For High-Impact Information Systems

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

CP-1.1 – **Examine** contingency planning policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with contingency planning and plan implementation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents contingency planning policy and procedures;				
(ii)	The organization disseminates contingency planning policy and procedures to appropriate elements within the organization;				
(iii)	Responsible parties within the organization periodically review contingency planning policy and procedures; and				
(iv)	The organization updates contingency planning policy and procedures when organizational review indicates updates are required.				

CP-1.2 - Examine contingency planning policy and procedures; other relevant documents or records, **and**

Interview organizational personnel with contingency planning and plan implementation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The contingency planning policy addresses purpose, scope, roles and responsibilities, management commitment, coordination among				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	organizational entities, and compliance;				
(ii)	The contingency planning policy is consistent with the organization's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance; and				
(iii)	The contingency planning procedures address all areas identified in the contingency planning policy and address achieving policy-compliant implementations of all associated security controls.				

CP-2 CONTINGENCY PLAN - The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

CP-2.1 – Examine contingency planning policy; procedures addressing contingency operations for the information system; NIST Special Publication 800-34; contingency plan; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization develops and documents a contingency plan for the information system;				
(ii)	The contingency plan is consistent with NIST Special Publication 800-34;				
(iii)	The contingency plan addresses contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the information system after a disruption or failure;				
(iv)	The contingency plan is reviewed and approved by designated organizational officials; and				
(v)	The organization disseminates the contingency plan to key contingency personnel.				

CP-2.2 – Interview organizational personnel with contingency planning and plan implementation responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if key contingency personnel and the key operating elements within the organization understand the contingency plan and are ready to implement the plan.				

CP-2(1).1 – Examine contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; other related plans; other relevant documents or records, **and**

Interview organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization coordinates the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan).				

CP-3 CONTINGENCY TRAINING - The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].

CP-3.1- Examine contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; information system security plan (for organization-defined frequency for refresher contingency training); other relevant documents or records, **and**

Interview organizational personnel with contingency planning, plan implementation, and training responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization provides contingency training to personnel with				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	significant contingency roles and responsibilities;				
(ii)	The organization records the type of contingency training received and the date completed;				
(iii)	The organization defines frequency of refresher contingency training; and				
(iv)	The organization provides initial training and refresher training in accordance with organization-defined frequency, at least annually.				

CP-3.2- Examine contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if contingency training material addresses the procedures and activities necessary to fulfill identified organizational contingency roles and responsibilities.				

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES - The organization: (i) tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.

CP-4.1 – Examine contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; information system security plan (for the organization-defined frequency of contingency plan tests and/or exercises and the list of the organization-defined contingency plan tests and/or exercises); contingency plan testing and/or exercise documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the frequency of contingency plan tests and/or exercises;				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(ii)	The organization defines the set of contingency plan tests and/or exercises;				
(iii)	The organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency;				
(iv)	The organization documents the results of contingency plan testing/exercises; and				
(v)	The organization reviews the contingency plan test/exercise results and takes corrective actions.				

CP-4.2 – Examine contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; contingency plan test results; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the contingency plan tests/exercises address key aspects of the plan.				

CP-4(1).1 – Examine contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; contingency plan testing and/or exercise documentation; other relevant documents or records, **and**

Interview organizational personnel with contingency planning, plan implementation, and testing responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan).				

CP-5 CONTINGENCY PLAN UPDATE - The organization reviews the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

CP-5.1 – Examine contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; information system security plan (for organization-defined frequency of contingency plan reviews and updates); other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the frequency of contingency plan reviews and updates;				
(ii)	The organization updates the contingency plan in accordance with organization-defined frequency, at least annually; and				
(iii)	The revised plan reflects the needed changes based on the organization's experiences during plan implementation, execution, and testing.				

CM-5.2 – Examine contingency planning policy; contingency plan; procedures addressing contingency plan reviews and updates; other relevant documents or records, **and**

Interview organizational personnel with contingency plan review and update responsibilities; organizational personnel with mission-related and operational responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization communicates necessary changes to the contingency plan to other organizational elements with related plans.				

CP-6 ALTERNATE STORAGE SITE - The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.

CP-6.1 - Examine contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site agreements; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies an alternate storage site; and				
(ii)	Alternate storage site agreements are currently in place (if needed) to permit storage of information system backup information.				

CP-6.2 - Examine contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records, **and**

Interview organizational personnel with alternate storage site responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the alternate storage site is available, accessible, and meets the requirements (including necessary equipment and supplies) to permit the storage of information system backup information consistent with the organization's recovery time objectives and recovery point objectives.				

CP-6(1).1 - Examine contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The contingency plan identifies the primary storage site hazards; and				
(ii)	The alternate storage site is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site.				

CP-6(3).1 - Examine contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; other relevant documents or records to determine if the following requirements are met:

Requirement	S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The contingency plan identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and				
(ii)	The contingency plan defines explicit mitigation actions for potential accessibility problems.				

CP-7 ALTERNATE PROCESSING SITE - The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable.

CP-7.1 - **Examine** contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; information system security plan (for organization-defined time period within which processing must be resumed at the alternate processing site); other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies an alternate processing site;				
(ii)	The organization defines the time period within which processing must be resumed at the alternate processing site; and				
(iii)	Alternate processing site agreements are currently in place (if needed) to permit the resumption of information system operations for critical mission/business functions within organization-defined time period.				

CP-7.2 - **Examine** contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records, **and**

Interview organizational personnel with alternate processing site responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the alternate processing site is available, accessible, and meets the requirements (including necessary equipment and				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	supplies) for resuming information system operations for critical mission/business functions within organization-defined time period.				

CP-7(1).1 - **Examine** contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The contingency plan identifies the primary processing site hazards; and				
(ii)	The alternate processing site is sufficiently separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site.				

CP-7(2).1 - **Examine** contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The contingency plan identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and				
(ii)	The contingency plan defines explicit mitigation actions for potential accessibility problems.				

CP-7(3).1 - **Examine** contingency planning policy; contingency plan; procedures addressing alternate processing sites; alternate processing site agreements; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if alternate processing site agreements contain priority-of-				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	service provisions in accordance with the organization's availability requirements.				

CP-8 TELECOMMUNICATIONS SERVICES - The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.

CP-8.1 - Examine contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; information system security plan (for organization-defined time period within which resumption of information system operations must take place); primary and alternate telecommunications service agreements; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization identifies primary and alternate telecommunications services to support the information system;				
(ii)	The organization defines the time period within which resumption of information system operations must take place; and				
(iii)	Alternate telecommunications service agreements are in place to permit the resumption of telecommunications services for critical mission/business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.				

CP-8.2 - Examine contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Telecommunications services supporting the organization are used				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	for national security emergency preparedness; and				
(ii)	A common carrier provides telecommunications services.				

CP-8(1).1 - Examine contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the availability requirements defined in the organization's contingency plan.				

CP-8(2).1 - Examine contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; primary and alternate telecommunications service agreements; other relevant documents or records, **and**

Interview organizational personnel with contingency planning and plan implementation responsibilities; telecommunications service providers to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if primary and alternate telecommunications services share a single point of failure.				

CP-9 INFORMATION SYSTEM BACKUP - The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and protects backup information at the storage location.

CP-9.1 - Examine contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for information system backup); backup storage location(s); other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the frequency of information systems backups;				
(ii)	The organization defines the user-level and system-level information (including system state information) that is required to be backed up; and				
(iii)	The organization identifies the location(s) for storing backup information.				

CP-9.2 - Examine contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for information system backup); backup storage location(s); other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization backs up the required user-level and system-level information (including system state information) in accordance with the organization-defined frequency; and				
(ii)	The organization stores the backup information in designated locations in accordance with information system backup procedures.				

CP-9(1).1 - Examine contingency planning policy; contingency plan; procedures addressing information system backup; information system security plan (for organization-defined frequency for testing backup information); information system backup test results; backup storage location(s); other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	The organization defines the frequency of information system backup testing;				
(ii)	The organization conducts information system backup testing within the organization-defined frequency; and				
(iii)	Testing results verify backup media reliability and information				

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
	integrity.				

CP-9(4).1 - Examine contingency planning policy; contingency plan; procedures addressing information system backup; information system design documentation; backup storage location(s); information system configuration settings and associated documentation; other relevant documents or records, **and**

Interview (DEPTH, COVERAGE): Organizational personnel with information system backup responsibilities to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization employs appropriate mechanisms to protect the integrity of information system backup information.				

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION - The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure

CP-10.1 - Examine contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization identifies the means for capturing the information system's operational state including appropriate system parameters, patches, configuration settings, and application/system software prior to system disruption or failure.				

CP-10.2 - Examine contingency planning policy; contingency plan; procedures addressing information system recovery and reconstitution; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records to determine if the following requirements are met:

Requirement		S	N	Document(s) Examined, Person(s) Interviewed, and Findings	Initials & Date
(i)	Determine if the organization makes available and applies mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure.				

and

Test automated mechanisms implementing information system recovery and reconstitution operations to determine if the following requirements are met:

Test Steps		S	N	Findings	Initials & Date
1	Validate through a test recovery that information system's operational state including appropriate system parameters, patches, configuration settings, and application/system software prior to system disruption or failure.				