be well versed in the test/exercise objectives and evaluation criteria and should have those criteria in hand. They need to observe test/exercise play against the criteria developed before the event. Each data collector should remain in contact with the control cell and should inform them if certain objectives are not being exercised as intended. Data collectors are encouraged to record their observations and comments regarding plans, policies, procedures, and equipment.
- **Note Takers.** Note takers document the proceedings of a test or exercise. Like data collectors, they should be well versed in the objectives and evaluation criteria and be familiar with the system's CP procedures. Note takers should especially look for issues, problems, or action items that will be addressed in an After Action Report.

E.3.3. Phase III: Evaluation Mechanisms

TT&E activities must be evaluated to determine the effectiveness of the event and areas requiring additional TT&E attention to improve the viability of the system's CP capability.

Data Collectors and Note Takers are assigned to specific events conducted under the TT&E Program Plan to record and then analyze comments and observations from the TT&E event and the hot wash session. Using data collected during the event and from the hot wash session, the Facilitator, Data Collectors, and Note Takers will determine if the event met the objectives established for it, and then compile an After Action Report. An After Action Report serves as a collection point for information on each event and as a documentation of aspects of the event that went well or need further training, exercising, or procedural modifications, or issues that need to be addressed by the ISO (or designee). The focus of an After Action Report is to identify areas for additional training to further enhance personnel or plan procedure effectiveness; the report should not be used to document specific personnel deficiencies.

Based on the After Action Report, the ISO will evaluate each CP TT&E activity in terms of:

- Validation of CP procedures
- Enhancement of the mission readiness of the CP
- Enhancement of the participants' understanding of the CP mission
- Improvement in the skill level of participants
- Improvement in coordination between participants
- Validation of identified CBPs
- Accomplishment of training objectives
- Overall value of the training to the CP personnel
- Degree to which the training event met program needs.

The ISO, contractor personnel, or other designee prepare After Action Reports for all events. Draft reports are distributed for review to senior leadership. Once all appropriate comments are reflected in the report, a revised draft is distributed to CP technical staff or teams for review. After all comments are received and adjudicated, a final After Action Report is delivered to senior leadership and stored in RISCS.

Resolution of issues identified in the After Action Report are tracked in a follow-on Correction Actions Report (CAR). The CAR summarizes the results of CP TT&E events and details on deficiencies and issues requiring resolution.

Information included in the CAR includes issue status (“open” or “closed”), proposed corrections, tentative completion dates, and assigned priorities.

[1] Note: In the designated ISO actions in this Contingency Planning Handbook, except for approval actions, these responsibilities may be delegated to the CP Coordinator.

[2] Note: A system that uses a database management system is a transaction-based system.

[3] Risk Assessments are typically conducted as part of, and throughout, the RMF process. Refer to [NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*](#) and [NIST SP 800-30, *Guide for Conducting Risk Assessments*](#).

[4] Provided that such components are used in a manner consistent with ITS-HBK-2810.11-2, Media Protection and Sanitization.

[5] Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization’s COOP, BCP, and DRP, as required.

[6] The [FIPS 199](#) category for the availability security objective serves as the initial basis of the BIA.

[7] 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](#).

[8] The CP Coordinator, in coordination with the ISO, 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.

[9] Per [SP 800-53](#), methods for testing CP to determine the effectiveness of the plans and to identify potential weaknesses in the plans include, for example, walk-through and tabletop exercises, checklists, simulations (parallel, full interrupt), and comprehensive exercises.