



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.8.62

JANUARY 18, 2024

## EFFECTIVE DATE

(01-18-2024)

## PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.62, *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program*.

## MATERIAL CHANGES

- (1) 10.8.62.1, Program Scope and Objectives - Subsection updated to align with standard security policy language.
- (2) 10.8.62.1.1.1, Scope - Subsection removed to align with standard security policy language and IRM 1.11.2.2.4 .
- (3) 10.8.62.1.1.2, Objectives - Subsection removed to align with standard security policy language and IRM 1.11.2.2.4 .
- (4) 10.8.62.1.2, Authority - Subsection updated to align with standard security policy language.
- (5) 10.8.62.1.3, Roles and Responsibilities - Subsection relocated from 10.8.62.2 to align with standard security policy language and IRM 1.11.2.2.4.
- (6) 10.8.62.1.3.1, Security Risk Management (SRM) Organization - Subsection relocated from 10.8.62.2.1 to align with standard security policy language and IRM 1.11.2.2.4. Clarified FISMA-reportable assets.
- (7) 10.8.62.1.3.2, IRS Information Technology (IRS IT) Services Operations - Subsection relocated from 10.8.62.2.2 to align with standard security policy language and IRM 1.11.2.2.4. Updated KISAM to IRWorks.
- (8) 10.8.62.1.3.3, Business Operating Division (BOD) Information System Owners - Subsection relocated from 10.8.62.2.3 to align with standard security policy language and IRM 1.11.2.2.4.
- (9) 10.8.62.1.3.4, Information System Contingency Plan (ISCP) Coordinator - Subsection relocated from 10.8.62.2.4 to align with standard security policy language and IRM 1.11.2.2.4.
- (10) 10.8.62.1.4, Program Management and Review - Subsection added to align with standard security policy language and IRM 1.11.2.2.4.
- (11) 10.8.62.1.5, Program Controls - Subsection added to align with standard security policy language and IRM 1.11.2.2.4.
- (12) 10.8.62.1.6, Terms and Acronyms - Subsection added to align with standard security policy language and IRM 1.11.2.2.4.
- (13) 10.8.62.1.7, Related Resources - Subsection added to align with standard security policy language and IRM 1.11.2.2.4.
- (14) 10.8.62.2, Risk Acceptance and Risk-Based Decisions - Updated URL.

- (15) 10.8.62.3.1.1 ISCP and DR Test, Training, and Exercises (TT&E) Requirement - Updated to include Mission Essential Functions (MEFs).
- (16) 10 8.62.3.1.1.1, Test, Training, and Exercises (TT&E ) Program - Updated to include assets supporting Mission Essential Functions (MEFs).
- (17) 10 8.62.3.1.1.4, ISCP Tabletop Exercises - Removed "DR" from the name of ISCP Testing Checklist.
- (18) 10.8.62 3.1.1.5, Functional Exercises - Removed annual testing frequency and added FIPS 199 LOW systems for semi-annual testing frequency.
- (19) 10.8.62 3.1.1.6, DR Tests - Updated to include assets supporting MEFs. Updated location of ECC-Martinsburg to Kearneysville, West Virginia. Removed requirement about ECC test report packages being combined with application schematics. Updated to include ECC Disaster Recovery (DR) Test Job Aid.
- (20) 10.8.62 3.1.1.7, Alternative Site Processing (ASP) Tests - Updated to include assets supporting MEFs. Removed requirement about screen shots after restoration of services. Updated to include Ad Hoc Disaster Recovery/ASP Testing SOP.
- (21) 10.8.62.3.1.1.8, Training - Updated to remove ISCP Testing Schedule from training documents.
- (22) 10.8.62 3.1.2.1, ISCP Testing Checklist - Updated subsection title to remove "DR". Updated to include functional exercises. Added leading "0" for NIST security control identifiers, per NIST 800-53, rev 5.1.1.
- (23) 10.8.62.3.1.3.1, Tabletop Exercises - Updated tabletop exercise invitations time line to thirty (30) calendar days. Updated sharing of the checklist at least seven (7) business days prior to the tabletop exercise. Updated that the AO has 15 work days to sign the Checklist (after testing) and removed June 1st requirement. Updated that BOD has fifteen (15) work days to revise the ISCP. Updated to include Tier 1 classification. Clarified training information. Updated changes "in Tabletop Exercise" to "on the Checklist."
- (24) 10.8.62 3.1.3.3, DR Tests - Updated to include assets supporting MEFs. Updated name of Executive Overview to ISCP Observation Report.
- (25) 10.8.62.3.1.4.2, Treasury FISMA Inventory Management System (TFIMS) - Updated ISCP to ISCPPT for updating Contingency Planning (CP) fields in TFIMS.
- (26) Exhibit 10.8.62-1, ISCP Testing Checklist - Updated ISCP URL.
- (27) Exhibit 10.8.62-2, ISCP Functional Exercise Methodology and Procedures - Updated ISCP URL.
- (28) Exhibit 10.8.62-3, Ad Hoc Disaster Recovery/ASP Testing Standard Operating Procedures - Added exhibit.
- (29) Exhibit 10.8.62-4, (Renumbered from 10.8.62-3), BOD ISCP Standard Operating Procedures - Updated ISCP URL.
- (30) Exhibit 10.8.62-5, ECC Disaster Recovery (DR) Test Job Aid - Added exhibit.
- (31) Exhibit 10.8.62-6, (Renumbered from 10.8.62-4) Glossary - Updated title to Terms and Acronyms and added acronyms MEF, NARA, and RBD.
- (32) Exhibit 10.8.62-7, (Renumbered from 10.8.62-5) References - Updated title to Related Resources, updated release version and date for TD P 85-01, and removed OUO designation. Updated revision and release date for NIST 800-53 and 800-53A.

- (33) Updated KISAM to IRWorks/ServiceNow throughout the IRM.
- (34) Updated “section” to “subsection” throughout the IRM, as appropriate.
- (35) Updated use of “shall” throughout the IRM.
- (36) Subsections were renumbered throughout the IRM to align with standard security policy language and IRM 1.11.2.2.4.
- (37) Editorial changes (including grammar, spelling, and minor clarification) were made throughout the IRM.

#### **EFFECT ON OTHER DOCUMENTS**

IRM 10.8.62 dated February 24, 2022, is superseded. This IRM supersedes all prior versions of IRM 10.8.62. This IRM supplements IRM 10.8.1, Information Technology (IT) Security Policy and Guidance; IRM 10.8.2, Information Technology Security Roles and Responsibilities. Also, this IRM supplements IRM 10.8.60.

#### **AUDIENCE**

IRM 10.8.62 must be distributed to all personnel responsible for ensuring that ISCPs or DR plans and procedures are exercised and/or tested to determine the capability of the IRS to recover and restore its systems in the event of a disruption, disaster, or catastrophe. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya  
Acting, Chief Information Officer



10.8.62

Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process

## Table of Contents

### 10.8.62.1 Program Scope and Objectives

#### 10.8.62.1.1 Background

#### 10.8.62.1.2 Authority

#### 10.8.62.1.3 Roles and Responsibilities

##### 10.8.62.1.3.1 Security Risk Management (SRM) Organization

##### 10.8.62.1.3.2 IRS Information Technology (IRS IT) Services Operations

##### 10.8.62.1.3.3 Business Operating Division (BOD) Information System Owners

##### 10.8.62.1.3.4 Information System Contingency Plan (ISCP) Coordinator

#### 10.8.62.1.4 Program Management and Review

#### 10.8.62.1.5 Program Controls

#### 10.8.62.1.6 Terms and Acronyms

#### 10.8.62.1.7 Related Resources

### 10.8.62.2 Risk Acceptance and Risk-Based Decisions

### 10.8.62.3 IT Security Controls

#### 10.8.62.3.1 CP – Contingency Planning (CP)

##### 10.8.62.3.1.1 ISCP and DR Test, Training, and Exercises (TT&E) Requirement

###### 10.8.62.3.1.1.1 Test, Training, and Exercises (TT&E) Program

###### 10.8.62.3.1.1.2 Information System Contingency Plan (ISCP)

###### 10.8.62.3.1.1.3 Keystroke Procedures

###### 10.8.62.3.1.1.4 ISCP Tabletop Exercises

###### 10.8.62.3.1.1.5 Functional Exercises

###### 10.8.62.3.1.1.6 DR Tests

###### 10.8.62.3.1.1.7 Alternative Site Processing (ASP) Tests

###### 10.8.62.3.1.1.8 Training

#### 10.8.62.3.1.2 ISCP& DR Exercise and Testing

##### 10.8.62.3.1.2.1 ISCP Testing Checklist

#### 10.8.62.3.1.3 Conducting Exercises and Tests

##### 10.8.62.3.1.3.1 Tabletop Exercises

##### 10.8.62.3.1.3.2 Functional Exercises

##### 10.8.62.3.1.3.3 DR Tests

#### 10.8.62.3.1.4 Annual FISMA Reporting Cycle Activities

##### 10.8.62.3.1.4.1 Scorecard

---

10.8.62.3.1.4.2 Treasury FISMA Inventory Management System (TFIMS)

Exhibits

- 10.8.62-1 ISCP Testing Checklist
- 10.8.62-2 ISCP Functional Exercise Methodology and Procedures
- 10.8.62-3 Ad Hoc Disaster Recovery/ASP Testing Standard Operating Procedures
- 10.8.62-4 BOD ISCP Standard Operating Procedures
- 10.8.62-5 ECC Disaster Recovery (DR) Test Job Aid
- 10.8.62-6 Terms and Acronyms
- 10.8.62-7 Related Resources

---

# Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process 10.8.62

page 1

## 10.8.62.1 (01-18-2024) Program Scope and Objectives

- (1) **Overview:** This Internal Revenue Manual (IRM) lays the foundation to implement and manage security controls and guidance for the use of the Information Systems Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training and Exercise (TT&E) Process within the Internal Revenue Service (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 the IRS TT&E program.
- (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. Individuals 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
- (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.

## 10.8.62.1.1 (02-24-2022) Background

- (1) This IRM defines test, training, and exercise processes to ensure that:
  - a. Internal Revenue Service (IRS) information systems (IS) resources can be fully recovered in the event that IS contingency or disaster recovery plans must be activated.
  - b. Systems and their associated Information Systems Contingency Plans (ISCPs) or disaster recovery (DR) plans and procedures are exercised and/or tested to determine the capability of the IRS to recover and restore its systems in the event of a disruption, disaster, or catastrophe.
- (2) IRM 10.8.62 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

## 10.8.62.1.2 (01-18-2024) Authority

- (1) All IRS 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 IRM augments the security controls as defined in IRM 10.8.60, *IT Service Continuity Management (ITSCM) Policy and Guidance* to ensure IRS information technology (IT) resources and business processes can be recovered.

- (3) The guidance within this IRM are recommendations taken in whole or in part from NIST 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*.

10.8.62.1.3  
(01-18-2024)  
**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 information system security and is the authoritative source for such information.
- (2) The supplemental roles and responsibilities provided below are specific to the implementation of Test, Training, and Exercise (TT&E) processes.

10.8.62.1.3.1  
(01-18-2024)  
**Security Risk  
Management (SRM)  
Organization**

- (1) Refer to IRM 10.8.60 for additional guidance on Security Risk Management (SRM) program roles and responsibilities.
- (2) SRM Information System Contingency Plan Test (ISCPT) personnel are responsible for:
- a. Implementing an effective TT&E program on behalf of SRM. The program must include at a minimum the following components:
    - i. Developing and preparing processes, templates, schedules, and procedures for ISCP exercises and tests.
    - ii. Coordinating with appropriate organizations, all ISCP and DR exercises and tests for FISMA-reportable assets in the FISMA master inventory: including Tier 1, 2, and 3 assets; applications on the IRS Mission Essential Functions (MEFs) list; and cloud assets that do not fully inherit Contingency Plan (CP) controls from the Cloud Service Provider (CSP).
    - iii. Documenting ISCP tabletop and DR exercise test results and lessons learned.
    - iv. Monitoring ISCP reviews and updates.
- (3) SRM responsibilities for monitoring ISCP reviews and updates include:
- a. Ensuring that the ISCP is updated within 15 work days after AO signature on the ISCP Testing Checklist.
  - b. Ensuring AO or Authorizing Official Designated Representative (AODR) signs the ISCP Testing Checklist validating the performance of the annual ISCP tabletop exercise, functional exercise, and/or DR test.
  - c. Ensuring Business Operating Division (BOD) and IRS IT personnel with an application/system recovery role are trained annually in their responsibilities related to ISCP and DR testing.
  - d. Developing and maintaining a master ISCP and DR testing schedule for all FISMA-reportable assets in the FISMA Master Inventory.
  - e. Coordinating with BODs and IRS IT to identify recovery and support personnel needed to participate in planned tests and exercises.
  - f. Facilitating ISCP tabletop exercises to familiarize recovery and support personnel with contingency plan's recovery procedures in the ISCP.
  - g. Identifying inconsistencies and outdated information in the ISCPs that could affect capabilities to support contingency and recovery operations.
  - h. Ensuring that all contingency and recovery tests performed by the IRS meet all Federal requirements and follow the standard guidelines set forth by the Director of SRM.
  - i. Coordinating with IRS IT and BOD IT personnel to ensure they perform the following tests for all FISMA-reportable applications and systems in



# Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process 10.8.62

page 3

- the FISMA master inventory, or as directed in the annual SRM program memorandum:
- i. A functional exercise/test of the backed-up application or system data for FISMA-reportable assets with a FIPS 199 LOW or MODERATE availability categorization.
  - ii. A DR test of the ISCP/DR plan for a FISMA-reportable asset with FIPS 199 high categorization or an asset designated as a Critical Infrastructure Protection (CIP) asset or an asset that supports any of the MEFs.
  - j. Validating that previous ISCP and DR related findings are reviewed prior to performing tests and exercises to ensure that testing activities address corrective actions taken for resolution of the findings.
  - k. Collaborating with BOD and IRS IT personnel to create DR test cases, scenarios, milestones, and summarize all in the DR test plan.
  - l. Validating that a documented process is in place for creating system and application backup files.
  - m. Validating that a documented process is in place for storing backup files at an alternate offsite location by either electronically transferring them to that designated location or by creating tapes to ship to the alternate offsite storage facility.
  - n. Developing and maintaining scorecard/metrics to keep management, BOD personnel, Security Program Management Officers (PMOs), and Associate Chief Information Officers (ACIOs) informed about the status of annual ISCP exercising/testing progress.
  - o. Collaborating with IT representatives to define and document the evidence and artifacts needed to validate testing activities.
  - p. Uploading completed exercise/test evidence and documentation to the Treasury FISMA Inventory Management System (TFIMS).
  - q. Recording the completed ISCP testing dates and ISCP update completion dates into TFIMS.
  - r. Uploading updated ISCPs to TFIMS and Toolkit Suite Command Center (TSCC).
  - s. Maintaining and updating ISCP and DR testing processes, templates, and procedures.

#  
#

## 10.8.62.1.3.2 (01-18-2024) **IRS Information Technology (IRS IT) Services Operations**

- (1) IRS IT operations provides support for all IRS information technology with only documented exceptions. During the ISCP tabletop exercises, functional exercises and DR tests, IRS IT must:
  - a. Support the activities that relate to exercises and tests of the ISCP and procedures.
  - b. Perform system backup, rebuild, recovery, reconstitution, cutover, relocation, etc., for systems supported and/or owned by IRS IT.
  - c. Provide documented backup procedures to include information about the backup frequency, encryption of backup media, offsite storage, and timelines for replicated data and/or receipt of backup media from offsite storage.
  - d. Perform functional and/or DR tests annually for applications and systems supported and/or owned by IRS IT.

- e. Provide resources for ISCP tabletop exercises and functional and/or DR tests annually for applications and systems supported and/or owned by IRS IT, including staffing and funding for backup solutions and equipment.
  - f. Complete the ISCP Testing Checklist (Refer to Exhibit 10.8.62-1) to report the results of all functional exercises, and/or recovery tests, of production servers that host applications or systems owned or supported by IT personnel in the Master Inventory.
  - g. Provide annual recommendations for updates to the ISCP Functional Exercise Methodology and Procedures (refer to Exhibit 10.8.62-2).
  - h. Facilitate planning meetings between various IRS IT and BOD areas in preparation for scheduled DR tests.
  - i. Create the schedule of daily exercise activities and milestones in preparation for scheduled DR tests.
  - j. Coordinate with appropriate areas when creating DR test scenario and scope.
  - k. Coordinate with the IRWorks Project Office and Enterprise Service Desk for support and use of the IRWorks/ServiceNow system during DR tests.
  - l. Coordinate with appropriate areas (Cybersecurity, BODs, AD, etc.) annually to develop a DR test.
  - m. Facilitate post DR test meetings with test participants to review issues and resolutions to determine if any followup actions are required by appropriate areas.
  - n. Work with appropriate areas to close action items that appear on the Vulnerabilities Matrix report.
- (2) The appropriate IRS IT organizations responsible for supporting the ISCP must review, update, exercise, and/or test the ISCP at least annually (or as significant changes occur).
- (3) System resources owned by contractors or vendors on behalf of the IRS and by BODs must also be compliant with the IRS IT requirements identified within this IRM.

10.8.62.1.3.3  
(01-18-2024)

**Business Operating  
Division (BOD)  
Information System  
Owners**

- (1) The BOD/Information System Owner is responsible for:
- a. Ensuring that systems or applications' ISCP are exercised and tested annually. (For step-by-step procedures refer to the BOD ISCP SOP, Exhibit 10.8.62-4.)
  - b. Identifying ISCP Leadership and operational-level personnel, to include a data collector, that should receive a tabletop invite to the ISCP tabletop exercise.
  - c. Ensuring that the most current version of the ISCP is loaded in TFIMS (the authoritative repository for FISMA documentation) and that the current ISCP is used during all ISCP tabletop exercises and DR tests.
  - d. Reviewing the most currently open Plan of Action and Milestones (POA&M) information in TFIMS prior to performing ISCP tabletop exercises or functional and/or DR tests to identify ISCP and/or recovery related issues and to determine if the annual ISCP testing results can be used as evidence to close the POA&M.
  - e. Completing the ISCP Testing Checklist (refer to Exhibit 10.8.62-1) prior to ISCP tabletop exercises and ensuring that tabletop participants receive a copy of the completed Checklist for use during the ISCP tabletop exercise.

# Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process 10.8.62

page 5

- f. Participating in tabletop exercises to ensure that application and system ISCPs are kept current and accurate and that participants validate roles and procedures documented in the plans.
  - g. Providing annual recommendations for updates to the ISCP testing templates.
  - h. Ensuring that the AO of the application or system receives and reviews the results, ISCP Testing Checklist, which documents the results of the ISCP tabletop exercise and functional and/or DR tests results. The AO or AODR must validate that the tabletop exercise and functional and/or DR testing are completed by signing and dating the ISCP Testing Checklist.
  - i. Ensuring that the changes from the Checklist are incorporated into the ISCP within fifteen (15) work days from the date the AO signs the Checklist.
  - j. Returning the signed ISCP Testing Checklist, and approved, updated ISCP to the ISCPPT facilitator for uploading into TFIMS.
  - k. Performing IT activities during ISCP testing exercises and tests for BOD-owned applications and systems that are not supported by IRS IT.
- (2) Information system resources owned by Contractors or Vendors and used by IRS personnel must also be compliant with the IRS IT requirements identified within the IRS IT Services Operations subsection in this IRM.

10.8.62.1.3.4  
(01-18-2024)

## Information System Contingency Plan (ISCP) Coordinator

- (1) The ISCP Coordinator, having selected the backup and system recovery strategies, must designate appropriate teams to implement the strategy.

10.8.62.1.4  
(01-18-2024)

## 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 requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.
- (2) It is the policy of the IRS:
- a. 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.
  - b. To 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.
  - c. To 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, NARA guidance, other regulatory guidance, and best practice methodologies.
  - d. To use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Software Development Life Cycle (SDLC), Informa-

tion Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.62.1.5  
(01-18-2024)

#### Program Controls

- (1) Each IRM in the 10.8 series is assigned an author who reviews their IRM annually 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 requirement 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 requirement checklists that have recently been revised or are in the process of being revised.
- (3) This IRM applies to all IRS information and information systems, which include IRS production, development, test, and contractor systems. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *National Security Information, Classified National Security Information (NSI)*, 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.

10.8.62.1.6  
(01-18-2024)

#### Terms and Acronyms

- (1) Refer to Exhibit 10.8.62-6 for a list of terms, acronyms, and definitions

10.8.62.1.7  
(01-18-2024)

#### Related Resources

- (1) Refer to Exhibit 10.8.62-7 for a list of related resources and references

10.8.62.2  
(01-18-2024)

#### 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 Risk Based Decision Standard Operating Procedures (SOP).

#  
#  
#  
#  
#

---

# Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process 10.8.62

---

page 7

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

## 10.8.62.3 (02-24-2022) **IT Security Controls**

- (1) The security controls in this IRM supplement the requirements found 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.

## 10.8.62.3.1 (02-24-2022) **CP – Contingency Planning (CP)**

- (1) Refer to IRM 10.8.1 and IRM 10.8.60, for additional guidance on Contingency Planning. (IRS-defined)

## 10.8.62.3.1.1 (02-24-2022) **ISCP and DR Test, Training, and Exercises (TT&E) Requirement**

- (1) All IRS applications and systems listed in the FISMA master inventory are required to undergo a tabletop exercise of the ISCP annually for all categories of potential impact on availability. (IRS-defined)
- (2) In addition to an annual tabletop exercise, applications and systems with a FIPS 199 LOW and MODERATE availability categorization also require a functional exercise (described in the Functional Exercises subsection) be performed. (IRS-defined)
- (3) In addition to an annual tabletop exercise, applications and systems that are CIP assets, systems that have a FIPS 199 HIGH availability categorization or assets that support any of the MEFs, must undergo testing equivalent to a DR test (described in DR tests subsection). (IRS-defined)
- (4) All annual testing and exercises must be completed during the July 1 through June 30 timeframe each year in order to meet IRS FISMA reporting requirements. (IRS-defined)
- (5) For each ISCP tabletop exercise conducted, the results must be documented in the ISCP Testing Checklist artifact. (IRS-defined)

## 10.8.62.3.1.1.1 (01-18-2024) **Test, Training, and Exercises (TT&E) Program**

- (1) Organizations must develop and operate a testing program in non-disaster situations so that IRS leadership and personnel have familiarity with contingency plans and procedures and validates the IRS' contingency capabilities through regular tests, training, and exercises. It can also identify issues or deficiencies for remediation. (IRS-defined)
- (2) Exercises and tests offer different ways of ensuring that ISCPs provide viable and actionable procedures to recover or restore IRS systems and applications to their original state in the event of a disruption. (IRS-defined)

- (3) Steps to establish a Test, Training and Exercise (TT&E) program should include the following: (NIST 800-84: Chapter 2)
  - a. Develop TT&E policy.
  - b. Identify TT&E roles and responsibilities.
  - c. Establish overall TT&E schedule.
  - d. Document TT&E methodology for planning and performing TT&E events.
    - i. Design the event - topic, scope, roles and responsibilities and objectives.
    - ii. Develop the event documentation - may include briefing materials, participant manuals, instructor and facilitator guides, test plans, and evaluation criteria.
    - iii. Conduct the event.
    - iv. Evaluate and document lessons learned from the event.
- (4) The following elements are suggested to be included in a TT&E policy: (NIST 800-84: Section 2.1)
  - Purpose
  - Effective date
  - Objectives
  - Applicability and scope
  - Authorities and related policies
  - Roles and responsibilities of key business units and staff positions
  - TT&E requirements
  - TT&E review and approval
  - Enforcement and compliance
  - Points of contact for additional information
  - Definition of terms
- (5) Refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-84, for guidance on establishing an effective ISCP testing program and the various methods and approaches for conducting exercise activities. (IRS-defined)
- (6) All tests and exercises must include some kind of determination of the effects on the organization's operations and provide for a mechanism to update and improve the plan as a result. (IRS-defined)
- (7) The depth and rigor of ISCP testing activities increases with the FIPS 199 availability security objective. Refer to the ISCP templates (FIPS 199 LOW, MODERATE, and HIGH systems) in NIST SP 800-34 Contingency Planning Guide for Federal Information Systems, for details for conducting testing activities appropriate to their respective impact level. (IRS-defined)
- (8) The depth and rigor of ISCP testing activities increases with the FIPS 199 availability security objective. (IRS-defined)
  - **For LOW and MODERATE-availability systems, a tabletop and functional exercise must be conducted annually to ensure that a basic level of recovery capability is available for all reportable assets within these categories.** The tabletop should follow a scenario that simulates a disruption, include points of contact whose roles appear in the ISCP, be attended by the business and system owners or responsible authority, and be facilitated by ISCPT personnel. The functional exercise must be performed by IRS IT or BOD IT personnel.



---

# Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process 10.8.62

---

page 9

- **For HIGH-impact systems, Critical Infrastructure Protection assets, or assets that support any of the MEFs, a tabletop exercise and full-scale end-to-end or DR test must be conducted annually to ensure that a full recovery capability is available for the most critical reportable assets.** The tabletop should follow a scenario that simulates a disruption, include points of contact whose roles appear in the ISCP, be attended by the business and system owners or responsible authority, and be facilitated by ISCPPT personnel. The full-scale test should include a system restoration at the designated alternate location. The test must also include a full recovery and reconstitution of the system to a known state.

10.8.62.3.1.1.2  
(10-04-2012)

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

- (1) The ISCP must provide procedures and capabilities for recovering a system or application in the event of a system disruption. The plan must address the resources, roles, responsibilities, and procedures for restoration of information systems and recovery of business applications and processes after a disruption. (IRS-defined)

10.8.62.3.1.1.3  
(02-24-2022)

## **Keystroke Procedures**

- (1) The keystroke procedures located in the ISCP are an information system-focused part of the plan designed to restore operability of the target system or application, at an alternate site after an emergency. (IRS-defined)
- (2) The purpose of the keystroke recovery procedures is to provide documented, detailed step-by-step procedures to facilitate recovery of capabilities at an alternate site; the scope is information system-focused and limited to major disruptions. (IRS-defined)

10.8.62.3.1.1.4  
(02-24-2022)

## **ISCP Tabletop Exercises**

- (1) Tabletop exercises are discussion-based exercises only and do not involve deploying or recovering systems, equipment, or other resources. (NIST 800-84: Chapter 4)
- (2) An ISCP tabletop exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an ISCP. (NIST 800-84: Chapter 2)
- (3) Personnel with roles and responsibilities in a particular ISCP should be invited to attend the tabletop exercise to validate the content of the plan during a discussion of their roles and responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that do not include using the actual operational environment. (NIST 800-84: Chapter 2)
- (4) ISCP tabletop exercises are scenario-driven (such as a power failure in one of the organization's computing centers or a fire causing certain systems to be damaged) with additional situations often being presented during the course of an exercise. (NIST 800-84: Chapter 2)
- (5) ISCP tabletop exercises help to identify gaps and inconsistencies within ISCPs and procedures, as well as cases where personnel need additional training or when training needs to be changed. Deficiencies identified during tabletop exercises are documented in the ISCP Testing Checklist as part of the exercise process. (NIST 800-84: Chapter 2)

- (6) Information or procedures needing validation during the ISCP tabletop exercise include but are not limited to roles and responsibilities, hardware and software inventories, keystroke recovery procedures, data back-up procedures, and interdependencies that are documented in the plan. (NIST 800-84: Section 4.2.3)
- (7) An ISCP tabletop exercise schedule must be created annually by the ISCPT staff. BOD POC's must be notified and their approval obtained by the ISCPT staff when a tabletop exercise is being scheduled. (NIST 800-84: Section 4.1)
- (8) IRS must conduct ISCP tabletop exercises for applicable applications or systems at least annually. Applicable applications or systems include those that are classified as Tier 1, 2 or 3. (IRS-defined)
- (9) The topics should be determined. Discussion topics may include the roles and responsibilities of personnel with regard to disaster recovery and incident response. Discussion topics may also include processes and procedures for disaster recovery and incident response. (NIST 800-84: Section 4.2.1)
- (10) The scope should be determined. Senior-level teams and operational-level teams should participate in separate tabletop exercises initially because of their different levels of responsibility and then in a combined exercise to validate coordination between the groups. (NIST 800-84: Section 4.2.2)
- (11) Application or system ISCP Leadership and operational-level personnel, including a data collector (as designated by the BOD), should be invited to ISCP tabletop exercises to discuss individual and team roles, responsibilities, and to validate information contained in the plan. (NIST 800-84: Section 4.2.4)
- (12) The ISCPT facilitator leads the discussion among the tabletop exercise participants. (NIST 800-84: Section 4.2.5)
- (13) Logistics for ISCP tabletop exercises should be coordinated. (NIST 800-84: Section 4.2.6)
- (14) The tabletop exercise material should be developed. (NIST 800-84: Section 4.3)
- (15) The ISCP Testing Checklist is an IRS internal document designed to assist BODs and support staff in navigating through tabletop exercise events. The BOD designated data collector records information and actions that occur during the exercise using an applicable version of the ISCP Testing Checklist. Refer to Exhibit 10.8.62-1 and 10.8.62-2 at the end of this document. (NIST 800-84: Section 4.2.5; IRS-defined)

10.8.62.3.1.1.5  
(01-18-2024)

#### Functional Exercises

- (1) Functional exercises allow personnel to validate application/system operational readiness for emergencies by validating backup procedures – specifically with regards to backup retrieval, reading backup data, and validation of offsite storage. (NIST 800-84: Chapter 5)
- (2) Functional exercises allow staff to execute their roles and responsibilities as they would in a recovery situation. (NIST 800-84: Chapter 5)
- (3) A functional exercise schedule should be created annually by the ISCPT staff and shared with Data Management and BOD IT staff. The following should be identified: (NIST 800-84: Section 5.1)
  - a. Topics (NIST 800-84: Section 5.2.1)



- b. Scope (NIST 800-84: Section 5.2.2)
  - c. Objectives (NIST 800-84: Section 5.2.3)
  - d. Participants (NIST 800-84: Section 5.2.4)
  - e. Functional exercise staff (NIST 800-84: Section 5.2.5)
- (4) Data Management staff in IT and BOD IT must conduct functional testing using the following frequency: (IRS-defined)
- a. Quarterly for FIPS 199 HIGH systems.
  - b. Semi-annually for FIPS 199 MODERATE and LOW systems.
- (5) Logistics for functional exercises should be coordinated. (NIST 800-84: Section 5.2.6)
- (6) The functional exercise material should be developed. (NIST 800-84: Section 5.3)
- (7) Data Management staff within IT and BOD IT must provide evidence of conducted functional tests, to include evidence of media retrieval from an offsite storage location and screen shots to validate successful testing has been completed. (IRS-defined)
- (8) Data Management staff in IT and BOD IT must record functional test results using Part B of the applicable version of the ISCP Testing Checklist. (IRS-defined)
- (9) Evidence gathered from functional tests should be submitted to the Cybersecurity, ISCPT staff within five (5) work days from the test ending date. (IRS-defined)
- (10) Evidence packages for all applications/systems receiving a functional test will be uploaded to TFIMS by the Cybersecurity, ISCPT staff before the end of each FISMA cycle. (IRS-defined)

## 10.8.62.3.1.1.6 (01-18-2024) DR Tests

- (1) A DR test is the method used to evaluate the organization's readiness and ability to recover an application or system from varying degrees of non-functioning to its original functional state in an alternate operational environment specified in an ISCP. (IRS-defined)

**Note:** The term *test* is reserved for testing system hardware/software/OS recovery capability or system components; it is not used to describe *exercising* plans.

- (2) DR Tests are used to measure the effectiveness and suitability of the processes and procedures contained in ISCPs for the systems being tested and to evaluate compliance with a contingency plan. In the event of a disaster or disruption, the goal is to use ISCPs to ensure that documented operational procedures and plans result in successful recovery of business applications and systems. (IRS-defined)
- (3) The scope of tests can range from individual system components or systems to comprehensive tests of all systems and components that support an ISCP. (NIST 800-84: Section 6.2.1)

- (4) A test is conducted in as close to an operational environment as possible, testing components, or systems used to conduct daily operations. (NIST 800-84: Section 6.3)
- (5) A DR test is required annually for CIP assets, assets that support any of the MEFs or assets with a high availability categorization. (IRS-defined)
  - a. IRS must conduct two Enterprise Computing Center (ECC) tests at least annually – one at ECC-Martinsburg in Kearneysville, West Virginia, and the other at ECC-Memphis in Memphis, Tennessee. Evidence from successful ECC tests will satisfy annual DR testing requirements for several CIP, MEF and/or high availability assets.
  - b. CIP, MEF and high availability assets not included in the ECC tests must be scheduled for individual DR tests annually. Evidence from successful individual tests will satisfy annual DR testing requirements for CIP, MEF and/or high availability assets not included in the ECC DR tests.
  - c. Ad hoc DR test requests for applications/systems other than CIP, MEF or high availability assets must be evaluated on a case-by-case basis by EOps, ITCM.
- (6) A DR test schedule should be created and managed collaboratively between the Cybersecurity, ISCPT staff and BOD IT staff annually for DR tests needed to satisfy DR testing requirements for CIP, MEF or high availability assets managed by BOD IT personnel. (NIST 800-84: Section 6.1)
- (7) Each reportable application or system involved in a DR test must have a contingency plan that includes but is not limited to: (IRS-defined)
  - a. Environment description;
  - b. Host system information (if applicable);
  - c. Interconnecting system dependencies;
  - d. Alternate processing site information;
  - e. Hardware/Software inventories;
  - f. Keystroke recovery procedures (if applicable);
  - g. Configuration information;
  - h. Backup information;
  - i. Escalation and notification procedures; and
  - j. Key personnel contact list(s)
- (8) The DR test event should be designed. The following should be identified-  
:(NIST 800-84: Section 6.2)
  - a. Objectives (NIST 800-84: Section 6.2.2)
  - b. Testing tools (NIST 800-84: Section 6.2.3)
  - c. Participants (NIST 800-84: Section 6.2.4)
  - d. DR test staff (NIST 800-84: Section 6.2.5)
- (9) The DR test material should be developed. (NIST 800-84: Section 6.3)
  - a. Briefings are developed for senior management, and for the managers of others that might be affected by the test, to provide an understanding of what the test will comprise and why it is important.
  - b. The test guide outlines the basic steps involved in conducting a test and includes a list of the participants. Procedures for early termination of the test should be included.

- c. Test plans list steps that will be performed, required logistical items, expected outcomes, early test termination procedures, and emergency contact numbers.
  - d. The after action report, or Summary Report, contains an overall synopsis of the DR test, the results of individual tests, and the recommendations for improvement. This report may be provided to senior management.
- (10) Each DR test for CIP, MEF or high availability assets managed by EOps must be facilitated by the EOps, ITCM staff. EOps, ITCM personnel are responsible for: (IRS-defined)
  - a. All aspects of the DR exercises, including staffing, development, conduct, and oversight;
  - b. Appointing test director(s); and
  - c. Coordinating logistics. Sample logistic items for DR tests may include but are not limited to the following: (NIST 800-84: Section 6.2.6)
    - i. DR test date(s)
    - ii. Identification of applications/systems for testing
    - iii. Participant identifications
    - iv. Meeting invitations
    - v. Conference room reservation and set-up
    - vi. Setup and configuration of appropriate testing equipment
    - vii. Required testing tools
    - viii. Backup file strategies
    - ix. Dry-run/walk through of the test
    - x. Procedures to terminate the test
- (11) Each DR test for CIP, MEF or high availability assets managed by EOps must be observed by the Cybersecurity, ISCPT staff. (IRS-defined)
- (12) DR tests required for CIP, MEF or high availability assets managed by BOD IT personnel must be conducted by BOD IT staff. (IRS-defined)
- (13) Evidence gathered from each DR test must include: (IRS-defined)
  - a. Screen shot(s) of the Production and Recovery environment including the server names in each environment.
  - b. Screen shot(s) of production data copied (reloaded) into the Recovery environment.
  - c. Screen shot(s) from the Recovery environment showing the start and stop times of the server(s) to calculate the actual recovery time(s).
  - d. Keystrokes and/or failover plan from Toolkit Suite Command Centre (TSCC) or playbook.
  - e. Testing/validation of the restored data, batch runs, end user testing etc.
  - f. Documentation of any issues/problems encountered. (NIST 800-84: Chapter 2)
  - g. Documentation of action taken to resolve issues/problems encountered. (NIST 800-84: Chapter 2)
  - h. List of participants.
- (14) Evidence gathered from DR tests should be submitted to the Cybersecurity, ISCPT staff within fifteen (15) work days from the test ending date. (IRS-defined)

- (15) The Cybersecurity, ISCPT staff must produce a test report presentation for the DR tests at ECC-Martinsburg and ECC-Memphis. (IRS-defined)
- (16) The ECC test report presentation must include: (IRS-defined)
  - a. An ISCPT Observation Report of the test for Senior Management and Executives (refer to part (20) below).
  - b. Evidence gathered during the test, including screen shots.
  - c. A vulnerabilities matrix listing tickets submitted using the IRWorks/ ServiceNow ticketing system for problems identified and actions taken to resolve issues.
- (17) Evidence packages for all applications/systems tested during the DR test will be uploaded to the TFIMS by the Cybersecurity, ISCPT staff before the end of each FISMA cycle. (IRS-defined)
- (18) The ISCPT Observation Report is a presentation for Senior Management and Executives. This overview is a summary report of an ECC DR test which contains an overall synopsis of the recovery capabilities. The ISCPT Observation Report may include: (IRS-defined)
  - a. Scenario
  - b. Test Objectives
  - c. Summary Test Results
  - d. Test Scope
  - e. Commendable Observations
  - f. Gaps Identified
  - g. Cybersecurity Recommendations
  - h. Problem Ticket Information
  - i. ISCPT Team Contact Information
- (19) Refer to Exhibit 10.8.62-5, ECC Disaster Recovery (DR) Test Job Aid. This exhibit provides step-by-step procedures for IRS IT personnel to perform the ECC DR Tests. All ECC Disaster Recovery (DR) Tests will be conducted using the approved procedures in Exhibit 10.8.62-5. (IRS-defined)

10.8.62.3.1.1.7  
(01-18-2024)

**Alternative Site  
Processing (ASP) Tests**

- (1) An Alternate Site Processing (ASP) test may be conducted in lieu of a Disaster Recovery test. (IRS-defined)
- (2) During an ASP test, the application/system that is transitioned will run at the alternate site for a predetermined period of time. (IRS-defined)
- (3) An ASP test schedule must be managed by the Enterprise Operations (EOps), IT Continuity Management (ITCM) Branch staff for each ASP test EOps conducts. This schedule may be combined with the DR test schedule. (IRS-defined)
- (4) The ASP test schedule must be shared with the Cybersecurity ISCPT staff by the EOps staff annually. (IRS-defined)
- (5) Each reportable application or system involved in an ASP test must have a contingency plan that includes, but is not limited, to the following information: (IRS-defined)
  - a. Environment description;
  - b. Host system information (if applicable);
  - c. Interconnecting system dependencies;

- d. Alternate processing site (APS) information;
  - e. Hardware/Software inventories;
  - f. Keystroke recovery procedures (if applicable);
  - g. Configuration information;
  - h. Backup information;
  - i. Escalation and notification procedures; and
  - j. Key personnel contact list(s)
- (6) Each ASP test for CIP, MEF or high availability assets managed by EOps must be facilitated by the EOps ITCM staff. EOps ITCM personnel are responsible for: (IRS-defined)
- a. All aspects of the ASP exercise, including staffing, development, conduct, and oversight;
  - b. Appointing test director(s); and
  - c. Coordinating logistics. Sample logistic items for ASP tests may include, but are not limited, to the following:
    - i. ASP test date(s)
    - ii. Identification of applications/systems for testing
    - iii. Participant identifications
    - iv. Meeting invitations
    - v. Conference room reservation and set-up
    - vi. Setup and configuration of appropriate testing equipment
    - vii. Required testing tools
    - viii. Backup file strategies
    - ix. Dry run/walk through of the test
    - x. Procedures to terminate the test
- (7) Each ASP test for CIP, MEF or high availability assets managed by EOps must be observed by the Cybersecurity ISCPT staff. (IRS-defined)
- (8) ASP tests required for CIP, MEF or high availability assets managed by BOD IT personnel must be conducted by BOD IT staff. (IRS-defined)
- (9) Evidence gathered from each ASP test must include: (IRS-defined)
- a. Screen shot(s) of the Production and Alternate Processing Site (APS) environments including the server names in each environment.
  - b. Screen shot(s) of a successful replication of data from the Production environment to the APS.
  - c. Screen shot(s) from the APS environment showing the start and stop times of the server(s) to calculate the actual recovery time(s).
  - d. Keystrokes and/or failover plan from TSCC or playbook.
  - e. Testing/validation of the restored data, batch runs, end user testing etc.
  - f. Documentation of any issues/problems encountered. (NIST 800-84: Chapter 2)
  - g. Documentation of action taken to resolve issues/problems encountered. (NIST 800-84: Chapter 2)
  - h. List of participants.
- (10) Evidence gathered from ASP tests should be submitted to the Cybersecurity ISCPT staff within 15 work days from the test ending date. (IRS-defined)

- (11) Evidence collected for applications/systems tested during an ASP test will be uploaded to the TFIMS by the Cybersecurity ISCPT staff before the end of each FISMA cycle. (IRS-defined)
- (12) Refer to Exhibit 10.8.62-3, Ad Hoc Disaster Recovery/ASP Testing SOP. This exhibit provides step-by-step procedures for IRS IT or BOD Information System personnel to perform Disaster Recovery/ASP exercises. All Ad Hoc Disaster Recovery/ASP Testing will be conducted using the approved procedures in Exhibit 10.8.62-2. (IRS-defined)

10.8.62.3.1.1.8  
(02-24-2022)

#### **Training**

- (1) Training refers to informing personnel of their roles and responsibilities within an information system contingency plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the information system contingency plan. (NIST 800-84: Chapter 3)
- (2) The scheduling of training sessions will be coordinated closely with the schedules for ISCP tabletop exercises, functional exercises, and DR tests. (NIST 800-84: Chapter 3)
- (3) Training sessions will emphasize understanding the ISCP Testing process, to include following documents in preparation for participating in each test or exercise: (IRS-defined)
  - a. ISCP – Participants will be able to answer questions about the purpose of the plan, system recovery procedures, specific application processes, recovery roles and responsibilities, notification procedures, and all appendices included in the plan.
  - b. ISCP Testing Checklist – Participants will gain knowledge of the purpose of the Checklist, how to complete it, and the procedures for its use during the scheduled exercises and tests of the ISCP.
  - c. FISMA Contingency Plan (CP) Controls – Participants will gain knowledge of the Contingency Plan family of security controls (NIST 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*) and how exercising and testing the contingency plans address the CP controls.
- (4) Recovery personnel must be trained on the following plan elements: (IRS-defined)
  - Purpose of the plan
  - Reporting procedures
  - Security requirements
  - Activation and Notification, Recovery, and Reconstitution Phases

10.8.62.3.1.1.2  
(02-24-2022)

#### **ISCP& DR Exercise and Testing**

- (1) The ISCPT Staff must solicit comments from BOD and IRS IT Point-of-Contacts (POCs) to evaluate the lessons learned from the previous ISCP testing period to ensure that the ISCP testing process continues to be viable, cost-effective, resource efficient, and compliant with new regulations. (IRS-defined)
- (2) ISCPT Staff will work with appropriate Organizations to develop a testing schedule each year to exercise or test the ISCP, for all the applications and systems found in the FISMA Master Inventory. (IRS-defined)



- (3) The ISCPT Staff will facilitate all tabletop exercises for each FISMA reporting cycle. During the Security Assessment and Authorization (SA&A) process, ISCPT personnel will collaborate with the FISMA Certification Program Office (CPO) to ensure that the ISCP testing schedule is in sync with the SA&A process and the Security Control Assessment schedule. (IRS-defined)
- (4) The schedule will be reviewed by IRS IT and BOD personnel to ensure that ISCP tabletop exercises, functional exercises, and DR tests are scheduled to coordinate each application, or more than one application if requested on a case-by-case basis, using the following keys: (IRS-defined)
  - a. Platform
  - b. System
  - c. BOD
  - d. Site
- (5) ISCPT will present the revised ISCP Testing Checklist template, ISCP template, the previous POC lists, and the new ISCP and DR Exercise/Testing Schedule to the Security PMO to initiate the annual exercise and testing activities. The PMO will vet the schedule and the POC list with their respective organizations and will coordinate errors, questions, and changes with the ISCPT Staff through the \*IT IT DR Mailbox. When the information is finalized and approved, ISCPT will use the approved schedule and POC lists for the testing cycle. (IRS-defined)
- (6) The approved schedule is published, distributed, and followed to perform ISCP and DR exercises and tests. The schedule includes: (IRS-defined)
  - a. A designated ISCPT Staff member as the Facilitator for each tabletop exercise.
  - b. Changes as submitted by BOD and IRS IT personnel, to the schedule and documented by ISCPT.
  - c. Modifications to the schedule are completed as needed during the annual FISMA reporting cycle.
- (7) ISCPT will enter the completed testing and updated ISCP dates in TFIMS for every application and system listed in the FISMA master inventory. (IRS-defined)
- (8) Changes to dates of scheduled exercises or tests will be coordinated by IRS IT personnel, BOD Security PMOs and ISCPT to establish a new date. ISCPT will update the schedule with the new exercise/test date. However, no tests will be scheduled after April 30 of each FISMA reporting cycle and all tests will be completed by June 1 to facilitate loading of all completed test packages in TFIMS by the FISMA reporting deadline of June 30. (IRS-defined)
- (9) ISCPT will schedule and present training for all BOD and IRS IT participants to ensure that they are ready to participate in the exercise. ISCPT will answer any questions the POCs may have about the exercise/test process or the Checklist. (IRS-defined)

10.8.62.3.1.2.1  
(01-18-2024)

**ISCP Testing Checklist**

- (1) The ISCP Testing Checklist is a three part form that allows BODs and Support Organizations to document multiple ISCP exercise/test results on one form to create a testing artifact that includes AO authority. (IRS-defined)
  - a. Part A of the Checklist is the Tabletop Exercise
  - b. Part B is the Functional Exercise
  - c. Part C is the Disaster Recovery (DR) Test or Production Operational Recovery which documents DR Testing activities. Refer to Exhibit 10.8.62-1 for a copy of the Checklist. (IRS-defined)
- (2) The ISCP Testing Checklist provides a step-by-step process to guide participants through the most pertinent sections of the ISCP. The Checklist provides an area to document changes for each section in the ISCP and changes to procedures that might be needed. The Checklist also provides areas to document the results of functional exercises and DR tests, if applicable. (IRS-defined)
- (3) The Checklist standardizes the process for all applications and systems, and documents all testing activities and ISCP changes. The Checklist serves as the validated artifact for ISCP testing, functional exercises, and DR Testing exercises and events. The Checklist and supporting documentation are uploaded to TFIMS after it has been reviewed and signed by the AO or AODR. (IRS-defined)
- (4) The Checklist is used to train personnel in their contingency roles and responsibilities with respect to their application or system. (IRS-defined)
- (5) Completion of the Checklist documenting performance of the required ISCP testing exercises and/or tests serves as an evidentiary artifact in TFIMS to verify that the following family of controls, if appropriate (Reference NIST 800-53): (IRS-defined)
  - a. CP-02 Contingency Plan – The ISCP is pulled from TFIMS and distributed to each participant for the tabletop exercise validating that the plan exists.
  - b. CP-03 Contingency Training – The requirements, roles and responsibilities, and recovery procedures are discussed during the ISCP tabletop exercise.
  - c. CP-04 Contingency Plan Testing and Exercises – Completion of the ISCP Testing Checklist with test dates and the AO's signature and signature date serves as evidentiary documentation that the ISCP was exercised and appropriate testing was conducted during the applicable FISMA cycle.
  - d. CP-06 Alternate Storage Site – As the tabletop exercise is performed, the ISCP is reviewed and discussed to ensure that information about backup procedures and an alternate storage site is identified and included in the plan. If backup procedures or alternate storage sites are not in place, a summary finding is annotated on the Checklist to document this issue.
  - e. CP-07 Alternate Processing Site – During tabletop exercises, the ISCP Test Plan must be reviewed to ensure an alternate processing site has been identified. If an alternate processing site has not been identified, a summary finding is annotated on the Checklist to document the issue.
  - f. CP-08 Telecommunication Services – Tabletop exercises for IRS IT systems and business applications not supported by IRS IT will include



# Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process 10.8.62

page 19

discussions about the telecommunication infrastructure and its DR capabilities, backup procedures, and validation that a DR plan exists for its recovery.

- g. CP-09 Information System Backup – Discussions during tabletop exercises will focus on the ISCP to ensure that backup procedures are documented and implemented. The procedures must include information about the backup frequency, encryption of backup media, offsite storage, and timelines. If backup procedures have not been implemented, a summary finding is annotated on the Checklist to document this issue.
- h. CP-10 Information System Recovery and Reconstitution – Tabletop discussions for this control will focus on the information in Section 5 of the ISCP to validate that procedures are in place to recover and reconstitute IRS IT systems and applications.

- (6) Each BOD will be responsible for identifying a Data Collector who must document changes, issues, or findings identified during the tabletop exercise in the appropriate sections of the ISCP Testing Checklist. (IRS-defined)
- (7) The ISCP Testing Checklist will be used as an artifact in TFIMS to document all tabletop exercises, functional exercises, and DR tests that are conducted. (IRS-defined)

## 10.8.62.3.1.3 (02-24-2022) Conducting Exercises and Tests

- (1) The following subsections provide procedures and guidance for performance of the activities for the testing and exercising portions of the TT&E Program. (IRS-defined)
- (2) When a production application or system is being tested in the designated disaster recovery environment (on IRS computer systems in an IRS facility), live data from the production backup media, including entire file(s) and database(s), may be used to test the backup recovery capability of production data. IRS employees and contractors with approved access are not required to submit a Live Data Waiver to test the restoration/recovery of the live data on the production backup media. (IRS-defined)

## 10.8.62.3.1.3.1 (01-18-2024) Tabletop Exercises

- (1) ISCPPT utilizes the tabletop session as a training opportunity, as well as a testing exercise, to thoroughly understand the ISCP information and verify its accuracy and effectiveness. Training credit will be given to those that attend the entire tabletop exercise. (IRS-defined)
- (2) Using the approved testing schedule, the assigned ISCPPT Facilitator will send a calendar invitation for the tabletop exercise to all POCs **thirty (30) calendar days** prior to the day of the exercise. (IRS-defined)
- (3) The assigned ISCPPT Facilitator must provide the ISCP Testing Checklist with items 1-4 of the checklist pre-populated, along with the converted ISCP, to the Data Collector who is designated by the BOD Security PMO or application/system AO prior to the tabletop exercise. (IRS-defined)
- (4) Using the converted version of the ISCP along with POA&M information stored in TFIMS the Data Collector must populate items 5 through 7 and Part A on the Checklist, prior to the tabletop exercise. If necessary, the Data Collector will communicate with appropriate BOD or IRS IT personnel to complete this

task. The assigned ISCPT Facilitator must provide the ISCP Testing Checklist with items 1-4 of the checklist pre-populated to the Data Collector who is designated by the BOD Security PMO or application/system AO. (IRS-defined)

- (5) Once the Data Collector has populated items 5 through 7 and Part A of the Checklist, the Data Collector must forward the Checklist and converted ISCP to all recipients, including the ISCPT Facilitator at least seven (7) business days prior to the tabletop exercise. (IRS-defined)
- (6) During the tabletop exercise, the Data Collector is responsible for capturing on the Checklist all changes, observations, lessons learned, and summary findings that result from the tabletop discussions. **The Date Exercise Completed** block must be entered with the date the tabletop was performed. (IRS-defined)
  - a. At the start of the exercise, the Facilitator should welcome the participants to the event and request that the participants introduce themselves by name and give a general description of their roles as it relates to the application or system being tested. The Facilitator will discuss the scope of the exercise and logistical information. The Facilitator will walk the participants through the scenario and initiate a group discussion of the contents of the ISCP. The Facilitator may inject additional questions periodically for clarification purposes. The Data Collector documents issues to be included in the after action report. (NIST 800-84: Section 4.4)
  - b. Immediately following the facilitated discussion, the Facilitator and Data Collector should conduct an exercise debrief, in which they ask the participants in which areas they felt they excelled, in which areas they could use additional training, and which areas of the plan should be updated. (NIST 800-84: Section 4.4)
- (7) After the exercise, the Data Collector has fifteen (15) work days to update the Checklist with the results of the exercise. The Facilitator will coordinate with the Data Collector as needed to provide guidance and to compare notes taken during the exercise. (IRS-defined)
  - a. The comments from the debrief, along with lessons learned during the exercise, must be captured on the checklist. The Checklist should include background information about the exercise, documented observations made by the Facilitator and Data Collector, and recommendations for updates to the ISCP for the application or system that was exercised. (NIST 800-84: Section 4.5)
  - b. Following the development of the of the Checklist after the tabletop exercise, the Data Collector may assign action items to select personnel to update the ISCP that was exercised. (NIST 800-84: Section 4.5)
- (8) Once the post-tabletop Checklist update is completed, the Data Collector must send it to the ISCPT group mailbox at \*IT IT DR Mailbox and the BOD Security PMO. ISCPT personnel must forward it to the assigned ISCPT Facilitator, who must review the Checklist to ensure that all information has been recorded. If Checklist corrections are needed, the Facilitator will coordinate with the Data Collector to ensure that the modifications are made. (IRS-defined)
- (9) The ISCP Facilitator will ensure that all required testing has been completed for the application or system named on the Checklist. This may mean that the Facilitator will hold the Checklist until all additional testing has been completed and can be documented in Part B or Part C of the Checklist. If no other testing

---

# Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process 10.8.62

page 21

is required, the ISCPT Facilitator must prepare and send the Checklist back to the Data Collector and the BOD Security PMO within seven (7) business days for AO or AODR digital signature. (IRS-defined)

- (10) The AO or AO Designee has **15 work days** to sign the Checklist. (IRS-defined)

#  
#  
#  
#  
#  
#  
#  
#  
#

## 10.8.62.3.1.3.2 (02-24-2022) Functional Exercises

- (1) Functional exercises are performed by IRS IT personnel or by the BOD's information system personnel when the application is not supported by IRS IT. Functional exercises are completed on backed-up data or information to prove back-up resiliency. (Refer to Exhibit 10.8.62-1.) (IRS-defined)
- (2) Refer to Exhibit 10.8.62-2, ISCP Functional Exercise Methodology and Procedures. This exhibit provides step-by-step procedures for a backup retrieval and sampling pull for functional exercise activities. All functional exercises will be conducted using the approved procedures in Exhibit 10.8.62-2. (IRS-defined)
- (3) As the production environment implements new technologies, strategies, and procedures, IRS IT and SRM must assess when to modify Exhibit 10.8.62-2 procedures to ensure that functional exercises can be performed to accommodate the updated production environment. (IRS-defined)
- (4) During the functional exercise,
  - a. Functional exercises should prompt participants to carry out their roles and responsibilities as realistically as possible. Data Management from EOps or BOD IT personnel will conduct functional exercises. (NIST 800-84: Section 5.4)
  - b. The IRS IT or BOD information system personnel must take screen prints while the test is being conducted to submit to ISCPT as evidence. Evidence of backup recovery capabilities, includes, but is not limited to: (IRS-defined)
    - A screenshot that includes the name of the production server and the time the testing began.
    - If data is backed-up to media, evidence in the form of routing sheets, logs, or e-mail requests proving the length of time needed between the request for backup media from offsite storage and the receipt of that media at the test site.
    - If data is replicated, evidence that the data size from the production server matches the data size from the test site after the data is repli-

cated.  
- Evidence that backup media and/or replicated data is readable.

- c. The exercise director announces the conclusion of the exercise. Immediately following the exercise, the exercise director, controllers, and data collectors conduct an exercise debrief with the participants, requesting feedback from everyone present. (NIST 800-84: Section 5.4)
- (5) IRS IT or BOD information system personnel must also provide evidence to validate that documented backup procedures in the ISCP are in place and that the ISCP includes information about the backup frequency, encryption of backup media, offsite storage site, and timelines for receipt of backup media from offsite storage during normal working hours and after hours. (IRS-defined)
- (6) If no documented procedures are in the ISCP describing the backup process, the issue will be documented in Part B of the Checklist. In addition, if the backed-up data or information cannot be successfully retrieved or read, or if evidence cannot be captured for the exercise, these issues will also be documented in Part B of the Checklist. (IRS-defined)

#  
#  
#  
#  
#

- (8) Once the final checklist has been prepared for AO or AODR signature, ISCP will send the checklist to the BOD Security PMO or Data Collector.(IRS-defined)

#  
#  
#  
#  
#  
#

- (10) Upon receipt of the signed Checklist and supporting documentation from the AO or AODR, ISCP must upload the Checklist into TFIMS as the validated artifact along with all supporting documentation. (IRS-defined)

10.8.62.3.1.3.3  
(01-18-2024)  
**DR Tests**

- (1) IRS is required to perform DR tests on all applications with a FIPS 199 High availability categorization, on assets that support any of the MEFs and on CIP assets. (IRS-defined)
- (2) DR tests involve activities such as performing cutovers from one platform or system to another, relocation of systems/applications, or recovery of platforms and their hosted applications. As DR tests are performed on systems, sites, or platforms, hosted applications can benefit from these tests through coordination of the application ISCP review and the DR test activities. (IRS-defined)
- (3) IRS or BOD IT personnel perform DR tests. During the performance of the DR Test, IRS or BOD IT personnel must complete the ISCP Testing Checklist Part C, and Test Case templates as they conduct the test. (Refer to Exhibit 10.8.62-1.) (IRS-defined)

- (4) The ISCPT Staff will coordinate with IRS IT or BOD information system personnel to identify components, systems, and/or comprehensive tests to be planned based on FISMA, Treasury, and NIST requirements, and IRS executive-level priorities. (IRS-defined)
- (5) Successful recovery of a production location at the alternate processing site is considered meeting the IRS DR Testing requirement if documentation and evidence are gathered. The Service may also consider combining tests with planned operational activities, such as restoring a backup, moving a server from one room to another, upgrading or patching operating systems or applications, or changing hardware components (e.g., swapping hard drives, replacing a failed power supply etc.). The results of this collaboration will define the scope and objectives for the tests. (IRS-defined)
- (6) The ISCPT Staff will collaborate with designated BOD POCs to determine if the tests identified in collaboration with IRS IT or BOD IT personnel are compatible with the priorities and processing timeframes of the Business Unit. ISCPT and/or IRS IT information system personnel will coordinate with BODs to determine the level of involvement required from the BOD POCs. (IRS-defined)
- (7) The ISCPT will collaborate with IRS IT or BOD information system personnel to create a DR test schedule annually based on IRS and FISMA requirements, FISMA timeframes, and business processing priorities. (IRS-defined)
- (8) The ISCPT Staff will coordinate activities with IRS IT or BOD information system personnel to ensure that the ISCP Testing Checklist, Summary Report, and all testing documentation is completed before, during, and after testing. (IRS-defined)
- (9) For Enterprise Computing Center or DR tests performed by BOD IT information system, IRS IT or BOD information system personnel will: (IRS-defined)
  - a. Coordinate with the designated IRS IT or BOD POCs to ensure the Test Case Template has been populated with pertinent information about the test such as scope detail, objectives, recovery personnel, support personnel, and test activities planned.
  - b. Ensure that IRS IT or BOD information system personnel identify the files needed to be transmitted in preparation for the tests and determine the date for transmission of data via IRS approved protocols.
  - c. Coordinate with Enterprise Computing Center (ECC) Security Management Office (SMO) personnel to reserve a conference room to hold meetings before, during, and after planned test activities as needed.
  - d. Coordinate with stakeholders to ensure that pre-test activities are completed.
  - e. Facilitate the creation of procedures to terminate the test in case operational issues necessitate it.
  - f. Coordinate with IRS IT and BOD POCs to ensure that all test participants including end users are familiar with the test termination procedures.
  - g. Coordinate with IRS IT or BOD information system personnel and POCs to ensure that end users are not adversely affected during planned test activities.

- h. Conduct the DR test. (NIST 800-84: Section 6.4)
  - i. The locations for tests vary based on the type of test being conducted and the test's scope.
  - ii. During a test, the mission of the organization should not be disrupted to the extent that the organization can no longer function and provide the services that it was created to provide. If there is any sign of a possible catastrophic disruption, or the safety of an individual is at stake or the security of the organization or its data is in question, the test director and any other member of the test staff should have the ability to terminate the test immediately.
  - iii. After the test concludes, the test director should conduct an informal test debrief, requesting feedback from everyone present.
- i. Coordinate with IRS IT organization or BOD POCs at the end of the test to ensure that test deactivation procedures are completed.
- j. Review and evaluate the completed Test Case Template, worksheets, findings, corrective actions, and all test evidentiary documentation.
- k. Comments from the debrief, documented observations made by the exercise staff, and recommendations made during the DR test, should be captured in an after action report. Managers may need to be briefed on DR test results. (NIST 800-84: Section 6.6)
- l. Populate a test Summary Report to include findings, corrective actions, lessons learned, and summarize test worksheet results.
- m. Facilitate post test meetings as needed to go over Summary Report, lessons learned, and corrective actions.

10.8.62.3.1.4  
(02-24-2022)  
**Annual FISMA Reporting  
Cycle Activities**

- (1) The following subsections describe the activities needed to capture the results of the ISCP testing program. Reporting and testing artifact controls are critical to the successful completion of ISCP exercises and testing processes each FISMA cycle and are performed on a regular basis throughout the FISMA Reporting Cycle. (IRS-defined)

10.8.62.3.1.4.1  
(09-04-2015)  
**Scorecard**

- (1) For the purposes of reporting on the progress of exercises and testing, ISCP must maintain a scorecard to document the progress of the ISCP tabletop and functional exercises and the status of the DR tests. (IRS-defined)

10.8.62.3.1.4.2  
(02-24-2022)  
**Treasury FISMA  
Inventory Management  
System (TFIMS)**

- (1) ISCP must upload the updated ISCP, signed Checklist, and all evidence and documentation for each ISCP tested application or system into TFIMS in a timely manner. ISCP will also update the Contingency Planning (CP) fields in TFIMS with the appropriate dates. (IRS-defined)
- (2) The following ISCP Testing documentation is uploaded into TFIMS after exercise/testing is completed: (IRS-defined)
  - Updated Contingency Plan (ISCP)
  - ISCP Testing Checklist
  - Evidence collected from functional and/or DR tests
- (3) The following Contingency Planning (CP) fields will be updated in TFIMS after exercise/testing is completed: (IRS-defined)
  - Last CP Test Date (date all tests were completed).
  - Next CP Test Date (one year from CP Test Date)

---

Information System Contingency Plan (ISCP) and Disaster  
Recovery (DR) Test, Training, and Exercise (TT&E)  
Process 10.8.62

---

page 25

**Exhibit 10.8.62-1 (01-18-2024)**  
**ISCP Testing Checklist**

#  
#  
#  
#  
#  
#



Exhibit 10.8.62-2 (02-24-2022)  
ISCP Functional Exercise Methodology and Procedures

#  
#  
#  
#  
#



---

Information System Contingency Plan (ISCP) and Disaster  
Recovery (DR) Test, Training, and Exercise (TT&E)  
Process 10.8.62

---

page 27

Exhibit 10.8.62-3 (01-18-2024)

Ad Hoc Disaster Recovery/ASP Testing Standard Operating Procedures

#  
#  
#  
#  
#

Exhibit 10.8.62-4 (02-24-2022)  
BOD ISCP Standard Operating Procedures

#  
#  
#  
#  
#

---

Information System Contingency Plan (ISCP) and Disaster  
Recovery (DR) Test, Training, and Exercise (TT&E)  
Process 10.8.62

---

page 29

Exhibit 10.8.62-5 (01-18-2024)

ECC Disaster Recovery (DR) Test Job Aid

#  
#  
#  
#

**Exhibit 10.8.62-6 (01-18-2024)****Terms and Acronyms**

<b>Term</b>	<b>Definition or description</b>
<b>ACIO</b>	Associate Chief Information Officer
<b>After Action Report</b>	A document containing findings and recommendations from an exercise or a test.
<b>AO</b>	Authorizing Official
<b>AODR</b>	Authorizing Official Designated Representative
<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>Alternate Site Processing Test</b>	An ASP test is an orchestrated and scheduled transition of an application/system from the production location to the designated alternate site.
<b>BCP</b>	Business Continuity Plan
<b>BOD</b>	Business Operating Division
<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>CIO</b>	Chief Information Officer
<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>Comprehensive Test</b>	A test of all systems and components that support a particular IT plan, such as a contingency plan or computer security incident response plan.
<b>COOP</b>	Continuity of Operations Plan
<b>CP</b>	Contingency Planning
<b>CPO</b>	Certification Program Office
<b>CSP</b>	Cloud Service Provider
<b>Disaster Recovery (DR) Test</b>	A Disaster Recovery (DR) test is a method used to evaluate the organization's readiness and ability to recover an application or system from varying degrees of non-functioning to its original functional state in an alternate operational environment specified in an ISCP.
<b>DR</b>	Disaster Recovery
<b>EA</b>	Enterprise Architecture

# Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process 10.8.62

page 31

## Exhibit 10.8.62-6 (Cont. 1) (01-18-2024)

### Terms and Acronyms

Term	Definition or description
<b>ECC</b>	Enterprise Computing Center
<b>ESA</b>	Essential Supporting Activity
<b>ESP</b>	Enterprise Standards Profile
<b>Event</b>	The suite of test or exercise activities.
<b>Exercise</b>	A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.
<b>FIPS</b>	Federal Information Processing Standard
<b>FISMA</b>	Federal Information Security Management Act
<b>Functional Exercise</b>	A functional exercise is 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., backup procedures, communications, emergency notifications, IS equipment setup).
<b>IRM</b>	Internal Revenue Manual
<b>IRS</b>	Internal Revenue Service
<b>IS</b>	Information System
<b>ISCP</b>	Information System Contingency Plan
<b>ISCPT</b>	Information System Contingency Plan Testing (ISCPT)
<b>IT</b>	Information Technology
<b>MEF</b>	Mission Essential Function
<b>NARA</b>	National Archives and Records Administration
<b>NIST</b>	National Institute of Standards and Technology
<b>Plan</b>	In the context of this policy, the capitalized term, "Plan", refers to any of the various IT plans, including Technical Contingency Plan Documents, Continuity of Operations Plans, and any equivalent planning documents.
<b>POA&amp;M</b>	Plan of Actions and Milestones
<b>POC</b>	Point of Contact
<b>PMO</b>	Program Management Office
<b>RBD</b>	Risk-Based Decision
<b>SA&amp;A</b>	Security Assessment and Authorization
<b>SOP</b>	Standard Operating Procedure

**Exhibit 10.8.62-6 (Cont. 2) (01-18-2024)****Terms and Acronyms**

<b>Term</b>	<b>Definition or description</b>
<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.
<b>SP</b>	Special Publication
<b>SRM</b>	Security Risk Management
<b>Tabletop Exercise</b>	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
<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>TFIMS</b>	Treasury FISMA Inventory Management System
<b>TSCC</b>	Tool Suite Command Center
<b>TT&amp;E</b>	Test, Training, and Exercise
<b>TT&amp;E Event</b>	An event used to support the maintenance of an IT plan by allowing organizations to identify problems related to an IS plan and implement solutions before an adverse situation occurs.

---

# Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process 10.8.62

page 33

---

## Exhibit 10.8.62-7 (01-18-2024)

### Related Resources

#### IRS Publications

- IRM 10.8.1 – *Information Technology (IT) Security, Policy and Guidance*.
- IRM 10.8.2 – *Information Technology (IT) Security, Roles and Responsibilities*.
- IRM 10.8.60 - *Information Technology (IT) Service Continuity Management (ITSCM) Policy and Guidance*
- IRM 10.9.1 - *Classified National Security Information*

#### Department of Treasury Publications

- 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*.
- NIST FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*.
- NIST SP 800-34, Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010 (Errata page - Nov. 11, 2010).
- NIST SP 800-35, *Guide to Information Technology Security Services*, October 2003.
- NIST SP 800-37 Rev 2, *Guide for Applying the Risk Management Framework to Federal Information Systems*, September 2018.
- NIST SP 800-53 Rev 5.1.1, *Security and Privacy Controls for Federal Information Systems and Organizations*, November 7, 2023.
- NIST SP 800-53A Rev 5.1.1, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, November 7, 2023.
- NIST SP 800-60 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes)*, August 2008.
- NIST SP 800-84, *Guide to Test, Training, and Exercise Program for IT Plans and Capabilities*, September 2006.

#### Department of Homeland Security Publications

- Homeland Security Presidential Directive/HSPD-20, *National Continuity Policy*, May 2007.
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.
- Department of Homeland Security (DHS), *National Response Plan*, May 2006.

#### Other Publications

- E-Government Act of 2002 (P.L. 107-347), Title III, *Federal Information Security Modernization Act of 2014* (FISMA).
- Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, July 2016.
- Public Law 100-235, *Computer Security Act of 1987*.



