



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.8.60

JULY 26, 2024

## EFFECTIVE DATE

(07-26-2024)

## PURPOSE

- (1) This transmits the revised IRM 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*.

## MATERIAL CHANGES

- (1) 10.8.60.1, Program Scope and Objectives - Updated subsection to align with standard security policy language.
- (2) 10.8.60.1.1, Background - Updated subsection to align with standard security policy language.
- (3) 10.8.60.1.1.1, Scope - Removed subsection to align with standard security policy language and IRM 1.11.2.2.4.
- (4) 10.8.60.1.1.2, Objectives - Removed subsection to align with standard security policy language and IRM 1.11.2.2.4.
- (5) 10.8.60.1.3, Roles and Responsibilities - Subsection relocated from 10.8.60.2 and updated to align with standard security policy language and IRM 1.11.2.2.4.
- (6) 10.8.60.1.4, Program Management and Review - Added subsection to align with standard security policy language and IRM 1.11.2.2.4.
- (7) 10.8.60.1.5, Program Controls - Added subsection to align with standard security policy language and IRM 1.11.2.2.4.
- (8) 10.8.60.1.6, Terms and Acronyms - Added subsection to align with standard security policy language and IRM 1.11.2.2.4.
- (9) 10.8.60.1.7, Related Resources - Added subsection to align with standard security policy language and IRM 1.11.2.2.4.
- (10) 10.8.60.2, Risk Acceptance and Risk-Based Decisions - Subsection relocated from 10.8.60.1.3 to align with standard security policy language and IRM 1.11.2.2.4.
- (11) 10.8.60.3, IT Roles and Responsibilities - Subsection added to contain supplemental roles and responsibilities specific to the implementation of the IRS ITSCM program.
- (12) 10.8.60.3.1, IRS Executive Sponsors, Program Managers, and Technical Leads - Subsection relocated from 10.8.60.2.1 to align with standard security policy language and IRM 1.11.2.2.4.
- (13) 10.8.60.3.2, Security Risk Management (SRM) Organization - Subsection relocated from 10.8.60.2.2 to align with standard security policy language and IRM 1.11.2.2.4. Removed Business Impact Analysis (BIA) language that has transitioned to IRM 10.8.13, *Information Technology (IT) Security, Business Impact Analysis (BIA) Security Policy*.
- (14) 10.8.60.3.3, Security Operations & Standards Division (SOSD), IT Continuity Services (ITCS) Organization - Subsection relocated from 10.8.60.2.3 to align with standard security policy language and IRM 1.11.2.2.4.

- (15) 10.8.60.3.4, Information Technology (IT) - Subsection relocated from 10.8.60.2.4 to align with standard security policy language and IRM 1.11.2.2.4.
- (16) 10.8.60.3.5, Business Operating Division (BOD) Information System Owners - Subsection relocated from 10.8.60.2.5 to align with standard security policy language and IRM 1.11.2.2.4.
- (17) 10.8.60.3.6, Contracting Officer (CO) - Subsection relocated from 10.8.60.2.6 to align with standard security policy language and IRM 1.11.2.2.4.
- (18) 10.8.60.3.7, Functional Groups - Subsection relocated from 10.8.60.2.7 to align with standard security policy language and IRM 1.11.2.2.4.
- (19) 10.8.60.3.8, Employee: Single Entry Time Reporting - Subsection relocated from 10.8.60.2.8 to align with standard security policy language and IRM 1.11.2.2.4.
- (20) The introduction of subsection 10.8.60.3, IT Roles and Responsibilities caused a renumbering of all remaining original 10.8.60.3.x subsections to 10.8.60.4.x.
- (21) 10.8.60.4, IT Security Controls - Subsection renumbered from 10.8.60.3.
- (22) 10.8.60.4.2 (10.8.60.3.2), CP-02 Contingency Plan - Subsection renamed to align with standard security policy language.
- (23) 10.8.60.3.2.7, IT Business Impact Analysis (IT BIA) - Subsection relocated to IRM 10.8.13.
- (24) 10.8.60.3.2.7.1, BIA Requirement - Subsection relocated to IRM 10.8.13.
- (25) 10.8.60.3.2.7.2, Conducting the IT BIA - Subsection relocated to IRM 10.8.13.
- (26) 10.8.60.4.3 (10.8.60.3.3), CP-03 Contingency Training - Subsection renamed to align with standard security policy language.
- (27) 10.8.60.4.5 (10.8.60.3.5), CP-06 Alternate Storage Site - Subsection renamed to align with standard security policy language.
- (28) 10.8.60.4.6 (10.8.60.3.6), CP-07 Alternate Processing Site - Subsection renamed to align with standard security policy language.
- (29) 10.8.60.4.7 (10.8.60.3.7), CP-09 System Backup - Subsection renamed to align with standard security policy language.
- (30) 10.8.60.4.8 (10.8.60.3.8), CP-10 System Recovery and Reconstitution - Subsection renamed to align with standard security policy language.
- (31) 10.8.60.3.9.2, TIGTA/GAO Audits and Information Requests - Removed this subsection, as the subsection content exists within IRM 10.8.1.
- (32) Exhibit 10.8.60-1, Terms and Acronyms - Exhibit renamed to align with standard security policy language and IRM 1.11.2.2.4.
- (33) Exhibit 10.8.60-2, Related Resources - Exhibit renamed to align with standard security policy language and IRM 1.11.2.2.4.
- (34) Updated language “shall” to “must” throughout the IRM.
- (35) Editorial changes (including grammar, spelling, and minor clarification) were made throughout the IRM. Reviewed and updated plain language, grammar, titles, website addresses, legal references, and IRM references.

## **EFFECT ON OTHER DOCUMENTS**

This supersedes IRM 10.8.60, dated July 16, 2021, and all prior versions of IRM 10.8.60. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance*, IRM 10.8.2, *Information Technology (IT) Security, Information Technology Security Roles and Responsibilities*, IRM 10.8.13, **Information Technology (IT) Security, Business Impact Analysis (BIA) Security Policy**, IRM 10.8.24, **Information Technology (IT) Security, Cloud Computing Security Policy**, and IRM 10.8.62, *Information Technology (IT) Security, Information Systems Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program*.

## **AUDIENCE**

IRM 10.8.60 must be distributed to all personnel responsible for ensuring that adequate security and/or availability is provided for IRS information and information systems. This policy applies to all employees, contractors, and vendors of the IRS.

Rajiv Uppal  
Chief Information Officer



10.8.60

IT Service Continuity Management (ITSCM) Policy and Guidance

## Table of Contents

10.8.60.1 Program Scope and Objectives

10.8.60.1.1 Background

10.8.60.1.2 Authority

10.8.60.1.3 Roles and Responsibilities

10.8.60.1.4 Program Management and Review

10.8.60.1.5 Program Controls

10.8.60.1.6 Terms and Acronyms

10.8.60.1.7 Related Resources

10.8.60.2 Risk Acceptance and Risk-Based Decisions

10.8.60.3 IT Roles and Responsibilities

10.8.60.3.1 IRS Executive Sponsors, Program Managers, and Technical Leads

#

#

10.8.60.3.4 Information Technology (IT)

10.8.60.3.5 Business Operating Division (BOD) Information System Owners

10.8.60.3.6 Contracting Officer (CO)

#

#

10.8.60.4 IT Security Controls

10.8.60.4.1 AT - Security Awareness and Training

10.8.60.4.2 CP-2 Contingency Plan

10.8.60.4.2.1 Contingency Planning/Disaster Recovery and Business Continuity

10.8.60.4.2.2 Contingency Planning/Disaster Recovery Plans

10.8.60.4.2.3 ISCP Plan Appendices

10.8.60.4.2.4 Information System Contingency Plan (ISCP) Requirements

10.8.60.4.2.4.1 Supporting Information

10.8.60.4.2.4.2 Activation and Notification Phase

10.8.60.4.2.4.3 Information System Contingency Plan (ISCP) Maintenance

10.8.60.4.2.5 Disaster Recovery Plan (DRP)

10.8.60.4.2.5.1 DRP Requirement

10.8.60.4.2.5.2 IT DRP Planning Process

10.8.60.4.2.6 Information System Contingency Planning Process

10.8.60.4.2.7 Critical Business Processes (CBPs)/Critical Functions

10.8.60.4.3 CP-03 Contingency Training

10.8.60.4.3.1 Disaster Recovery Training Guidelines

- 10.8.60.4.3.2 Disaster Recovery Certifications
- 10.8.60.4.3.3 Information System Contingency Plan (ISCP) Training
- 10.8.60.4.4 Contingency Plan Testing
  - 10.8.60.4.4.1 ISCP Testing, Training, and Exercise
  - 10.8.60.4.4.2 Information System Contingency Plan (ISCP) Exercises
  - 10.8.60.4.4.3 IT Service Continuity Management (ITSCM) Test
- 10.8.60.4.5 CP-06 - Alternate Storage Site
- 10.8.60.4.6 CP-07 - Alternate Processing Site
- 10.8.60.4.7 CP-09 System Backup
- 10.8.60.4.8 CP-10 System Recovery and Reconstitution
  - 10.8.60.4.8.1 Recovery Phase
  - 10.8.60.4.8.2 Reconstitution Phase
  - 10.8.60.4.8.3 Recovery Strategies
  - 10.8.60.4.8.4 Identify Resource Requirements
  - 10.8.60.4.8.5 Identify System Resource Recovery Priorities
  - 10.8.60.4.8.6 Identify Preventive Controls
  - 10.8.60.4.8.7 Equipment Replacement
  - 10.8.60.4.8.8 Cost Considerations
- 10.8.60.4.9 Access and Requests for IS Contingency/Disaster Recovery Information
  - 10.8.60.4.9.1 Internal Information Requests
- 10.8.60.4.10 Hosting Non-IRS Agencies for Disaster Recovery
- 10.8.60.4.11 Technical Contingency Planning Considerations
  - 10.8.60.4.11.1 Common Considerations
  - 10.8.60.4.11.2 Client/Server Systems
    - 10.8.60.4.11.2.1 Client/Server Systems Contingency Considerations
    - 10.8.60.4.11.2.2 Client/Server Systems Contingency Solutions
  - 10.8.60.4.11.3 Telecommunications Contingency Considerations
    - 10.8.60.4.11.3.1 Telecommunications Contingency Solutions
  - 10.8.60.4.11.4 Mainframe Systems
    - 10.8.60.4.11.4.1 Mainframe Contingency Solutions

Exhibits

- 10.8.60-1 Glossary and Acronyms
- 10.8.60-2 References

10.8.60.1  
(07-26-2024)  
**Program Scope and Objectives**

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of IT Service Continuity Management (ITSCM) within the IRS.
  - a. This policy is subordinate to IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS ITSCM for on-premise systems, including on-premise cloud deployments.
  - b. This policy is subordinate to IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy* and augments the existing requirements identified within IRM 10.8.24, as they relate to IRS ITSCM for off-premise cloud deployments.
- (2) **Purpose of the Program:** Develop and publish security policies to protect the IRS against potential IT threats and vulnerabilities and ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this policy apply to:
  - a. All offices and business, operating, and functional units within the IRS.
  - b. IRS personnel and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate systems that store, process, or transmit IRS Information or connect to an IRS network or system.
- (4) **Policy Owner:** Chief Information Officer (CIO).
- (5) **Program Owner:** Cybersecurity, Threat Response and Remediation (an organization within Cybersecurity)
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.60.1.1  
(07-16-2021)  
**Background**

- (1) This IRM provides policies and guidance to be used by IRS organizations to carry out their respective responsibilities under ITSCM for information systems security and availability regarding Information System Contingency Plans (ISCP) and Disaster Recovery (DR).
  - a. The Associate Chief Information Officer (ACIO) of Information Technology (IT) Cybersecurity is responsible for defining relevant policy requirements for the IRS enterprise-wide ITSCM program and for ensuring Information System (IS) Contingency Plans are developed, executable, and successfully implemented.
  - b. This IRM defines the overall requirements to ensure compliance with policy and regulations and the ability to recover the IRS's Critical Business Processes (CBPs), hereinafter referred to as Critical Functions, through the systems and applications that support them.
- (2) IRM 10.8.60 is part of the IRM Part 10, Security, Privacy and Assurance series for IRS IT Cybersecurity.

10.8.60.1.2  
(07-16-2021)  
**Authority**

- (1) All IRS information systems and applications must be compliant with Executive Orders (EOs), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), Department of the Treasury, and IRS guidelines as they apply.
- (2) This ITSCM policy provides requirements and guidance to ensure that
  - a. All IRS IT systems and applications must have sufficient Disaster Recovery (DR) capability to recover IRS data with system/application functionality (data is available and usable to customer) according to agreed upon pre-defined Recovery Time Objectives (RTOs)/Recovery Point Objectives (RPOs)/Maximum Tolerable Downtime (MTD) documented in the ISCP.
- (3) In accordance with Federal laws and regulations, the IRS must:
  - a. Establish and manage an Information Security Program within all its offices.
  - b. Assign security responsibility to appropriate officials.
  - c. Ensure continuity of operations for information systems that support the operations and assets of the agency.
  - d. Authorize Security Assessment & Authorization (SA&A) for systems and applications prior to operations, and periodically after deployment.
  - e. Conduct tabletops, functional exercises, or disaster recovery tests (e.g., Alternate Processing Sites (APS)) as required for their systems' disaster recovery planning documents capabilities at least annually within a FISMA period. FISMA periods run from July 1 thru June 30 each year. Exercises and tests will be conducted with all impacted parties.
  - f. Train appropriate personnel in their continuity roles in accordance with ITSCM policy.
  - g. Track and document findings and lessons learned to ensure that corrective action plans and executive briefings can be developed.
  - h. Ensure that findings are reported to executive management for the direction and leadership to assure timely implementation of corrective action plans to resolve findings or accept risks.
- (4) The Capability Maturity Model Integration (CMMI) must be used to judge the maturity of all IRS organizational processes and related procedures and process assets and can be used to plan further improvements. CMMI sets the standard for the essential elements of effective and mature processes, improved with quality and efficiency.
- (5) The Information Technology Infrastructure Library (ITIL), a collection of best practices, must be used by the IRS to build an efficient framework for delivering IT Service Management (ITSM), ITSCM, and ensuring that the IRS is meeting business goals and delivering benefits that facilitate business change, transformation, and growth.
- (6) The Project Management Institute (PMI) organization advances the project management profession through globally recognized standards and certifications. PMI standards, such as the Project Management Body of Knowledge (PMBOK), are the preferred IRS method of project management.



- (7) All artifacts developed or acquired by the IRS, must incorporate CMMI, ITIL, and/or PMI requirements, in order to meet the business objectives of the IRS because the artifacts represent investments by the organization that are expected to provide current and future business value to the IRS.
- 10.8.60.1.3  
(07-26-2024)  
**Roles and Responsibilities**
- (1) IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*, defines IRS-wide roles and responsibilities related to IRS information and system security and is the authoritative source for such information.
- (2) The supplemental roles and responsibilities specific to the implementation of the IRS ITSCM program are located in IRM 10.8.60.3 , IT Roles and Responsibilities of this IRM.
- 10.8.60.1.4  
(07-26-2024)  
**Program Management and Review**
- (1) The IRS Security Policy Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8 series and the development of technology specific security requirements checklists. Stakeholders are notified when revisions to the security policies and security requirements checklists are made.
- (2) It is the policy of the IRS to:
- Establish and manage an Information Security Program within all its offices. This policy provides uniform policies and guidance to be used by each office.
  - Protect all IT resources belonging to, or used by, the IRS at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.
  - Protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, OMB guidance, Treasury Directives (TDs), NIST Publications, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
  - Use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Enterprise Life Cycle (ELC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.
- 10.8.60.1.5  
(07-26-2024)  
**Program Controls**
- (1) Each IRM in the 10.8 series is assigned an author who reviews the IRM to ensure accuracy. The IRM authors continuously monitor federal guidance (e.g., OMB, CISA, NIST, Defense Information Systems Agency (DISA)) for potential revisions to security policies and security requirements checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.
- (2) Security Policy provides a report identifying security policies and security requirements checklists that have recently been revised or are in the process of being revised.

- (3) This IRM applies to all IRS information and systems, which store, process, or transmit IRS information or connect to an IRS network or system. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (CNSI)*, for additional guidance for protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for all IRS IT assets in order to:

a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.

b. Prevent unauthorized access to IRS assets.

c. Enable IRS IT computing environments to meet the security requirements of this policy and support the business needs of the organization.
- (5) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this policy are more restrictive.

10.8.60.1.6  
(07-26-2024)  
**Terms and Acronyms**

- (1) Refer to Exhibit 10.8.60-1 for a list of terms, acronyms, and definitions.

10.8.60.1.7  
(07-26-2024)  
**Related Resources**

- (1) Refer to Exhibit 10.8.60-2 for a list of related resources and references.

10.8.60.2  
(07-26-2024)  
**Risk Acceptance and Risk-Based Decisions**

- (1) Any exception to this policy requires the Authorizing Official (AO) to make a Risk-Based Decision (RBD).
- (2) Users must submit RBD requests in accordance with Cybersecurity’s Security Risk Management (SRM) Risk Acceptance Process documented in the Request for Risk Acceptance and Risk Based Decision (RBD) Standard Operating Procedures (SOP).

#

#

#

- (3) Refer to IRM 10.8.1 for additional guidance on Risk Acceptance.

10.8.60.3  
(07-26-2024)  
**IT Roles and Responsibilities**

- (1) The following supplemental roles and responsibilities are specific to the implementation of the IRS ITSCM program.

10.8.60.3.1  
(07-26-2024)  
**IRS Executive Sponsors, Program Managers, and Technical Leads**

- (1) IRS Executive Sponsors, Program Managers, and Technical Leads must be identified for all major ITSCM infrastructure initiatives. These initiatives must:

a. Comply with One Solution Delivery Lifecycle (OneSDLC) requirements.

b. Address infrastructure changes.

c. Support day-to-day operations (e.g., desktop support, Unified Work Request (UWR) process, change requests, service desk support, server support, security, email support, and asset inventory).

- d. Comply with or establish service level agreements (SLAs).
- e. Complete infrastructure integration tests.

#####

#####

10.8.60.3.3  
(07-26-2024)

- (2) SOSD ITCS is responsible for coordinating the efforts of the enterprise-wide ITSCM Program as follows:

**#**

**#**

#  
#  
#  
#  
#  
#  
#  
#10.8.60.3.4  
(07-26-2024)**Information Technology  
(IT)**

(1) IT is responsible for:

- Ensuring NIST SP 800–53 contingency plan controls are implemented and documented.
- Providing updates to the ISCP with changes to the owner as updates are identified, but not less than annually.
- Providing subject matter expertise for DR capabilities.
- Providing subject matter expertise to write the detailed content (keystrokes/step-by-step) of each plan.
- Assigning a DR Test Director.
- Performing annual execution and exercise of each ISCP.
- Performing annual execution and tests of each disaster recovery planning document.
- Updating the disaster recovery planning documents with changes after each DR Test.
- Partnering with SRM and BODs to coordinate requirements, priorities, recovery times, cost evaluations, and support to procurement activities to enhance DR capabilities to meet stated business objectives.
- Maintaining/owning the content of the disaster recovery planning documents.
- Providing resources for DR planning, including staffing, location, and procuring funded equipment.
- Establishing a succession planning document to ensure the service is protected from experiencing a personnel single point of failure within their organization in the event of a disaster, which would negatively impact the recovery of systems and/or applications.
- Securing concurrence, in writing, from the Director, SRM, and business unit (BU) Manager prior to closing all ISCP/disaster recovery planning documents related to POA&M and OneSDLC items.
- Ensuring that staff, who have roles in developing and/or exercising information system contingency plans and/or disaster recovery plans, attend contingency planning and disaster recovery awareness and training.
- Identifying backup storage sites and coordinating with Business Owners to document site location in the ISCP and disaster recovery planning documents.
- Ensuring that all data/applications code has been backed up and sequence is identified in the ISCP.
- Ensuring backup media has been encrypted with encryption procedures listed in the ISCP.
- Ensuring backup media is sent to an offsite location and coordinating with Business Owners to document site location in the ISCP.

- (1) The BOD/Information System Owner is the agency official responsible for the overall procurement, development, integration, modification, operation and maintenance of the information system. For applications housed on systems owned by or operated by IT, IRS IT will work with BODs to determine appropriate enterprise priorities and identify funding sources for the procurement of equipment. The Information System Owner is also known as the Business and Functional Unit Owner.
- (2) Each BOD that owns or operates IT resources must comply with the IT requirements. Refer to the Information Technology (IT) subsection in this IRM.
- (3) Each contractor or vendor that owns or operates IT resources on behalf of the IRS must comply with the IT requirements.

#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#

- (5) In addition to the Information System Owner/Business and Functional Unit Owner responsibilities defined in IRM 10.8.2, Business and Functional Unit Owners must:
- Include security requirements in their capital planning and investment business cases.
  - Ensure security requirements are adequately funded and documented in accordance with OMB Circular A-11 (Preparation, Submission, and Execution of the Budget).
  - Fully describe and document the information system in the ISCP.
  - Clearly define system and application priorities, subsequent needs, and related risk acceptance or avoidance for recovery.
  - Determine recovery needs and timeframes needed for business restoration through comprehensive DR evaluations.
  - Determine what data needs to be recovered and the priority order for recovery.
  - Develop DR requirements during the development phase of all new systems and throughout any production system upgrades.
  - Provide the funding for the DR equipment/space/storage needed to meet the recovery goals (set by the business).

- Fully describe and document the details of the information system in the ISCP that is required by FISMA for each system.
  - Ensure ISCPs and DR plans for all applications and systems are reviewed annually, have a tabletop exercise performed annually and tested annually if applicable per current requirements.
  - Work jointly with IT Operations, SRM, and A&I in development and tests of DR plans to ensure business continuity.
  - Support the development of processing priorities for completion of work following emergencies that degrade computer processing capabilities.
  - Work jointly with IT in the tests of the disaster recovery planning documents to ensure availability of data from the recovered system.
  - Work with SRM regarding enterprise priorities.
- (6) When integrated Business Continuity (BC) ITCSM exercises are planned, it is recommended that BODs work jointly with FMSS, IRS IT operations, and SRM to conduct these exercises and to validate the recovery times of critical functions and supporting applications.

10.8.60.3.6  
(07-26-2024)  
**Contracting Officer (CO)**

- (1) Each contractor or vendor that owns or operates IT resources on behalf of the IRS must also comply with IRS IT requirements in that particular contract and the Information Technology (IT) subsection of this IRM.
- (2) Contracting Officers (COs) acting on IRS behalf are required to ensure the inclusion of IRS DR expectations within contracts for the purpose of DR support. The contract must include the following:

#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#

- (3) SRM or A&I (as applicable) are responsible for preparing justification and requirement documents to support the letting of any contracts needed to support ITSCM; to provide necessary recovery capability; or to support continuity plans in conjunction with the ITIL Supplier Management process.

#  
#  
#  
  
#  
#  
#



[illegible]



[illegible]


#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#

10.8.60.4  
(07-16-2021)  
**IT Security Controls**

- (1) The security controls in this IRM supplement the requirements defined in IRM 10.8.1.
  - a. Refer to IRM 10.8.1 for security control families and security controls not addressed within this IRM.
- (2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.
- (3) To configure less restrictive requirements requires a risk-based decision. Refer to the Risk Acceptance and Risk-Based Decisions subsection within this IRM for additional guidance.

10.8.60.4.1  
(10-04-2012)  
**AT - Security Awareness and Training**

- (1) FISMA requires that all agencies establish security awareness and training to inform personnel, including contractors and vendors, of information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures to protect the confidentiality, integrity, and availability of information and information systems. (IRS-defined)
- (2) Refer to IRM 10.8.1, IRM 10.8.24, and IRM 10.8.2 for additional guidance on Security Awareness and Training.

10.8.60.4.2  
(10-04-2012)  
**CP-2 Contingency Plan**

- (1) The IRS must have the ability to withstand all hazards and sustain its mission through environmental changes. These changes can be gradual, such as economic or mission changes, or sudden, as in a disaster event. Rather than just working to identify and mitigate threats, vulnerabilities, and risks, organizations can work toward building a resilient infrastructure, minimizing the impact of any disruption on mission-essential functions. (NIST 800-34: Section 2.1)
- (2) Resilience is the ability to quickly adapt and recover from any known or unknown changes to the environment. The Department of Homeland Security (DHS) Risk Lexicon (September 2008) defines resilience as the “ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions.” The goal of the disaster recovery program is to continually improve

IRS's ability to adapt to changes, risks, and unexpected events that can affect IRS' ability to continue critical functions and mission. (NIST 800-34: Section 2.1)

- (3) Contingency planning focuses on the Federal Information Processing Standards (FIPS) 199 Standards for Security Categorization of Federal Information and Information Systems security categorization of availability when looking at the contingency needs of information systems. Strategies for high-impact systems should consider high availability options in their design, where a low availability system may not need to be available for several weeks in the event of a significant disruption. High availability options are usually expensive and include options such as redundant systems, data mirroring, and database replication; these options should only be considered for critical, high availability systems. (NIST 800-34: Section 2.1)
- (4) Effective contingency planning includes incorporating security controls early in the development of an information system, and maintaining these controls on an ongoing basis. NIST SP 800-53 identifies Contingency Planning (CP) security controls for information systems. Not all controls are applicable to all systems. The IRS uses the FIPS 199 security categorization as a baseline to determine which controls apply to a particular system. For example, information systems that have availability as a security objective categorized as moderate-impact may only require compliance with only the first system backup control enhancements. Once a baseline has been identified, the IRS can then tailor the baseline to meet IRS business needs and then apply the appropriate controls and control enhancements to IRS information systems. Refer to IRM 10.8.1 for information on the tailored baseline of contingency planning security controls that are applicable. (NIST 800-34: Section 2.1)

**Note:** The CP security controls defined in IRM 10.8.1 are the minimum controls. The IRS requires all systems to have a DR site and those systems or applications supporting an IRS Critical Business Process may also have an increased requirement.

- (5) Refer to IRM 10.8.1 or IRM 10.8.24 for additional guidance on Contingency Plan

10.8.60.4.2.1  
(12-02-2019)  
**Contingency  
Planning/Disaster  
Recovery and Business  
Continuity**

- (1) ISCPs and disaster recovery planning documents are supporting documents in an organization's overall Contingency Plan. In the event of a significant incident, the IRS would use a suite of plans to effectively respond, react, recover, and resume business. The BCP acts as an over-arching plan, that encompasses all activities that ensure business resumes and continues in the event of a significant impact or disaster. (NIST 800-34: Section 2.2)
- (2) Note the difference between Contingency Planning and Continuity Planning, both critical components of the overall BCP: (NIST 800-34: Section 2.2)

Contingency Planning applies to *information systems* and addresses the steps necessary to recover operations at an existing or new location in an emergency.

Continuity Planning applies to the *business/mission* of the service and the ability to continue critical functions and functions during and after an emergency event.

(3) Numerous plans contribute to the organizations overall BCP. (NIST 800-34: Section 2.2)

a. Nine core documents from a DR perspective are:

- Business Continuity Plan (BCP)
- Continuity of Operations Plan (COOP)
- Crisis Communications Plan (CCP)
- Critical Infrastructure Protection (CIP) Plan
- Incident Response Plan
- Disaster Recovery (DR)
- Information System Contingency Plan (ISCP)
- Occupant Emergency Plan (OEP)
- Incident Management Plan (IRS-defined)

b. These documents relate as indicated in the table:

Business Continuity Plan								
Business Continuity Plan (BCP)	Continuity of Operations Plan (COOP)	Crisis Communications Plan (CCP)	Critical Infrastructure Protection (CIP) Plan	Incident Response Plan	Disaster Recovery (DR) Plan	Information System Contingency Plan (ISCP)	Occupant Emergency Plan (OEP)	Incident Management Plan

## 10.8.60.4.2.2 (12-02-2019) Contingency Planning/Disaster Recovery Plans

- (1) The BCP is the business/functional unit plan that includes the advance planning and preparations necessary to minimize loss and ensure continuity of Mission Essential Functions (MEFs), as well as Critical Business Processes (CBPs), during and after a disruption. (NIST 800-34: Section 2.2.1)
  - a. The ISCP Coordinator must coordinate with information system owners to ensure that the BCP expectations and IS capabilities are matched. (NIST 800-34: Section 2.2.1)
  - b. Refer to Business Continuity Plan subsection in IRM 10.8.1 for additional guidance on BCP. (IRS-defined)
- (2) The Incident Response Plan should outline procedures to enable security personnel to identify, mitigate, and recover from malicious computer incidents,

such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data. (NIST 800-34: Section 2.2.5)

- a. Refer to IRM 10.8.1, for additional guidance on Incident Response.
  - b. Refer to IRM 10.8.2, for Incident Response roles and responsibilities.
- (3) The Critical Infrastructure Protection (CIP) Plan addresses the security, protection, and resiliency of those components of the national infrastructure critical to national and economic security. (TD P 85-01: Appendix J)
- a. CIP's Plan defines the roles and responsibilities for protection, develops partnerships and information sharing relationships, implements the risk management framework defined in the National Infrastructure Protection Plan (NIPP) and Homeland Security Presidential Directive (HSPD) - 7 for critical infrastructure and key resources, and integrates federal, state and local emergency preparedness, protection, and resiliency of critical infrastructure. (NIST 800-34: Section 2.2.4)
  - b. CIP's Plan applies to all components that own, administer, or operate Treasury Designated Cyber Critical Infrastructure, including those housed in contractor and non-Treasury government facilities. (TD P 85-01: Appendix J)
  - c. Refer to IRM 10.8.1 for additional guidance on CIP.
- (4) The Crisis Communications Plan (CCP), also known as an Emergency Communication Plan (ECP), must document standard procedures for internal and external communications in the event of a disruption. The Crisis Communications Plan specifies the following (NIST 800-34: Section 2.2.3):
- a. Individual(s) as the only authority for answering questions from or providing information to the public regarding emergency response. Designated person(s) must have access to IRS' senior leadership.
  - b. Procedures for disseminating reports to personnel on incident status.
  - c. Templates for public press releases.
- (5) The Occupant Emergency Plan (OEP) must outline first-response procedures for occupants of a facility in the event of a threat or incident to the health and safety of personnel, the environment, or property. (NIST 800-34: Section 2.2.8)
- a. Shelter-in-place procedures must be included in the OEP.
- Note:** OEPs and shelter-in-place procedures for IRS employees can be found on the Office Resources website under Emergency and Safety for topics of "Emergencies, Safety, & Health" at: <https://irsgov.sharepoint.com/sites/EmployeeResources/SitePages/EmergencySafety.aspx>
- b. Refer to IRM 10.8.1 for additional guidance on Emergency Response Capability.
- (6) The Continuity of Operations Plan (COOP) must outline procedures to restore MEFs at an alternate site for a period of up to 30 days of operation. (NIST 800-34: Section 2.2.2)
- a. The COOP must include, at a minimum:
    - i. Program plans and procedures
    - ii. Risk Management
    - iii. Budgeting and acquisition of resources

- iv. Essential functions
- v. Order of succession
- vi. Delegation of authority
- vii. Continuity Facilities
- viii. Continuity communications
- ix. Vital records management
- x. Human capital
- xi. Test, training, and exercise
- xii. Devolution
- xiii. Reconstitution

**Note:** COOP plans are mandated for organizations by HSPD-20/NSPD-51, National Continuity Policy and DHS Federal Continuity Directive (FCD), Federal Executive Branch Continuity Program and Requirements.

- (7) The Disaster Recovery (DR) Plan must house a centralized set of information system contingency plans for major disruptions that result in denied access to the primary facility infrastructure for an extended period of time and that further require relocation and transition of information systems. The DRP is site-specific. A DRP must exist for each site, including the primary site, as well as the alternate site(s). (NIST 800-34: Section 2.2.6)
- (8) The Information System Contingency Plan (ISCP) must outline procedures for information system recovery following major disruptions. ISCPs must document roles and responsibilities, inventory information, system assessment procedures, detailed recovery procedures, and system testing procedures. The ISCP documents technical capabilities designed to support contingency operations. The ISCP is information system-specific. ISCPs are developed for site-specific applications, business unit level applications, and enterprise-wide applications. An ISCP must exist for each information system. (NIST 800-34: Section 2.2.7)

#### 10.8.60.4.2.3 (12-02-2019) **ISCP Plan Appendices**

- (1) Consideration of appendices for inclusion in contingency plans must include the following (NIST 800-34: Section 4.5):
  - Contact information for contingency planning team personnel
  - Vendor contact information, including offsite storage and alternate site POCs
  - BIA

**Note:** Refer to IRM 10.8.13 for additional guidance regarding BIA.

  - Detailed recovery procedures and checklists
  - Detailed validation testing procedures and checklists
  - Equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations. Details must be provided for each entry, including model or version number, specifications, and quantity
  - Alternate mission/business processing procedures that may occur while recovery efforts are being done to the system
  - ISCP testing and maintenance procedures
  - System interconnections (systems that directly interconnect or exchange information)

- Vendor SLAs, reciprocal agreements with other organizations, and other vital records

10.8.60.4.2.4  
(10-04-2012)

**Information System  
Contingency Plan (ISCP)  
Requirements**

- (1) IRM 10.8.1 requires the development and maintenance of continuity of support plans/ISCPs. (IRS-defined)
- (2) The ISCP must provide the procedures and capabilities for recovering systems and applications when relocation of those assets is not necessary. In addition, the ISCP addresses the resources, roles, responsibilities, and procedures for recovering IT systems after a disruption. (NIST 800-34: Chapter 4)

**Note:** Refer to the Disaster Recovery Plan (DRP) subsection in this IRM for additional guidance.

- (3) All FISMA-reportable systems must have an ISCP. (IRS-defined)
- (4) All FISMA-reportable systems must exercise their ISCP annually. (IRS-defined)

**Note:** The ISCP tabletop/test processes and documentation are the same during an Accreditation and Authorization and during the SRM ISCP FISMA Process.

#  
#  
#

- (6) ISCPs must be reviewed no less than annually, and when major changes are made to the system, or contact information necessary in the event of an incident have changed. (IRS-defined)

10.8.60.4.2.4.1  
(12-02-2019)

**Supporting Information**

- (1) Supporting information included in the ISCP must include an introduction section and a concept of operations section, as well as BIA, POC lists and procedures. (NIST 800-34: Section 4.1)
- (2) The introduction section must include the background, scope and assumptions (NIST 800-34: Section 4.1):
  - Background - This subsection establishes the reason for developing the ISCP and defines the plan objectives.
  - Scope - The scope identifies the FIPS 199 impact level and associated RTOs as well as the alternate site and data storage capabilities (as applicable).
  - Assumptions - This subsection includes the list of assumptions that were used in developing the ISCP as well as a list of situations that are not applicable.
- (3) The concept of operations section must provide additional details about the information system, the phases of the contingency plan, and a description of the information system contingency plan roles and responsibilities (NIST 800-34: Section 4.1):
  - System description - The description of the information system addressed by the contingency plan must include the information system architecture, location(s), and any other important technical consider-



ations. System description content may include an input/output (I/O) diagram and a system architecture diagram.

- Overview of three phases - The ISCP recovery is implemented in three phases: (1) Activation and Notification, (2) Recovery, and (3) Reconstitution.
- Roles and responsibilities - The roles and responsibilities subsection presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The subsection also provides an overview of team member roles and responsibilities in a contingency situation. Teams and team members must be designated for specific response and recovery roles during contingency plan activation.

**Note:** Refer to NIST SP 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, for further details concerning information system documentation.

## 10.8.60.4.2.4.2 (12-02-2019) **Activation and Notification Phase**

- (1) The ISCP must be activated if one or more of the activation criteria for that system are met. Activation criteria may include (NIST 800-34: Section 4.2.1):
  - Extent of any damage to the system (e.g., physical, operational, or cost).
  - Criticality of the system to the organization's mission (e.g., critical infrastructure protection asset).
  - Expected duration of the outage lasting longer than the RTO.
- (2) The appropriate recovery teams may be notified once the system outage or disruption has been identified and the ISCP Coordinator has determined that activation criteria have been met. (NIST 800-34: Section 4.2.1)
- (3) Notification procedures must describe methods that will be effective for 24 hours a day / 7 days a week / 365 days a year timeframe. Prompt notification is important for reducing the effects of a disruption on the system. Notifications may be accomplished, either automated or manual, via telephone, pager, electronic mail (email), cell phone, and messaging methods. (NIST 800-34: Section 4.2.2)
  - a. Automated notification systems follow established protocols and criteria and can include rapid authentication and acceptance and secure messaging. Automated notification systems may require up-front investment and learning curve.
  - b. A common manual notification method is a call tree. This technique involves assigning notification duties to specific individuals, who are team leaders of a functional or geographic area and who in turn are responsible for notifying other recovery personnel. The call tree must account for primary and alternate contact methods. The call tree must identify personnel by their team position, name, and contact information (e.g., home, work, cell phone, email addresses, and home addresses).
  - c. Information to be included in notification may include the following:
    - i. Nature of the outage or disruption that has occurred or is impending
    - ii. Any known outage estimates
    - iii. Response and recovery details
    - iv. Where and when to convene for briefing or further response instruc-

tions

v. Instructions to prepare for relocation for estimated time period (if applicable)

vi. Instructions to complete notifications using the call tree (if applicable)

**Note:** Notifications sent via email must be done with caution because there is no way to ensure receipt and acknowledgement. Notifications must be sent to work or personal accounts to ensure greater visibility by recovery personnel.

**Note:** Notification procedures must define procedures when designated personnel cannot be contacted.

**Note:** Point of contacts must be identified for each external organization or interconnected system partner that may be adversely affected if POC's are unaware of the situation. These POCs may be included in notification procedures.

- (4) To determine how the ISCP will be implemented following a system disruption or outage, it is essential to assess the nature and extent of the disruption. The outage assessment must be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority. The following areas must be addressed: (NIST 800-34: Section 4.2.3)

- 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)
- Estimated time to restore normal services

10.8.60.4.2.4.3

(12-02-2019)

**Information System  
Contingency Plan (ISCP)  
Maintenance**

- (1) To be effective, the plan must be maintained in a ready state that accurately reflects current system requirements, procedures, organizational structure, and policies. (NIST 800-34: Section 3.6)
- a. ISCPs must be reviewed no less than annually, and when major changes are made to the system, or contact information necessary in the event of an incident have changed.
- (2) At a minimum, plan reviews must focus on the following elements (NIST 800-34: Section 3.6):
- Operational requirements
  - Security requirements
  - Technical procedures
  - Hardware, software, and other equipment (types, specifications, and amount)
  - Names and contact information of team members

- Names and contact information of vendors, including alternate and offsite vendor POCs
  - Alternate and offsite facility requirements
  - Vital records (electronic and hardcopy)
- (3) The ISCP Coordinator must maintain a record of copies of the plan and to whom the copies were distributed. (NIST 800-34: Section 3.6)
- a. To ensure its availability and good condition in the event local plan copies cannot be accessed because of disaster, a copy must also be stored at the alternate site and with the backup media.
  - b. Strict version control must be maintained by requesting old plans or plan pages to be returned to the ISCP Coordinator in exchange for the new plan or plan pages.
  - c. Other information that must be stored with the plan includes the following:
    - i. Contracts with vendors (SLAs and other contracts)
    - ii. Software licenses
    - iii. System user manuals
    - iv. Security manuals
    - v. Operating procedures
- (4) Changes made to the plan, strategies, and policies must be coordinated through the ISCP Coordinator, who must communicate changes to the system owner. (NIST 800-34: Section 3.6)
- a. The ISCP Coordinator must record plan modifications using a record of changes, which lists the page number, change comment, and date of change.
  - b. The ISCP Coordinator must coordinate frequently with system POCs, internal to the IRS, as well as external, to ensure that impacts caused by changes will be reflected in the contingency plan.
  - c. The ISCP Coordinator must evaluate the following supporting information to ensure that the information is current and continues to meet system requirements adequately:
    - i. Alternate site contract, including testing times
    - ii. Offsite storage contract
    - iii. Software licenses
    - iv. MOUs or vendor SLAs
    - v. Hardware and software requirements
    - vi. System interconnection agreements
    - vii. Security requirements
    - viii. Recovery strategy
    - viii. Contingency policies
    - x. Training and awareness materials
    - xi. Testing scope
    - xii. Other plans, e.g., COOP, BCP.
  - d. As new technologies become available, preventive controls may be enhanced and recovery strategies may be modified.
- (5) Plan maintenance must 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. (NIST 800-34: Section 3.6)

- (6) Availability of electronic vital records supporting contingency planning and disaster recovery planning may be impeded during periods of system outages or disruptions. Non-electronic paper copies must be considered for the following vital records (IRS-defined):

- Continuity of operations plan and other emergency plans and directives
- Staffing assignments
- Policy documents
- Selected program records
- Contracting and acquisition files
- Personnel files
- Insurance files
- Orders of succession
- Delegations of authority
- Contact information

## 10.8.60.4.2.5

(12-24-2013)

**Disaster Recovery Plan (DRP)**

- (1) The DRP defines the resources, roles, responsibilities, actions, tasks, and the steps required, down to a key step level, to restore an IT system to its full operational status at the alternate facility after a disruption. Within the IRS, the DRP is a standalone document contained within the automated tool TSCC. The DRP must include recovery keystroke procedures that provide system or application recovery steps with greater detail than the ISCP. Typically, these disaster recovery planning documents are activated only when there has been a significant incident requiring relocation of the system or application. (IRS-defined)
- (2) A DRP or disaster recovery planning document refers to an IT-focused plan designed to restore operability of the target system and/or application in computing space within an alternate site after an emergency. (IRS-defined)
- (3) The disaster recovery planning document must define the resources, roles, responsibilities, actions, tasks, and the detailed work steps (keystrokes) required to restore an IT system to its full operational status at the current or alternate facility after a major disruption with long-term effects. (IRS-defined)
- (4) The disaster recovery planning document must be developed with the following factors considered: (IRS-defined)
- Operational requirements.
  - Security requirements.
  - Technical procedures.
  - Hardware, software, and other equipment.
  - Names and contact information of team members.
  - Names and contact information of contractors and vendors.
  - Alternate and offsite requirements.
  - Vital records (electronic and hardcopy).
- (5) For assistance in developing a DRP/disaster recovery planning document and for copies of the DRP templates, email the SRM at \*IT IT DR Mailbox, and put DRP in the subject line to assist in routing the request. (IRS-defined)

## 10.8.60.4.2.5.1

(10-04-2012)

**DRP Requirement**

- (1) All FISMA-reportable systems must have recovery capability. (IRS-defined)

- a. Funding of the DR solution is the responsibility of the IT organization with input/support from the Business Owner and will be addressed in the SLA or MOU as appropriate.
- (2) All systems and applications, including FISMA-reportable systems must have disaster recovery planning documents. (IRS-defined)
  - a. All systems used for recovery must comply with existing IRS policies.
  - b. Refer to the CP-04 Contingency Plan Testing section within this IRM for additional guidance on disaster recovery planning documents.
- (3) DR-related information, including recovery times, must be documented in the disaster recovery planning documents and other areas within the ISCP as appropriate. (IRS-defined)
- (4) The owner of the system must be responsible for the disaster recovery planning documents.
  - a. The planning document must be maintained by the owner and IT operations responsible for the recovery of the system referenced by the plan. (IRS-defined)
- (5) IT assets that are not FISMA-reportable, which are determined to have interdependency with a FISMA-reportable asset, must have disaster recovery planning documents. (IRS-defined)
  - a. While the DR planning document can be a part of the overall ISCP, the document can also be a standalone document that provides guidance and procedures necessary for the technical recovery of a system or application at an alternate site.
  - b. Depending on the size and complexity of the disaster recovery planning documents, the document may be maintained separately from the ISCP.
  - c. High-level guidance and reference to the disaster recovery planning documents and where the documents may be obtained must be maintained in the ISCP.
- (6) The disaster recovery planning documents must be sufficiently detailed (detailed work steps/key strokes) and complete enough to recover the system and/or application to the working level prescribed by the ISCP/MOU/SLA for which the document was written, by any administrator/operations staff with the appropriate skills and permissions. (IRS-defined)
- (7) A risk assessment must be performed for all FISMA-reportable systems and applications that do not support the IRS's critical functions to determine the extent of necessary recovery capability. (IRS-defined)
- (8) Owners of all systems and applications supporting a critical function must annually test some or all of their recovery capability in order to ensure the continuity of the operations of the IRS. This may be done through functional or DR Tests. (IRS-defined)
- (9) Modifications to this annual requirement must be submitted to and approved by the Director, Security Risk Management. (IRS-defined)
  - a. Request must include:  
Name of BOD

#####

**Note:** Per Department of the Treasury: For some smaller (particularly FIPS 199 Low availability) systems, a full contingency plan may not exist when a bureau decides that the system's contingency plan is to not bring the system back up after an incident. This will still have to be documented. To satisfy

this requirement, include a summary of the Business Impact Analysis that supports the decision to not recover or reconstitute the system. The testing requirement for these systems can be satisfied by annually validating and appropriately updating documentation of the decision.

10.8.60.4.2.7  
(07-16-2021)  
**Critical Business  
Processes  
(CBPs)/Critical  
Functions**

- (1) Critical functions have been defined by the IRS Senior Executive team and business representatives as those most critical to the tax administration mission of the IRS supporting the overall continuity of the Federal Government. (IRS-defined)

##  
##  
  
##  
##  
##  
##  
##  
##  
##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##  
##  
  
##  
  
##  
##  
##  
  
##  
##  
##  
##  
##  
##  
##  
##  
##  
##

[illegible]



- (5) Because the RTO must ensure that the MTD is not exceeded, the RTO must be shorter than the MTD. (NIST 800-34: Section 3.2.1)

**Note:** For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.

- (6) COOP functions must be sustained within 12 hours and for up to 30 days from an alternate site; ISCP recovery time objectives are determined by the system-based BIA. (NIST 800-34: Section 3.2.1)
- a. Information systems that support COOP functions must have an RTO that meets COOP requirements.
  - b. Information systems that do not support COOP functions do not require alternate sites as part of the ISCP recovery strategy, but may have an alternate site security control requirement.

- (7) The ISCP Coordinator, working with management, must determine the optimum point (also known as the Cost Balance Point) to recover the information system by balancing the cost of system inoperability against the cost of resources required for restoring the system and its overall support for critical mission/business processes. 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. (NIST 800-34: Section 3.2.1)

**Note:** For example, if the system must be recovered immediately, zero downtime solutions and alternate processing site costs will be much higher, whereas a low-impact system with a longer RTO would be able to implement a less costly simple tape backup system.

- (8) Refer to IRM 10.8.13 for additional guidance regarding BIA.

## 10.8.60.4.3 (07-16-2021) CP-03 Contingency Training

- (1) SRM must be responsible for developing and disseminating training information through IRS IT/FISMA Program Management Office BOD representatives to identified employees. (IRS-defined)
- (2) SRM must establish training in support of the DR program. (IRS-defined)
- (3) The training established by SRM must support annual FISMA security training requirements. (IRS-defined)
- (4) The training established by SRM must be available through the Integrated Talent Management (ITM) system (IRS-defined)

**Note:** ITM is the official IRS system of record for training for all IRS employees.

- (5) For more information on training refer to NIST training publications, NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, and NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. (IRS-defined)

- (6) Refer to IRM 10.8.1, CP-03 or IRM 10.8.24, CP-3 Contingency Training for additional guidance on contingency training.

10.8.60.4.3.1  
(12-24-2013)  
**Disaster Recovery  
Training Guidelines**

- (1) Employees with DR responsibilities must be required to complete DR-focused training each year. (IRS-defined)
- a. Minimum training requirements for Employees with DR responsibilities are documented in IRS IT DR Training Curriculum located at: #
  - b. Additional training must be available through elective courses from the online services provided by IRS, on-the-job training, or through offerings of a private vendor.
  - c. DR training classes or seminars must count toward the employees' annual security training requirement.
- (2) Training hours must be based on employees roles with respect to DR as indicated in the ITSCM Training Curriculum. (IRS-defined)
- (3) Employees/managers must work with their training coordinator to ensure credit is given for classes relating to ITSCM/ISCP. (IRS-defined)

10.8.60.4.3.2  
(12-24-2013)  
**Disaster Recovery  
Certifications**

- (1) Employees with primary or full time DR duties are encouraged to complete formal, vendor-sponsored DR training and tests for DR certification. (IRS-defined)
- a. DR training must count towards the employee's annual security training requirement.
- Note:** Vendor-sponsored refers to vendors that provide training on ITSCM, Business Continuity, and/or ISCP.
- (2) Employees with DR certifications must be required to complete the appropriate number of hours (Continuing Professional Education (CPE)) yearly to maintain their certification. (IRS-defined)
- a. The CPE hours earned must count towards the employees' annual security training requirements.

#  
#

10.8.60.4.3.3  
(12-02-2019)  
**Information System  
Contingency Plan (ISCP)  
Training**

- (1) Training for personnel with contingency plan responsibilities must focus on familiarizing them with ISCP roles and teaching skills necessary to accomplish those roles. Training must be provided at least annually. Personnel newly appointed to ISCP roles must receive training shortly thereafter. (NIST 800-34: Section 3.5.2)
- (2) Recovery personnel must be trained on the following plan elements (NIST 800-34: Section 3.5.2):
- Purpose of the plan
  - Cross-team coordination and communication
  - Reporting procedures
  - Security requirements

	<ul style="list-style-type: none"><li>• Team-specific processes (Activation and Notification, Recovery, and Reconstitution Phases)</li></ul>	
10.8.60.4.4 (07-16-2021) <b>Contingency Plan Testing</b>	<p>(1) IRM 10.8.1 requires exercises or tests of a system's contingency plan capabilities to be conducted at least annually. (IRS-defined)</p> <p>(3) The following areas must be addressed in a contingency plan test, as applicable (NIST 800-34: Section 3.5.1):</p> <ul style="list-style-type: none"><li>• Notification procedures</li><li>• System recovery on an alternate platform from backup media</li><li>• Internal and external connectivity</li><li>• System performance using alternate equipment</li><li>• Restoration of normal operations</li><li>• Other plan testing (where coordination is identified, i.e., COOP, BCP)</li></ul> <p>(4) Guidance and procedures for IT Contingency Tests and Exercises are located in IRM 10.8.62, <i>Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery Test, Training, and Exercise Program</i>. (IRS-defined)</p> <p>(5) Refer to IRM 10.8.1 or IRM 10.8.24 , for additional guidance on Contingency Plan Testing.</p>	# #
10.8.60.4.4.1 (12-02-2019) <b>ISCP Testing, Training, and Exercise</b>	<p>(1) ISCPs must be maintained in a state of readiness, which includes having the following: (NIST 800-34: Section 3.5):</p> <ul style="list-style-type: none"><li>a. Personnel must be trained to fulfill their roles and responsibilities within the plan.</li><li>b. Plans must be exercised to validate their content.</li><li>c. Systems and system components must be tested to ensure their operability in the environment specified in the ISCP.</li></ul> <p>(2) Testing results must be used to assess and report on the overall sustainability of IT Service Continuity within the IRS. Through the evaluation, assessment, or exercise of the ITSCM Program, identified gaps may be mitigated by program changes, proposed investment strategies, process adjustments, or risk acceptance/avoidance/transference options. ISCP TT&amp;E improves the IRS's ability to prepare for, respond to, manage, and recover from adverse events. (NIST 800:34: Section 3.5)</p>	
10.8.60.4.4.2 (07-16-2021) <b>Information System Contingency Plan (ISCP) Exercises</b>	<p>(1) ISCP exercises must consist of Tabletop, Functional Exercises, or DR Test as required based on security availability and additional guidance issued by Director, Security Risk Management. (IRS-defined)</p> <p>(2) Department of the Treasury and OMB ISCP exercise requirements must be based on the FIPS 199 security availability category below: (NIST 800-34: Section 3.5.3)</p>	


#  
#  
#  
#  
#

- (3) For FIPS 199 LOW systems, the tabletop must simulate a disruption, include all main ISCP points of contact, and be conducted by the system owner. (NIST 800-34: Section 3.5.4)
- (4) For FIPS 199 MODERATE systems, the functional exercise must include all ISCP points of contact and be facilitated by the system owner. Exercise procedures must be developed to include an element of system recovery from backup media. (NIST 800-34: Section 3.5.4)
- (5) For FIPS 199 HIGH systems, the full-scale functional exercise must include a system failover to the alternate location. This could include additional activities such as full notification and response of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an alternate location. The test must also include a full recovery and reconstitution of the information system to a known state. (NIST 800-34: Section 3.5.4)
- (6) In addition to the exercise requirements above, an annual tabletop and a functional exercise must be conducted for all systems and applications that support one for more of the IRS critical functions. (IRS-defined)
- (7) Refer to Exhibit 10.8.60-1 for a definition of a tabletop and functional exercise. (IRS-defined)
- (8) Procedures for conducting ISCP Exercises are in IRM 10.8.62. (IRS-defined)
- (9) Additional guidance based on Department of the Treasury, OMB, or IRS requirements are issued by the SRM Director each FISMA period. (IRS-defined)

10.8.60.4.4.3  
(07-16-2021)  
IT Service Continuity  
Management (ITSCM)  
Test

- (1) Owners of FISMA-reportable systems that support a critical function must be required to test the recovery of their system annually. (IRS-defined)
- (3) All FISMA Non-Reportable (FNR) applications are required to have a DRP or disaster recovery planning document(s). As a general rule, applications not covered by any FISMA system or application DRP may develop a DRP-FNR as a general rule. (IRS-defined)
- (4) A tested DRP is a disaster recovery planning document that has been subjected to an evaluation using a DR Test Plan to identify the scope, objectives, and expected results, recovering the system/application using backup

#  
#  
#  
#  
#

data on different equipment or another location. The actual summary results are used to measure the ability of the recovery personnel using the disaster recovery planning document(s) to recover an IT system and its data to full operational status following a disruption. (IRS-defined)

- (5) Procedures for requesting and conducting DR Tests are in IRM 10.8.62. (IRS-defined)
- (6) The test results must be documented in the Summary Report within 30 calendar days after the conclusion of the annual Disaster Recovery Test. (IRS-defined)
  - a. Within 10 business days after finalization, the results must be shared with the Senior Management of the recovery personnel who participated in the Disaster Recovery Test from Enterprise Computing Centers and other Enterprise Operations organizations.
  - b. A copy of the completed documents must be provided to the SRM Test, Training & Exercise team.
- (7) All disaster recovery planning documents must be updated as appropriate based on lessons learned following any conducted tests/exercises. (IRS-defined)
- (8) Refer to IRM 10.8.1, CP-04 or IRM 10.8.24, CP-4 for additional guidance on contingency testing.

## 10.8.60.4.5 (12-02-2019) **CP-06 - Alternate Storage Site**

- (1) The alternate storage site storage location must be located in sufficient distance as to not be affected by a physical incident affecting the area of the production location, but within adequate distance to retrieve stored data/documents per the documented business needs. (IRS-defined)
- (2) Contracted services for retrieval from off premise storage facilities must be based on the system/applications RTO objectives. (IRS-defined)
- (3) Yearly verification must be performed and documented to ensure that: (IRS-defined)
  - a. Backup media are stored at designated alternate storage site locations and readily retrievable.
  - b. The backup/alternate storage site organization/vendor's delivery time is based on the business needs during normal and non-normal prime and non-prime business hours.
  - c. The backup alternate storage site information is documented in the ISCP with the site name and location of the alternate storage site.
- (4) The annual verification must extend to include a review and update of the access control list for the alternate storage site, making note that, in an incident, non-local may be staff called upon to retrieve/receive backup media. (IRS-defined)
- (5) The annual review must also ensure that the offsite copy of the DR plan is current. (IRS-defined)
- (6) Refer to IRM 10.8.1 or IRM 10.8.24, for additional guidance on Alternate Storage Sites.

10.8.60.4.6  
(12-02-2019)  
**CP-07 - Alternate  
Processing Site**

- (1) Alternate Processing sites must be IRS facilities or an approved contractor site. (IRS-defined)
  - a. Contractors may manage/operate some systems. These must be managed in accordance with IRS Security Policy guidance and contractual agreements.
- (2) IRS Enterprise Computing Centers must be the first choice for managing FISMA-reportable systems unless justification warrants a different site. (IRS-defined)
- (3) When selecting fixed-site locations for recovery of IRS FISMA-reportable systems and applications, the time and mode of transportation necessary to move personnel there must be taken into consideration. This is particularly critical if personnel at the potential location do not have the skills necessary to recover/operate the equipment, systems, and applications. (Example: During a widespread disaster, such as that of September 11, 2001, roads and bridges might be closed to vehicles and air transportation might be restricted.) In addition, the fixed site must be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site. (IRS-defined)
- (4) Use or development of designated and potential alternate processing sites must be submitted to and analyzed by the IT, Enterprise Operations, Operational Security Program Management Office. (IRS-defined)
- (5) The alternate processing site must have system security, management, operational, and technical controls that are equal to the production site. Such controls may include firewalls, physical access controls, data controls, and security clearance level of the site and staff supporting the site. (NIST 800-34: Section 3.4.3)

#  
#  
#  
#

- (7) Important Terms: (NIST 800-34: Section 3.4.3)
  - a. Sites categorized by operational readiness are as follows:
 

**Cold Sites** - are typically facilities with basic space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities. No equipment or telecommunications are established or in place. There is sufficient room to house needed equipment to sustain a system's critical functions.

**Note:** Cold sites are least expensive options as an alternate site option though characterized by the longest amount of time for recovery, several days to weeks.

**Warm Sites** - are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. However, the equipment is not loaded with the software or data required to operate the system. Warm sites should have backup media readers that are compatible with the system's backup strategy. Warm sites may not have equipment to run all systems or all components of a system, but rather only enough to operate critical mission/business processes.



**Note:** Warm sites fall in the middle of expense and in the middle of recovery time, as an alternate site.

**Hot Sites** - are locations with fully operational equipment and capacity to quickly take over system operations after loss of the primary system facility. A hot site has sufficient equipment and the most current version of production software installed, and adequate storage for the production system data. Hot sites should have the most recent version of backed-up data loaded, requiring only updating with data since the last backup. In many cases, hot site data and databases are updated concurrently with or soon after the primary data and databases are updated. Hot sites also need a way to quickly move system users' connectivity from the primary site. Hot sites also require having operational support nearly equal to the production.

**Note:** Hot sites are more expensive options as an alternate site option though characterized by short amount of time for recovery.

- b. Hybrid variations are as follows:

**Mobile Sites** - are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.

**Note:** Mobile sites may be delivered to desired location within 24 hours, though time for equipment installation and setup lengthens recovery time.

**Mirrored Sites** - are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

**Note:** Mirrored sites are the most expensive option as an alternate site option though characterized by the shortest amount of time for recovery.

- (8) When the alternate processing site is an approved contractor site, the following elements must be clearly negotiated and stated in an Memorandum of Understanding (MOU) or an SLA (NIST 800-34: Section 3.4.3):

- Contract/agreement duration
- Cost/fee structure for disaster declaration and occupancy (daily usage), administration, maintenance, testing, annual cost/fee increases, transportation support cost (receipt and return of offsite data/supplies, as applicable), cost/expense allocation (as applicable), and billing and payment schedules
- Disaster declaration (i.e., circumstances constituting a disaster, notification procedures)
- Site/facility priority access and/or use
- Site availability
- Site guarantee
- Other clients subscribing to same resources and site, and the total number of site subscribers, as applicable
- Contract/agreement change or modification process
- Contract/agreement termination conditions
- Process to negotiate extension of service

- Guarantee of compatibility
- Information system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software)
- Change management and notification requirements, including hardware, software, and infrastructure
- Security requirements, including special security needs
- Staff support provided/not provided
- Facility services provided/not provided (use of onsite office equipment, cafeteria, etc.)
- Testing, including scheduling, availability, test time duration, and additional testing, if required
- Records management (onsite and offsite), including electronic media and hardcopy
- Service-level management (performance measures and management of quality of information system services provided)
- Work space requirements (e.g., chairs, desks, telephones, personal computers)
- Supplies provided/not provided (e.g., office supplies)
- Additional costs not covered elsewhere
- Other contractual issues, as applicable
- Other technical requirements, as applicable

(9) Refer to IRM 10.8.1, CP-07 or IRM 10.8.24, CP-7 for additional guidance on Alternate Processing Sites. (IRS-defined)

10.8.60.4.7  
(07-16-2021)

**CP-09 System Backup**

- (1) All FISMA-reportable systems and applications and non-applications (as defined by FISMA) must be backed up in a restorable format on a regular basis, encrypted, and stored offsite. (IRS-defined)
- (2) Systems and applications must be frequently backed up in accordance with IRM 10.8.1 frequency requirements. (IRS-defined)
  - a. Refer to IRM 10.8.1, CP-09 or IRM 10.8.24 , CP-9 System Backup for additional guidance on backup frequencies. (IRS-defined)
- (3) Backup frequencies and type of backups must be defined in the Operations/ Customer SLA and documented in applicable SA&A documents. (IRS-defined)
  - a. Frequency and type of backups are based on data criticality and data fluidity. (NIST 800-34: Section 3.4.2)
  - b. Data backup policies may include the following (NIST 800-34: Section 3.4.2):
    - i. Location of stored data
    - ii. File-naming conventions
    - iii. Media rotation frequency
    - iv. Method for transporting data offsite
  - c. Storage media may include the following (NIST 800-34: Section 3.4.2):
    - i. Magnetic disk
    - ii. Tape
    - iii. Optical disks
  - d. Backup methods may include the following (NIST 800-34: Section 3.4.2):
    - i. Electronic vaulting
    - ii. Network storage
    - iii. Tape library systems



- (4) All backup media must be stored offsite. (IRS-defined)
  - a. Data must be backed up at an IRS approved facility and then labeled, packed and transported to the storage facility in accordance with IRM 10.8.1. (NIST 800-34: Section 3.4.2)
  - b. If the data is required for recovery or testing purposes, the IRS contacts the storage facility requesting specific data to be transported to the IRS facility or to an alternate facility designated by the IRS. (NIST 800-34: Section 3.4.2)
  - c. Selection of an offsite storage facility and vendor must include the following considerations (NIST 800-34: Section 3.4.2):
    - i. Geographic area – Distance from the IRS facility and the probability of the storage site being affected by same disaster as the IRS' site must be considered.
    - ii. Accessibility – Length of time of data retrieval upon request must be considered. Consider storage facility's operating hours.
    - iii. Security – Security capabilities of shipping method, storage facility and personnel must meet the data's security requirements.
    - iv. Environment – Physical environmental controls of storage facility must meet the IRS facility's security requirements.
    - v. Cost – Cost of shipping, operational fees, and disaster response/recovery services must be considered.
  - d. Depending on the FIPS 199 impact level, data encryption may be required for protecting system backup information while in transit and at rest to minimize the risk if backup media is lost or stolen. (NIST 800-34: Section 5.4.1)
- (5) All Mobile Media must be encrypted. (IRS-defined)
  - a. Refer to IRM 10.8.1, MP-05 or IRM 10.8.24, MP-5 Media Transport for additional guidance on encryption of mobile media. (IRS-defined)
- (6) Offsite backup storage must be identified and documented in the ISCP with the name of the location and location site. Offsite backup storage must be identified and documented in the ISCP with the name of the location and location site. (IRS-defined)
- (7) Refer to IRM 10.8.1 or IRM 10.8.24, for additional guidance on Information System Backup. (IRS-defined)

10.8.60.4.8  
(07-16-2021)  
**CP-10 System Recovery and Reconstitution**

- (1) In addition to the Recovery and Reconstitution guidance defined within this IRM, requirements for Recovery and Reconstitution must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24, as applicable.

10.8.60.4.8.1  
(12-02-2019)  
**Recovery Phase**

- (1) Recovery Phase activities must focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. (NIST 800-34: Section 4.3)
- (2) When recovering a complex system, recovery procedures must reflect system priorities identified in the BIA. The sequence of activities must reflect the system's MTD to avoid significant impacts to related systems. Procedures must be written in a stepwise, sequential format so system components may be restored in a logical manner. The procedures must also include escalation

instructions to coordinate with other teams where relevant when certain situations occur, such as (NIST 800-34: Section 4.3.1):

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

**Note:** Refer to IRM 10.8.13 for additional guidance regarding BIA.

- (3) The ISCP must provide detailed procedures to restore the information system or components to a known state. Recovery procedures may address the following actions (NIST 800-34: Section 4.3.2):
  - Obtaining authorization to access damaged facilities and/or geographic area
  - Notifying internal and external business partners associated with the system
  - Obtaining necessary office supplies and work space
  - Obtaining and installing necessary hardware components
  - Obtaining and loading backup media
  - Restoring critical operating system and application software
  - Restoring system data to a known state
  - Testing system functionality including security controls
  - Connecting system to network or other external systems
  - Operating alternate equipment successfully
- (4) Effective escalation and notification procedures must 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. (NIST 800-34: Section 4.3.3)
- (5) Refer to IRM 10.8.1 or IRM 10.8.24, CP-10 System Recovery and Reconstitution for additional guidance on information system recovery and reconstitution.

10.8.60.4.8.2  
(12-02-2019)  
**Reconstitution Phase**

- (1) The Reconstitution Phase must define the actions taken to test and validate system capability and functionality. Recovery activities are completed and normal system operations are resumed. (NIST 800-34: Section 4.4)
  - a. Validation of Recovery:
    - i. 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.
    - ii. Validation Data Testing - Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.
    - iii. Validation Functionality Testing - Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.

- b. ISCP Deactivation:
  - i. Notifications - Upon return to normal operations, users must be notified by the ISCP Coordinator (or designee) using predefined notification procedures.
  - ii. 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.
  - iii. Offsite data storage - If offsite data storage is used, procedures must be documented for returning retrieved backup or installation media to its offsite data storage location.
  - iv. Data Backup - As soon as reasonable following reconstitution, the system must be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup must be stored with other system backups and comply with applicable security controls.
  - v. Event Documentation - All recovery and reconstitution events must be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts. An after-action report with lessons learned must be documented and included for updating the ISCP.
  - vi. An announcement with the declaration must be sent to all business and technical contacts.

**Note:** The ISCP Coordinator, in coordination with BODs, IT Operations, SRM and A&I, must determine if the system has undergone significant change and will require reassessment and reauthorization.

- (2) Refer to IRM 10.8.1 or IRM 10.8.24, CP-10 System Recovery and Reconstitution for additional guidance on information system recovery and reconstitution.

10.8.60.4.8.3  
(12-02-2019)  
**Recovery Strategies**

- (1) Contingency strategies, covering backup and recovery, must be created in accordance with FIPS 199 and NIST SP 800-53 to mitigate risks arising from the use of information and information systems in the execution of mission/business processes. (NIST 800-34: Section 3.4)
- (2) Consideration of recovery methods must include the following (NIST 800-34: Section 3.4.1):
  - Commercial contracts with alternate site vendors
  - Reciprocal agreements with internal or external organizations
  - Service-level agreements (SLAs) with equipment vendors
  - Redundant arrays of independent disks (RAID)
  - Automatic failover
  - UPS
  - Server clustering
  - Mirrored systems

## 10.8.60.4.8.4

(10-04-2012)

**Identify Resource Requirements**

- (1) To effectively plan for realistic recovery, an evaluation of the resources required to resume mission/business processes as quickly as possible must be conducted. Necessary resources must be identified and listed in the appropriate sections of the ISCP/disaster recovery planning documents (e.g., facilities personnel, equipment, software, data files, system components, and vital records etc.). (NIST 800-34: Section 3.2.2)

**Note:** Examples of resources that must be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

## 10.8.60.4.8.5

(12-02-2019)

**Identify System Resource Recovery Priorities**

- (1) Developing recovery priorities is the last step and an important output of the BIA process. Utilizing the data gathered during the BIA (such as outage impact, tolerable downtime, resources required, and impact to the critical functions), recovery priorities can be effectively established. The ISCP Coordinator must consider system recovery measures and technologies to meet the resulting information system recovery priority hierarchy. (NIST 800-34: Section 3.2.3)
- (2) The data gathered during the BIA must be used to establish recovery priorities within systems, applications, and the enterprise. (NIST 800-34: Section 3.2.3)
- (3) Refer to IRM 10.8.13 for additional guidance regarding BIA.

## 10.8.60.4.8.6

(12-02-2019)

**Identify Preventive Controls**

- (1) Outage impacts identified in the BIA must be looked at to determine if the impacts may be mitigated or eliminated through preventive measures. Preventive controls or actions, where feasible and cost effective, reduce overall cost and actions that may be required to recover the system after a disruption. Some preventive controls are listed in NIST SP 800-53. Some common measures include: (NIST 800-34: Section 3.3)
  - Generators (e.g., gasoline or diesel-powered) to provide long-term backup power.
  - Fire suppression systems, fire and smoke detectors.
  - Water sensors in computer rooms' ceilings and floors.
  - Uninterruptible power supplies (UPS) to provide short-term backup power for system components including (environmental and safety controls).
  - Air-conditioning systems with adequate excess capacity to prevent failure of certain components, such as a compressor.
  - 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.
  - Frequent scheduled backups including where the backups are stored (onsite or offsite) and how often backup media are recirculated and moved to storage.
- (2) Refer to IRM 10.8.13 for additional guidance regarding BIA.

## 10.8.60.4.8.7

(12-02-2019)

**Equipment Replacement**

- (1) Detailed lists of equipment needs and specifications must be maintained within contingency plans. (NIST 800-34: Section 3.4.4)

- (2) If an IRS information system is damaged or destroyed or if the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. To prepare for equipment replacement, the following strategies exist: (NIST 800-34: Section 3.4.4)
  - a. Vendor Agreements - SLAs with hardware, software, and support vendors must be made for emergency maintenance service and maintained with contingency plans. SLAs must specify the following:
    - i. How quickly the vendor will respond after being notified.
    - ii. Priority of shipment of replacement equipment.
    - iii. Priority status that the IRS will receive from vendor in the event of a catastrophic disaster involving multiple vendor clients.
  - b. Equipment Inventory - IRS equipment may be purchased in advance and stored in inventory or at a warm site. This equipment will need to be reviewed periodically. Such equipment may become obsolete or unsuitable as system technologies and requirements change.
  - c. Existing Compatible Equipment - Agreements made with approved contractor sites, to be used as an Alternate Processing site, must stipulate that similar and compatible equipment will be available for contingency use by the IRS.
- (3) The ISCP coordinator must consider the following factors impacting equipment replacement: (NIST 800-34: Section 3.4.4)
  - a. Purchasing equipment can extend recovery time due to wait time for shipment and setup.
  - b. Storing equipment is expensive but reduces recovery time.
  - c. Availability of transportation may be limited or temporarily halted in the event of a catastrophic disaster.
  - d. Scope of disaster may entail mass equipment replacement and transportation delays that would extend the recovery period.

10.8.60.4.8.8  
(12-02-2019)  
**Cost Considerations**

- (1) The ISCP Coordinator must ensure that the strategy chosen can be implemented effectively with available personnel and financial resources. (NIST 800-34: Section 3.4.5)
- (2) The ISCP Coordinator must perform cost-benefit analysis of vendor, hardware, software, travel/shipping, labor/contractor, testing and supply costs for each of the following: (NIST 800-34: Section 3.4.5)
  - a. Alternate Site
    - i. Cold Site
    - ii. Warm Site
    - iii. Hot Site
  - b. Offsite Storage
    - i. Commercial
    - ii. Internal
  - c. Equipment Replacement
    - i. SLA
    - ii. Storage
    - iii. Existing Use

- 10.8.60.4.9  
(12-02-2019)  
**Access and Requests for IS Contingency/Disaster Recovery Information**
- (1) The ISCP contains potentially sensitive operational and personnel information. Its distribution must be marked accordingly and controlled. (NIST 800-34: Section 3.6)
    - a. Only employees or non-IRS individuals with an authorized need to know must view or receive documentation relating to ISCPs or disaster recovery planning documents.
  - (2) Requests for ISCP or DR data must be handled by the owner of the document/data. (IRS-defined)
    - a. Requests must be in writing and include sufficient information to determine type of documents requested, purpose/need and requestor's information/position.
- 10.8.60.4.9.1  
(12-24-2013)  
**Internal Information Requests**
- (1) Only system administrators, managers, or other individuals with responsibility for IT Contingency or ITSCM must have access to or copies of applicable ISCPs and/or disaster recovery planning documents. (IRS-defined)
  - (2) System administrators, managers, or other individuals with responsibility for IT Contingency or ITSCM must be provided copies of or access to system and application ISCPs and/or disaster recovery planning documents by their management or the system or application owner. (IRS-defined)
  - (3) Requests for copies of or access to system and application ISCPs and/or disaster recovery planning documents must be made through the employees' manager to the system and/or application owner. (IRS-defined)
  - (4) All other requests for copies of, or access to, system and application ISCPs and/or disaster recovery planning documents must be requested from the system or application owner. The request must specify what is being requested, purpose, contact person, and where the copy is to be sent. (IRS-defined)
- 10.8.60.4.10  
(12-24-2013)  
**Hosting Non-IRS Agencies for Disaster Recovery**
- (1) IRS allows, and currently has, a number of existing DR/Business Continuity/Continuity of Operations Plan agreements in place with other federal Government agencies, allowing them to house DR equipment within IRS facilities. (IRS-defined)
  - (2) A MOU must be prepared that specifically outlines the IRS and the other Agency's responsibilities. (IRS-defined)
  - (3) For information regarding the hosting of non-IRS Agencies, the appropriate Real Estate & Facilities Management team must be contacted. (IRS-defined)
  - (4) The SRM must have no regulatory control or responsibility for the hosting of non-IRS Agency equipment or staff within IRS space. (IRS-defined)
- 10.8.60.4.11  
(12-02-2019)  
**Technical Contingency Planning Considerations**
- (1) Technical Contingency Planning Considerations complement the process and framework guidelines presented in earlier subsections by discussing technical contingency planning considerations for specific types of information systems (NIST 800-34: Chapter 5):
    - Client/server systems
    - Telecommunications systems



- Mainframe systems

10.8.60.4.11.1  
(12-02-2019)

## Common Considerations

- (1) Encryption is most effective when applied to both the primary data storage device and on backup media going to an offsite location. Media readers (e.g., tape drives, CD or DVD readers) should be available at the alternate site location to correctly read the encrypted data during recovery efforts. The cryptographic key and the encryption software should both be available to the new system at the alternate processing site, along with the keying material. (NIST 800-34: Section 5.1.2)
- (2) The following common backup methods must be considered (NIST 800-34: Section 5.1.2):
  - a. Full - A full backup captures all files on the disk or within the folder selected for backup.
    - i. Because all backed-up files are recorded to a single media or media set, locating a particular file or group of files is simple.
    - ii. The time required to perform a full backup can be lengthy.
  - b. Incremental - An incremental backup captures files that were created or changed since the last backup, regardless of backup type.
    - i. Incremental backups afford more efficient use of storage media, and backup times are reduced.
    - ii. To recover a system from an incremental backup, media from different backup operations may be required.

**Note:** For example, consider a case in which a directory needs to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backups would be needed to restore the entire directory.

  - c. Differential - A differential backup stores files that were created or modified since the last full backup.
    - i. If a file is changed after the previous full backup, a differential backup will save the file each time until the next full backup is completed.
    - ii. A differential backup takes less time to complete than a full backup.
    - iii. Restoring from a differential backup may require fewer media than an incremental backup because only the full backup media and the last differential media would be needed.
    - iv. Differential backups take longer to complete than incremental backups because the amount of data since the last full backup increases each day until the next full backup is executed.
- (3) In developing a system backup policy, the following questions must be considered (NIST 800-34: Section 5.1.2):
  - Where and how will media be stored?
  - What data should be backed up and how often should the data be backed up?
  - How quickly are the backups to be retrieved in the event of an emergency?
  - Who is authorized to retrieve the media?
  - Where will the media be delivered and what is the rotation schedule of backup media?

- Who will restore the data from the media?
  - What is the media-labeling scheme?
  - How long will the backup media be retained?
  - When the media are stored onsite, what environmental controls are provided to preserve the media?
  - What is the appropriate backup medium for the types of backups to be performed?
- (4) Certain factors should be considered when choosing the appropriate backup solution (NIST 800-34: Section 5.1.2):
- a. Equipment interoperability - To facilitate recovery, the backup device should be compatible with the platform operating system and applications and should be easy to install onto different models or types of systems.
  - b. Storage volume - To ensure adequate storage, the amount of data to be backed up should determine the appropriate backup solution.
  - c. Media life - Each type of medium has a different use and storage life beyond which the media cannot be relied on for effective data recovery.
  - d. Backup Software - When choosing the appropriate backup solution, the software or method used to back up data should be considered.
- (5) Use of high availability (HA) processes to provide for online real-time resilient access to alternate system resources should be considered. HA denotes systems that can achieve an uptime of 99.999 percent or better. (NIST 800-34: Section 5.1.6)
- Note:** HA is a process for achieving high availability and should not be confused with FIPS 199 high-impact category systems.
- (6) A system should be resilient to environmental and component-level failures. The following strategies for protection of resources should be considered (NIST 800-34: Section 5.1.3):
- a. Critical hardware, such as servers, should be configured with dual power supplies that are used simultaneously. If the main power supply becomes overheated or unusable, the second unit will become the main power source, resulting in no system disruption.
  - b. If high availability is required, a gas- or diesel-powered generator must be used as part of a UPS/generator system support system. The generator can be wired directly into the site's power system and configured to start automatically when a power interruption is detected. Fuel availability should be considered.
  - c. Software and software licenses should be stored in an alternate location.
    - i. Original installation media
      - a) License terms and conditions
      - b) License keys
    - ii. Image loads for client systems (such as desktops and portable systems)
      - a) Documentation of the software included in the image load
      - b) Configuration information for the type of computer for which the image is intended
      - c) Installation instructions
  - d. When third-party vendors are used to recover data from failed storage devices, proper security vetting of the service provider must be



conducted before turning over equipment. The service provider and its employees must do the following:

- i. Sign non-disclosure agreements
- ii. Be properly bonded
- iii. Adhere to IRS-specific security policies

10.8.60.4.11.2  
(12-02-2019)

## Client/Server Systems

- (1) Client/server systems can have processing and data at both the server and client workstation levels. (NIST 800-34: Section 5.2)
  - a. Client workstations are normally desktop computers, along with portable devices such as laptops, notebook computers, and handheld devices (e.g., smart phones and specialized equipment such as inventory collection bar code readers).
  - b. Wireless and smart phone technology advances have allowed users access to key server functionality and services such as email from their mobile phones. This is normally done by using proprietary third-party software that establishes the communications and data transfer to and from the phone via the network provided by mobile cell carriers.
  - c. Servers support file sharing and storage, data processing, central application hosting (such as email or a central database), printing, access control, user authentication, remote access connectivity, and other shared system services. Local users log into the server through networked client machines to access resources that the server provides.

10.8.60.4.11.2.1  
(12-02-2019)

## Client/Server Systems Contingency Considerations

- (1) Backup of data must be automated for servers for client/server systems. (NIST 800-34: Section 5.2.1)
  - a. Refer to IRM 10.8.1, CP-09 or IRM 10.8.24, CP-9 System Backup for additional guidance on information system backups.
- (2) Hardware, software, and peripherals must be standardized. (NIST 800-34: Section 5.2.1)

**Note:** IRS Enterprise Architecture (EA) Enterprise Standards Profile (ESP) dictates the official products and versions of software within the IRS. Enterprise Archi-

#  
#

- (3) The amount of data stored on a client computer must be minimized. Critical user data must be stored on central servers that are backed up as part of an organization's enterprise backup strategy, rather than on the client computer hard drive. (NIST 800-34: Section 5.2.1)
- (4) The IRS must provide guidance to users on saving data on client computers (e.g., particular folders). (NIST 800-34: Section 5.2.1)
- (5) Refer to subsection Telecommunications Contingency Considerations in this IRM for further contingency considerations for servers for client/server systems. Servers must have the same contingency considerations as telecommunications. (NIST 800-34: Section 5.2.1)
  - a. Document system configurations and vendor information.
  - b. Coordinate with security policies and system security controls.

- c. Use results from the BIA.

**Note:** Refer to IRM 10.8.13 for additional guidance regarding BIA.

10.8.60.4.11.2.2  
(12-02-2019)

**Client/Server Systems  
Contingency Solutions**

- (1) Client/server system data backups can be accomplished in various ways, including the following (NIST 800-34: Section 5.2.2):
  - a. Digital video disc (DVD) - DVDs are low-cost storage media and have a higher storage capacity of around 4.7 gigabytes (GB). To read from a DVD-ROM, the operating system's file manager is sufficient; to write to a DVD-ROM, a rewritable DVD (DVD-RW) drive and the appropriate software are required.
  - b. Network Storage - Data stored on networked client/server systems can be backed up to a networked disk. The amount of data that can be backed up from a client/server system is limited by the network disk storage capacity or disk allocation to the particular user. If users are instructed to save files to a networked disk, the networked disk itself must be backed up through the network or server backup program. Common types of network storage architecture include network attached storage (NAS) and storage area network (SAN). These storage systems incorporate resiliency and redundancy within their design and can be configured to maintain redundancy across several locations.
  - c. External Hard Drives - Data replication or synchronization to an external hard drive is a common backup method for portable computers and stand-alone devices. Many external hard drives have backup software included for use in backing up primary drives.
  - d. Internet Backup - Internet Backup, or Online Backup, is a commercial service that allows desktop and portable device users to back up data to a remote location over the Internet for a fee. A utility is installed onto the desktop or portable device that allows the user to schedule backups, select files and folders to be backed up, and establish an archiving scheme to prevent files from being overwritten. Data can be encrypted for transmission; however, this will impede the data transfer. The advantage of Internet Backup is that the user is not required to purchase data backup hardware or media and that the data is readily available to be downloaded for recovery in a contingency situation.
- (2) The remotely hosted storage services must provide the same level of protection of data as the original site. (NIST 800-34: Section 5.2.2)
- (3) Refer to IRM 10.8.1, CP-09 or IRM 10.8.24 , CP-9 System Backup for additional guidance on information system backups.

10.8.60.4.11.3  
(12-02-2019)

**Telecommunications  
Contingency  
Considerations**

- (1) Telecommunications networks should be documented. (NIST 800-34: Section 5.3.1)
  - a. Physical diagrams should display up-to-date physical layouts of facilities that house LAN/WANs.
  - b. Physical diagrams should display up-to-date cable jack numbers.
  - c. Physical diagrams should display up-to-date network- connecting devices, IP addresses, Domain Name System (DNS) names, and types of communications links and vendors.
  - d. Logical diagrams should display up-to-date telecommunications infrastructure and its nodes.

- (2) Vendors and communication providers must be documented. (NIST 800-34: Section 5.3.1)
  - a. Configurations of network connective devices that facilitate telecommunication (e.g., circuits, switches, bridges, and hubs) must be documented.
  - b. Vendors and their contact information must be documented to provide for prompt hardware and software repair or replacement.
  - c. Communications providers, including POC and contractual or SLA information, must be documented.
- (3) Telecommunications contingency solutions must have system security, management, operational, and technical controls set that are equal to that of counterpart telecommunications networks in production. (NIST 800-34: Section 5.3.1)
- (4) The BIA must be reviewed to determine telecommunications recovery priorities. The BIA must identify the high-availability FIPS 199 impact levels for any data networks and email that support COOP Mission, Primary, or National Essential Functions. (NIST 800-34: Section 5.3.1)

**Note:** Refer to IRM 10.8.13 for additional guidance regarding BIA.

10.8.60.4.11.3.1  
(12-02-2019)  
**Telecommunications  
Contingency Solutions**

- (1) Single points of failure must be identified. (NIST 800-34: Section 5.3.2)
  - a. Threats to the cabling system, such as cable cuts, electromagnetic and radio frequency interference must be considered. Redundant cables may be installed when appropriate.
  - b. Damage resulting from fire, water, and other hazards must be considered.
- (2) Redundancy in critical components must be implemented. Contingency solutions must be developed for each device based on its BIA criticality. The following redundancy strategies must be considered (NIST 800-34: Section 5.3.2):
  - a. Redundant communications links, to ensure that the links have physical separation and do not follow the same path
  - b. Redundant network service providers
  - c. Redundant hubs, switches, routers, and bridges
  - d. Redundancy from network service providers (NSPs) or internet service providers (ISPs)

**Note:** Refer to IRM 10.8.13 for additional guidance regarding BIA.

- (3) Telecommunications networks must be monitored. (NIST 800-34: Section 5.3.2)
  - a. The monitoring software issues an alert (e.g., an electronic page or email) if a node or connection begins to fail or is not responding.
  - b. SLAs can facilitate prompt recovery following software or hardware problems associated with the telecommunications.
    - i. An SLA also may be developed with the NSP or ISP to guarantee the desired network availability and establish tariffs if the vendor's network is unavailable.

ii. If the NSP or ISP is contracted to provide network-connecting devices, such as routers, the availability of these devices must be included in the SLA.

- (4) Remote access and wireless local area network technology must be integrated. (NIST 800-34: Section 5.3.2)
  - a. If an emergency or serious system disruption occurs, remote access may serve as an important contingency capability by providing access to organization-wide data for recovery teams or users from another location. Refer to AC-17 Remote Access in IRM 10.8.1 or IRM 10.8.24 for additional guidance on remote access.
  - b. Wireless (or WiFi) local area networks can serve as an effective contingency solution to restore network services following a wired LAN disruption. Refer to AC-18 Wireless Access in IRM 10.8.1 or IRM 10.8.24 for additional guidance on wireless access.

10.8.60.4.11.4  
(12-02-2019)

#### Mainframe Systems

- (1) Refer to IRM 10.8.33, Information Technology (IT) Security, *Mainframe System Security Policy*, for addition guidance on mainframes.

10.8.60.4.11.4.1  
(12-02-2019)

#### Mainframe Contingency Solutions

- (1) Redundant system components are critical to ensure that a failure of a system component, such as a power supply, does not cause a system failure. (NIST 800-34: Section 5.4.2)
- (2) UPS and power monitoring and management systems must be used to ensure that power fluctuation will not affect the mainframe. Because mainframes typically process large critical applications, a long-term backup power solution may be needed. A gas or diesel generator can ensure that mainframe processing is not interrupted by a power outage. (NIST 800-34: Section 5.4.2)
- (3) Disk redundancy can be provided for the direct access storage devices (DASDs) by implementing a RAID solution. (NIST 800-34: Section 5.4.2)
- (4) Each mainframe architecture is unique and centralized. (NIST 800-34: Section 5.4.2)
  - a. A replacement system must be available at an alternate warm or hot site.
  - b. Vendor-support contracts must be maintained to support repairs of damaged units.

**Note:** The General Services Administration's Federal Technology Service Federal Computer Acquisition Center has a government-wide acquisition contract on behalf of the federal government. The program has been in place since 1993 and provides disaster recovery services to more than forty federal organizations.

- c. Vendor SLAs must be kept up to date and reviewed to ensure that the vendor provides adequate support to meet system availability requirements.
- (5) Backup and retention schedules for mainframes must be based on the criticality of the data being processed and the frequency that the data is modified. (NIST 800-34: Section 5.4.2)
  - a. Remote journaling or electronic vaulting to the alternate site must be considered for implementation.

- b. Disk replication, virtualization, or NAS or SAN technologies that replicate various platforms to one replicating server must be considered for implementation.

**This Page Intentionally Left Blank**

**Exhibit 10.8.60-1 (12-02-2019)**  
**Glossary and Acronyms**

Term	Definition or Description
<b>A&amp;I</b>	Architecture and Implementation
<b>ABM</b>	Authorization Boundary Memo
<b>ACIO</b>	Associate Chief Information Officer
<b>AEA</b>	Architecture and Engineering Advisory
<b>Alternate Processing Site (APS)</b>	Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Bureau-defined information system operations] for essential missions/ business functions within [Bureau-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable
<b>AO</b>	Authorizing Official
<b>Authorization Boundary Memo (ABM)</b>	Documents the authorization boundary and SA&A scope of the system.
<b>Backup</b>	The process of duplicating and storing the files and programs of an IT system on another medium or device to facilitate complete restoration of the system Mainframe System Security Policy and its data following a disruption.
<b>BC</b>	Business Continuity
<b>BIA</b>	Business Impact Analysis
<b>BOD</b>	Business Operating Division
<b>BU</b>	Business Unit
<b>Business Continuity</b>	Business Continuity is a collection of strategies and specialized plans that ensures a local IRS site can continue to manage efficiently and operate optimally in response to an impending/ actual incident without significant impact to overall IRS client services.
<b>Business Continuity Plan (BCP)</b>	The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. NIST 800-34, <i>Contingency Planning Guide for Federal Information Systems</i> , Rev 1, Errata Nov 1, 2010. In addition per IRM 10.6.1, <i>Continuity Operations Program, Overview of Continuity Planning</i> , states the BCP is an ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity operations through personnel training, plan tests, and maintenance.

## Exhibit 10.8.60-1 (Cont. 1) (12-02-2019)

## Glossary and Acronyms

Term	Definition or Description
<b>Business Impact Analysis (BIA)</b>	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
<b>CBP</b>	Critical Business Process
<b>Critical Infrastructure Protection (CIP)</b>	Addresses the security, protection, and resiliency of those components of the national infrastructure critical to national and economic security.
<b>Critical Infrastructure Protection (CIP) Assessment</b>	A methodical review of an organization's resources, services, and functions to determine those that are nationally critical.
<b>CMMI</b>	Capability Maturity Model Integration
<b>CO</b>	Contracting Officer
<b>Cold Site</b>	A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.
<b>Components</b>	Information System components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Information system components are either purchased commercially off-the-shelf or are custom-developed.
<b>Continuity of Operations Plan (COOP)</b>	The COOP focuses on restoring an organization's (usually a headquarters element) essential functions at an alternate site performing those functions for up to 30 calendar days before returning to normal operations. Because a COOP addresses headquarters-level issues, it is developed and executed independently from the business continuity plan. Standard elements of a COOP include Delegation of Authority statements, Orders of Succession, and Vital Records and Databases. Minor disruptions that do not require relocation to an alternate site are typically not addressed. However, the COOP may include the business continuity plan, business resumption plan, and disaster recovery plan as appendices.
<b>Contingency Planning</b>	The process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively impacts the organization.
<b>Continuity Plan</b>	Refer to Business Continuity Plan.



## Exhibit 10.8.60-1 (Cont. 2) (12-02-2019)

### Glossary and Acronyms

Term	Definition or Description
<b>Continuity of Support Plan</b>	OMB Circular A-130, Appendix III, requires the development, maintenance, and periodic tests of continuity of support plans for general support systems and contingency plans for major applications (referred to as systems and applications in this IRM). Because an ISCP is developed for each major application and general support system (or FISMA-reportable system and/or application), multiple contingency plans may be maintained within the organization's business continuity plan.
<b>COOP</b>	Continuity of Operations Plan
<b>COR</b>	Contracting Officer's Representative
<b>CP</b>	Contingency Planning
<b>CPE</b>	Continuing Professional Education
<b>Critical Business Process (CBP)/ Critical Functions</b>	IRS business processes defined by the IRS Business Units that are the most critical to the tax administration mission of the IRS and the Federal Government.
<b>Critical Infrastructure Protection (CIP)</b>	Addresses the security, protection, and resiliency of those components of the national infrastructure critical to national and economic security.
<b>Critical Infrastructure Protection (CIP) Assessment</b>	A methodical review of an organization's resources, services, and functions to determine those that are nationally critical.
<b>CSMW</b>	Computer Security Material Weakness
<b>DHS</b>	Department of Homeland Security
<b>DASD</b>	Direct Access Storage Device
<b>Disaster Recovery</b>	The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.
<b>Disaster Recovery Capability Analysis Report</b>	An analysis of the IRS's Disaster Recovery capability, identifying IT systems that are certified and accredited, have disaster recovery planning documents, have tested disaster recovery planning documents, and are backed up.
<b>Disaster Recovery Plan (DRP)</b>	A plan created and maintained by IT or any information technology service provider that defines the resources, roles, responsibilities, actions, tasks, and the steps required, down to a key step level, to restore an IT system to its full operational status at the current or alternate facility after a disruption. The DRP can be a part of the ISCP, a standalone document, or separate disaster recovery keystroke procedures.

**Exhibit 10.8.60-1 (Cont. 3) (12-02-2019)**  
**Glossary and Acronyms**

<b>Term</b>	<b>Definition or Description</b>
<b>Disaster Recovery Test</b>	Full-scale functional exercise that involves recovering the system and/or application on non-production equipment, simulated environment, or at the alternate processing site.
<b>Disruption</b>	An unplanned event that causes an information system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
<b>DRP</b>	Disaster Recovery Plan/ Detailed Recovery Plan
<b>DRWG</b>	Disaster Recovery Working Group
<b>EA</b>	Enterprise Architecture
<b>ECP</b>	Emergency Communication Plan
<b>ELC</b>	Enterprise Life Cycle
<b>ELMS</b>	Enterprise Learning Management System
<b>EOPS</b>	Enterprise Operations
<b>ERC</b>	Employee Resource Center
<b>ERM</b>	Enterprise Risk Management
<b>ESA</b>	Essential Supporting Activity
<b>ESP</b>	Enterprise Standards Profile
<b>Exercise</b>	A people-focused activity designed to execute one or more portions of a business continuity plan and evaluate the performance against approved standards or objectives. Through the exercise, validate the viability of one or more aspects of a Business Resumption Plan, Disaster Recovery Plan or IT Contingency Plan.
<b>FCD</b>	Federal Continuity Directive
<b>Federal Information Security Modernization Act of 2014 (FISMA)</b>	FISMA, among other things, amends Chapter 35 of title 44, United States Code, adding a new sub chapter: "SUBCHAPTER III — INFORMATION SECURITY" which provides additional security requirements on Federal Agencies.
<b>FIPS</b>	Federal Information Processing Standard
<b>FISMA</b>	Federal Information Security Modernization Act
<b>FISMA Master Inventory</b>	A record of IRS General Support Systems, Major Applications, and other applications as defined by FISMA guidelines.
<b>FISMA Non-Reportable (FNR)</b>	Applications not covered by any FISMA-reportable system or application.
<b>FISMA Period</b>	July 1 through June 30 of the following year.

## Exhibit 10.8.60-1 (Cont. 4) (12-02-2019)

### Glossary and Acronyms

Term	Definition or Description
<b>FISMA Reportable System and/or Application</b>	Systems or applications included in the FISMA Master Inventory. This term generally replaces <i>general support system</i> .
<b>FNR</b>	FISMA Non-Reportable
<b>FP</b>	Facility Plan
<b>FPS</b>	Federal Protection Service
<b>Functional Exercise</b>	Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner. (NIST SP 800-34).
<b>GAO</b>	Government Accountability Office
<b>General Support System (GSS)</b>	A <i>general support system</i> or <i>system</i> means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).
<b>GSS</b>	General Support System; see FISMA-reportable System and/or Application.
<b>HAZMAT</b>	Hazardous Materials
<b>Hot Site</b>	A fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption.
<b>HSPD</b>	Homeland Security Presidential Directive
<b>I/O</b>	Input/Output
<b>IBM</b>	Internal Business Machines
<b>IG</b>	Inspector General

**Exhibit 10.8.60-1 (Cont. 5) (12-02-2019)**  
**Glossary and Acronyms**

<b>Term</b>	<b>Definition or Description</b>
<b>IMP</b>	Incident Management Plan
<b>Impact</b>	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.
<b>Impact Level</b>	High, Moderate, or Low security categories of an information system established in FIPS 199 which classify the intensity of a potential impact that may occur if the information system is jeopardized.
<b>Incident Management Plan</b>	The Incident Management Plan is a site's specific plan that focuses on the command and control, coordination activities, and management of a disruption at any IRS site.
<b>Incident Response Plan</b>	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber attacks against an organization's information system(s).
<b>Information System</b>	A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
<b>IPSO</b>	Information Processing Service Organization
<b>Information System Contingency Plan (ISCP)</b>	Documents created and maintained by IT, Cybersecurity, and system owners that provide procedures and capabilities for recovering an information system and define the resources, roles, responsibilities, and procedures for recovering a single information system after a disruption.
<b>ISCP</b>	Information System Contingency Plan
<b>IT</b>	Information Technology
<b>ITDRO</b>	IT Disaster Recover Organization
<b>ITIL</b>	Information Technology Infrastructure Library
<b>Keystroke Recovery (KR)</b>	Detailed step-by-step instructions, including keystroke-by-keystroke details, to restore an IT system to its full operational status following a disruption.
<b>LAN</b>	Local Area Network
<b>Major Application</b>	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. (OMB Circular A-130, Appendix III) Major applications are part of the FISMA Master Inventory.

## Exhibit 10.8.60-1 (Cont. 6) (12-02-2019)

### Glossary and Acronyms

Term	Definition or Description
<b>Maximum Tolerable Downtime (MTD)</b>	The maximum amount of time a business can tolerate the outage of a critical business function. MTD is sometimes referred to as Maximum Tolerable Outage (MTO).
<b>MEF</b>	Mission Essential Functions
<b>MI</b>	Master Inventory
<b>MOU</b>	Memorandum of Understanding
<b>MTD</b>	Maximum Tolerable Downtime
<b>NCS</b>	National Communications System
<b>NEF</b>	National Essential Functions
<b>NIPP</b>	National Infrastructure Protection Plan
<b>NIST</b>	National Institute of Standards and Technology
<b>NSP</b>	Network Service Provider
<b>NSPD</b>	National Security Presidential Directive
<b>Occupant Emergency Plan (OEP)</b>	Provides a set of response procedures and actions taken during the onset of an emergency to minimize the impact of the incident. It includes building evacuation, shelter in place, and employee safety procedures.
<b>OMB</b>	Office of Management and Budget
<b>OneSDLC</b>	One Solution Delivery Lifecycle
<b>PM COMP</b>	Contingency Management Plan for Planned Maintenance Projects
<b>PMBOK</b>	Project Management Body of Knowledge
<b>PMEF</b>	Primary Mission Essential Function
<b>PMI</b>	Project Management Institute
<b>POA&amp;M</b>	Plan of Action & Milestones
<b>POC</b>	Point of Contact
<b>RAID</b>	Redundant arrays of independent disks
<b>Reciprocal Agreement</b>	An agreement that allows two organizations to back up each other.

## Exhibit 10.8.60-1 (Cont. 7) (12-02-2019)

## Glossary and Acronyms

Term	Definition or Description
<b>Recovery Point Objective (RPO)</b>	The point in time, prior to a disruption or system outage (e.g., end of previous day's processing) to which data can be recovered (given the most recent backup copy of the data) 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 might need to be recreated after the systems or functions have been recovered. RPO factors how much data will be lost based on the date of the last backup.
<b>Recovery Time Objective (RTO)</b>	The length of time an information system component can be in the recovery phase before negatively impacting the organization's mission or mission/business functions. RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.
<b>Resilience</b>	The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.
<b>Risk Analysis/Assessment</b>	Process of identifying risks/vulnerabilities to an organization, assessing critical functions necessary to continue business operations, defining controls in place to reduce exposure to risk, and evaluating cost for such controls.
<b>Risk-Based Decisions</b>	Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase and decision is made taking entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis, assessments, recommended risk mitigation strategies, and business impact. (This list is not intended to be all inclusive).
<b>RMF</b>	Risk Management Framework
<b>RMP</b>	Risk Management Plan
<b>SA&amp;A</b>	Security Assessment & Authorization
<b>SC</b>	Service Continuity
<b>Scenario</b>	A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives.

## Exhibit 10.8.60-1 (Cont. 8) (12-02-2019)

### Glossary and Acronyms

Term	Definition or Description
<b>Security Controls</b>	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
<b>Single Point of Failure (SPOF)</b>	Identified within the critical function using the following criteria: [Location: A critical function is conducted in only one location]; [IT Systems: IT system located in only one location]; [Unique Employee Skills: A critical function relies on a small set of people with unique knowledge, skills or abilities]; [Third Parties/Vendors: A critical function depends on a third party to complete the process]; [Vital Records: a critical function depends on paper (non-electronic) vital records to complete the process].
<b>SL</b>	Service Level
<b>SLA</b>	Service Level Agreement
<b>SLO</b>	Service Level Objective
<b>SLR</b>	Service Level Requirement
<b>SOP</b>	Standard Operating Procedure
<b>SRM</b>	Security Risk Management
<b>System Development Life Cycle (SDLC)</b>	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.
<b>Tabletop Exercise</b>	A discussion-based exercise where personnel with roles and responsibilities in a particular plan (ISCP, DRP or disaster recovery planning documents, or CP) meet to validate the content of the plan in the context of a particular emergency situation.
<b>TAF</b>	Trusted Agent FISMA
<b>Test</b>	In the context of DR, a test is the method used to evaluate the organization's readiness and ability to recover a system from varying degrees of non-functioning to its original functional state by following authorized ISCP/DR keystroke procedures.
<b>TIGTA</b>	Treasury Inspector General for Tax Administration



## Exhibit 10.8.60-1 (Cont. 9) (12-02-2019)

## Glossary and Acronyms

Term	Definition or Description
<b>Toolkit Suite with Command Centre (TSCC)</b>	IRS enterprise-level repository and incident management decision support tool and plan repository for Business Continuity and Disaster Recovery. These plans include, but are not limited to: IS Contingency Plans (ISCPs); Disaster Recovery Plans (DRPs) or other disaster recovery planning documents; Facility Plans (FPs), Business Continuity Plans (BCPs); Occupant Emergency Plans (OEPs), Emergency Communication Plans (ECPs); pandemic and other Vector Plans (VPs).
<b>TSCC</b>	Toolkit Suite with Command Centre
<b>TT&amp;E</b>	Testing, Training, and Exercises; also Test, Exercise, and Evaluation
<b>UPS</b>	Uninterrupted Power Supply
<b>UWR</b>	Unified Work Request
<b>Vital Records</b>	Records in either electronic or non-electronic format that are needed to meet operational responsibilities and perform essential functions under national security emergencies and/or disaster conditions; and protect the legal and financial rights of the Government and those affected by the Government. Examples of vital records include the continuity of operations plan and other emergency plans and directives, staffing assignments, policy documents, selected program records, contracting and acquisition files, personnel files, insurance files, orders of succession, delegations of authority, and contact information.
<b>WAN</b>	Wide Area Network
<b>Warm Site</b>	An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.
<b>Work Recovery Time (WRT)</b>	The period of time within which critical business functions are recovered and running once the systems are restored.



# IT Service Continuity Management (ITSCM) Policy and Guidance 10.8.60

page 59

Exhibit 10.8.60-2 (12-02-2019)

## References

### IRS Publications

- IRM 10.6.1 - *Continuity Operations Program, Overview of Continuity Planning*
- IRM 10.8.1 – *Information Technology (IT) Security, Policy and Guidance*
- IRM 10.8.2 – *Information Technology (IT) Security, IT Security Roles and Responsibilities*
- IRM 10.8.13 - *Information Technology (IT) Security, Business Impact Analysis (BIA) Security Policy*
- IRM 10.8.24 - *Information Technology (IT) Security, Cloud Computing Security Policy*
- IRM 10.8.33 - *Information Technology (IT) Security, Mainframe System Security Policy*
- IRM 10.8.62 – *Information Technology (IT) Security, Information Systems Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program*
- IRM 10.9.1 - *Classified National Security Information (CNSI)*
- Business Impact Analysis (BIA) Project site:

- IRS Enterprise Life Cycle site:

- Security Risk Management, DR Compliance site:

- Security Risk Management, FISMA site:

- Security Risk Management, IRS IT Disaster Recovery Training Curriculum site:

#  
#  
#  
#  
#

### Department of the Treasury

- TD P 85–01, Version 3.1.3 *Treasury Information Technology (IT) Security Program*, February 28, 2022.

### National Institute of Standards and Technology (NIST) Publications

- NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* February 2004.
- NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* March 2006.
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.
- NIST SP 800-34 Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010 (Errata page - Nov. 11, 2010).
- NIST SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, September 20, 2018
- NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.
- NIST SP 800-53 Rev 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 20, 2020 (includes updates as of December 10, 2020).
- NIST SP 800-53A Rev 5, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, January 2022.
- NIST SP 800-60 Vol 1 Rev 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

**Exhibit 10.8.60-2 (Cont. 1) (12-02-2019)****References****Other Publications**

- *E-Government Act of 2002* (Public Law 107-347), Title III, Federal Information Security Management Act of 2002 (FISMA).
- Department of Homeland Security, *DHS Risk Lexicon*, September 2010.
- Department of Homeland Security, Federal Emergency Management Agency, Federal Continuity Directive 1 (FCD-1), *Federal Executive Branch National Continuity Program and Requirements*, January 17, 2017.
- Department of Homeland Security, Federal Continuity Directive 2 (FCD 2), Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process, dated June 13, 2017.
- *Information Technology Management Reform Act of 1996* (Public Law 104-106), August 1996.
- Office of Management and Budget, Circular A-11, *Preparation, Submission, and Execution of the Budget*, July 2014.
- Office of Management and Budget, Circular A-130, Transmittal Memorandum #4, *Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources*, July 28, 2016.