

Contingency Planning Implementation Checklist

Policy and Documentation

- ☐ **CP-1:** Develop, document, and disseminate contingency planning policy at organization-level, mission/business process-level, or system-level that addresses purpose, scope, roles, responsibilities, management commitment, coordination, and compliance
- ☐ **CP-1:** Ensure contingency planning policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
- ☐ **CP-1:** Develop and document procedures to facilitate implementation of contingency planning policy and associated controls
- ☐ **CP-1:** Designate an official to manage development, documentation, and dissemination of contingency planning policy and procedures
- ☐ **CP-1:** Review and update contingency planning policy at least every 3 years and following significant changes
- ☐ **CP-1:** Review and update contingency planning procedures at least annually and following significant changes

Contingency Plan Development and Maintenance

- ☐ **CP-2:** Develop a contingency plan that identifies essential mission and business functions and associated contingency requirements
- ☐ **CP-2:** Include recovery objectives, restoration priorities, and metrics in the contingency plan
- ☐ **CP-2:** Document contingency roles, responsibilities, and assigned individuals with contact information
- ☐ **CP-2:** Address maintaining essential mission and business functions despite system disruption, compromise, or failure
- ☐ **CP-2:** Address eventual full system restoration without deterioration of originally planned controls
- ☐ **CP-2:** Address sharing of contingency information in the plan



FedRAMP Moderate Templates

- ☐ **CP-2:** Obtain review and approval of contingency plan from organization-defined personnel or roles
- ☐ **CP-2:** Distribute copies of contingency plan to key contingency personnel and organizational elements
- ☐ **CP-2:** Coordinate contingency planning activities with incident handling activities
- ☐ **CP-2:** Review the contingency plan for the system at least annually
- ☐ **CP-2:** Update contingency plan to address organizational, system, or environmental changes
- ☐ **CP-2:** Update contingency plan based on problems encountered during implementation, execution, or testing
- ☐ **CP-2:** Communicate contingency plan changes to key contingency personnel and organizational elements
- ☐ **CP-2:** Incorporate lessons learned from testing, training, or actual contingency activities
- ☐ **CP-2:** Protect contingency plan from unauthorized disclosure and modification
- ☐ **CP-2 (1):** Coordinate contingency plan development with organizational elements responsible for related plans
- ☐ **CP-2 (3):** Plan for resumption of all mission and business functions within time period defined in service provider and organization SLA
- ☐ **CP-2 (8):** Identify critical system assets supporting all or essential mission and business functions

Contingency Training

- ☐ **CP-3:** Provide contingency training to system users consistent with assigned roles and responsibilities within ten (10) days of assuming a contingency role
- ☐ **CP-3:** Provide contingency training when required by system changes
- ☐ **CP-3:** Provide contingency training at least annually after initial training
- ☐ **CP-3:** Review and update contingency training content at least annually
- ☐ **CP-3:** Update contingency training content following organization-defined events

Contingency Plan Testing

- ☐ **CP-4:** Test the contingency plan at least annually using functional exercises
- ☐ **CP-4:** Determine effectiveness of the plan through testing
- ☐ **CP-4:** Determine readiness to execute the plan through testing
- ☐ **CP-4:** Review contingency plan test results



FedRAMP Moderate Templates

- ☐ **CP-4:** Initiate corrective actions based on test results when needed
- ☐ **CP-4 (1):** Coordinate contingency plan testing with organizational elements responsible for related plans

Alternate Storage Site

- ☐ **CP-6:** Establish an alternate storage site with necessary agreements for storage and retrieval of system backup information
- ☐ **CP-6:** Ensure alternate storage site provides controls equivalent to the primary site
- ☐ **CP-6 (1):** Identify an alternate storage site sufficiently separated from primary site to reduce susceptibility to same threats
- ☐ **CP-6 (3):** Identify potential accessibility problems to alternate storage site during area-wide disruption or disaster
- ☐ **CP-6 (3):** Outline explicit mitigation actions for alternate storage site accessibility problems

Alternate Processing Site

- ☐ **CP-7:** Establish an alternate processing site with necessary agreements for transfer and resumption of system operations
- ☐ **CP-7:** Ensure alternate processing site supports essential mission and business functions within defined time period when primary processing is unavailable
- ☐ **CP-7:** Make available required equipment and supplies at alternate processing site or establish contracts for delivery
- ☐ **CP-7:** Provide controls at alternate processing site equivalent to primary site
- ☐ **CP-7 (1):** Identify an alternate processing site sufficiently separated from primary site to reduce susceptibility to same threats
- ☐ **CP-7 (2):** Identify potential accessibility problems to alternate processing site during area-wide disruption or disaster
- ☐ **CP-7 (2):** Outline explicit mitigation actions for alternate processing site accessibility problems
- ☐ **CP-7 (3):** Develop alternate processing site agreements with priority-of-service provisions in accordance with availability requirements and recovery time objectives

Telecommunications Services

- ☐ **CP-8:** Establish alternate telecommunications services with necessary agreements for resumption of system operations
- ☐ **CP-8:** Ensure alternate telecommunications services support essential mission and business functions when primary capabilities are unavailable
- ☐ **CP-8 (1):** Develop primary and alternate telecommunications service agreements with priority-of-service provisions
- ☐ **CP-8 (1):** Request Telecommunications Service Priority for all services used for national security emergency preparedness if provided by common carrier
- ☐ **CP-8 (2):** Obtain alternate telecommunications services to reduce likelihood of sharing single point of failure with primary services

System Backup

- ☐ **CP-9:** Conduct daily incremental and weekly full backups of user-level information in organization-defined system components
- ☐ **CP-9:** Conduct daily incremental and weekly full backups of system-level information
- ☐ **CP-9:** Conduct daily incremental and weekly full backups of system documentation, including security- and privacy-related documentation
- ☐ **CP-9:** Ensure all backup frequencies are consistent with recovery time and recovery point objectives
- ☐ **CP-9:** Protect confidentiality, integrity, and availability of backup information
- ☐ **CP-9 (1):** Test backup information at least annually to verify media reliability and information integrity
- ☐ **CP-9 (8):** Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all backup files

System Recovery and Reconstitution

- ☐ **CP-10:** Provide for recovery and reconstitution of the system to a known state within organization-defined time period after disruption, compromise, or failure
- ☐ **CP-10:** Ensure recovery time period is consistent with recovery time and recovery point objectives
- ☐ **CP-10 (2):** Implement transaction recovery for systems that are transaction-based



FedRAMP Moderate Templates

Key Timeframes Summary

- ☐ **Policy review:** At least every 3 years and following significant changes
- ☐ **Procedure review:** At least annually and following significant changes
- ☐ **Contingency plan review:** At least annually
- ☐ **Contingency training:** Within 10 days of assuming role, then at least annually
- ☐ **Contingency plan testing:** At least annually using functional exercises
- ☐ **Backup frequency:** Daily incremental and weekly full backups
- ☐ **Backup testing:** At least annually
- ☐ **CP-2 (3) resumption timeframe:** As defined in service provider and organization SLA