**Contingency Planning (CP)**

**CP-1: Contingency Planning Policy and Procedures**

NIST SP 800-53 Objective: The organization develops, disseminates, and reviews/updates [*Assignment: organization defined frequency]:*

a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Control Translation: Ensure contingency planning policy and procedures are in place.

Notes: The organizational risk management strategy is a key factor in the development of the contingency planning policy. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and Contingency Planning Policy (if available). Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency.

Technology specific: General

**CP-2: Contingency Plan**

NIST SP 800-53 Objective: The organization:

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

- Identifies essential missions and business functions and associated contingency requirements;

- Provides recovery objectives, restoration priorities, and metrics;

- Addresses contingency roles, responsibilities, assigned individuals with contact information;

- Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and

- Is reviewed and approved by designated officials within the organization;

1. Distributes copies of the contingency plan to [Assignment; organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements];
2. Coordinates contingency planning activities with incident handling activities;
3. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]:
4. e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during the contingency plan implementation, execution, or testing; and
5. f. Communicates contingency plan changes to [Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements].

Control Translation: Ensure contingency planning is in place for information systems and is part of an overall organizational program for achieving continuity of operations for mission/business operations.

Notes: The organizational mission/business operations is a key factor in the development of the contingency plan. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Related control: AC-14, CP-6, CP-7, CP-8, IR-4, PM-8, PM-11.

How to test and evaluate: Examine SSP and Contingency Planning Policy (if available). Verify that the policy and applicable documents identifies essential missions and business functions and whether it’s been reviewed and approved by designated organization officials. Verify and note what the recovery objectives are, the responsible team/roles/individuals, is it coordinated with incident handling activities, and how often is the contingency plan reviewed.

Technology specific: General

**CP-3: Contingency Training**

NIST SP 800-53 Objective: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency].

Control Translation: Ensure contingency training is in place.

Notes: None.

How to test and evaluate: Examine SSP and Contingency Planning Policy (if available). Verify that the policy requires personnel training in their contingency roles and responsibilities. Verify and note what the contingency training defined-frequency is and if automated mechanism is in place to remind personnel of training refresher. Review any output from the Contingency Training, whether Certificates of Completion, email records, calendar invitations, etc. to validate the training took place.

Technology specific: General

**CP-4: Contingency Plan Testing and Exercises**

NIST SP 800-53 Objective: The organization:

1. Tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests and/or exercises] to determine the plan’s effectiveness and the organization’s readiness to execute the plan; and
2. Reviews the contingency plan test/exercise results and initiates corrective actions.

Control Translation: Ensure contingency plan tests and exercises are in place.

Notes: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. Related controls: CP-10, SC-24.

How to test and evaluate: Examine SSP and Contingency Planning Policy (if available). Verify that the policy entails tests and/or exercises of the contingency plan and a defined-frequency for test and exercise is in place. Request for most recent contingency plan test/exercise results and verify that findings are listed in POA&M.

Technology specific: General

**CP-6: Alternate Storage Site**

NIST SP 800-53 Objective: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.

Control Translation: Ensure an alternate storage site is in place for storage and recovery of information system backup information.

Notes: Related controls: CP-2, CP-9, MP-4.

How to test and evaluate: Examine SSP and Contingency Planning Policy (if available) and verify that documents identify alternate storage site for storage and recovery of information system backup information. Verify and note whether alternate storage site is separated from primary storage site, that alternate storage site facilitate operations in accordance with recovery time and recovery point objectives, and whether potential problems to alternate storage site have been identified and outlines mitigation actions.

Technology specific: General

**CP-7: Alternate Processing Site**

NIST SP 800-53 Objective: The organization:

1. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period consistent with recovery time objectives] when the primary processing capabilities are unavailable; and
2. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.

Control Translation: Ensure an alternate processing site is in place including necessary agreements, equipment, and supplies required to resume operations.

Notes: Related controls: CP-2.

How to test and evaluate: Examine SSP and Contingency Planning Policy (if available) and verify that documents identify alternate processing site for resumption of operations for essential missions and business functions. Verify and note whether alternate processing site is separated from primary processing site, that alternate processing site have agreements in place that contain priority of service provisions, alternate site have been configured so that it is ready to be used as an operational site, and whether alternate site have security measures equivalent to that of the primary site.

Technology specific: General

**CP-8: Telecommunications Services**

NIST SP 800-53 Objective: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.

Control Translation: Ensure an alternate telecommunications services is in place including necessary agreements to permit the resumption of information system operations for essential missions and business functions.

Notes: Related controls: CP-2.

How to test and evaluate: Examine SSP and Contingency Planning Policy (if available) and verify that documents identify alternate telecommunications services for resumption of operations for essential missions and business functions. Verify and note whether alternate telecommunications services agreements contain priority of service provisions, primary and alternate telecommunications do not share a single point of failure, both primary and alternate telecommunications services are separated so that they are not susceptible to the same hazards, and that both primary and alternate telecommunications services providers have contingency plans for both.

Technology specific: General

**CP-9: Information System Backup**

NIST SP 800-53 Objective: The organization:

1. Conducts backups of user-level information contained in the information system [Assignment organization-defined frequency consistent with recovery time and recovery point objectives];
2. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]
3. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and
4. Protects the confidentiality and integrity of backup information at the storage location.

Control Translation: Ensure that organization conducts backups of user-level, system-level, and information system documentation.

Notes: System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control. Related controls: CP-6, MP-4.

How to test and evaluate: Examine SSP and Contingency Planning Policy (if available) and verify that documents identify that organization conducts backups of user-level, system-level, and information system documentation. Verify and note whether organization tests backup of information according to the organization-defined frequency, sample of backup information is used as part of contingency plan testing, backup copies of the operating system is stored in separate facility or in a fire-rated container, and backup information is transferred and stored at alternate storage site.

Technology specific: General

CP-10: Information System Recovery and Reconstitution

NIST SP 800-53 Objective: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Control Translation: Ensure the organization have mechanisms in place for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Notes: Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on organizational priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, SC-24.

How to test and evaluate: Examine SSP and Contingency Planning Policy (if available) and verify that documents identify that organization have mechanisms in place for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Verify and note whether information system implements transaction recovery for systems that are transaction-based (database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery). Verify if there are compensating security controls are in place, if there is capability to reimage that is controlled and is integrity protected disk images representing a secure and operational state, and if there is real-time or near-real-time failover (mirrored) capability at an alternate processing site.

Technology specific: General