3.6 CONTINGENCY PLANNING

Quick link to Contingency Planning Summary Table

CP-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] contingency planning policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Contingency planning policy and procedures address the controls in the CP family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of contingency planning policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [SP 800-12], [SP 800-30], [SP 800-34], [SP 800-39], [SP 800-50], [SP 800-100].

CP-2 CONTINGENCY PLAN

Control:

a. Develop a contingency plan for the system that:

   1. Identifies essential mission and business functions and associated contingency requirements;

   2. Provides recovery objectives, restoration priorities, and metrics;

   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

   4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;

   5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

   6. Addresses the sharing of contingency information; and

   7. Is reviewed and approved by [*Assignment: organization-defined personnel or roles*];

b. Distribute copies of the contingency plan to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system [*Assignment: organization-defined frequency*];

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to [*Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements*];

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

Discussion: Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system, as specified in IR-4(5). Incident response planning is part of contingency planning for organizations and is addressed in the IR (Incident Response) family.

Related Controls: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.

Control Enhancements:

(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS

Coordinate contingency plan development with organizational elements responsible for related plans.

Discussion: Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

Related Controls: None.

(2) CONTINGENCY PLAN | CAPACITY PLANNING

Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Discussion: Capacity planning is needed because different threats can result in a reduction of the available processing, telecommunications, and support services intended to support essential mission and business functions. Organizations anticipate degraded operations during contingency operations and factor the degradation into capacity planning. For capacity planning, environmental support refers to any environmental factor for which the organization determines that it needs to provide support in a contingency situation, even if in a degraded state. Such determinations are based on an organizational assessment of risk, system categorization (impact level), and organizational risk tolerance.

Related Controls: PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.

(3) CONTINGENCY PLAN | RESUME MISSION AND BUSINESS FUNCTIONS

Plan for the resumption of [*Selection: all; essential*] mission and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

Discussion: Organizations may choose to conduct contingency planning activities to resume mission and business functions as part of business continuity planning or as part of business impact analyses. Organizations prioritize the resumption of mission and business functions. The time period for resuming mission and business functions may be dependent on the severity and extent of the disruptions to the system and its supporting infrastructure.

Related Controls: None.

(4) CONTINGENCY PLAN | RESUME ALL MISSION AND BUSINESS FUNCTIONS

[Withdrawn: Incorporated into CP-2(3).]

(5) CONTINGENCY PLAN | CONTINUE MISSION AND BUSINESS FUNCTIONS

Plan for the continuance of [*Selection: all; essential*] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

Discussion: Organizations may choose to conduct the contingency planning activities to continue mission and business functions as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related Controls: None.

(6) CONTINGENCY PLAN | ALTERNATE PROCESSING AND STORAGE SITES

Plan for the transfer of [*Selection: all; essential*] mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.

Discussion: Organizations may choose to conduct contingency planning activities for alternate processing and storage sites as part of business continuity planning or business impact analyses. Primary processing and/or storage sites defined by organizations as part of contingency planning may change depending on the circumstances associated with the contingency.

Related Controls: None.

(7) CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS

Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

Discussion: When the capability of an organization to carry out its mission and business functions is dependent on external service providers, developing a comprehensive and timely contingency plan may become more challenging. When mission and business functions are dependent on external service providers, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization.

Related Controls: SA-9.

(8) CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS

Identify critical system assets supporting [*Selection: all; essential*] mission and business functions.

Discussion: Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations consider implementing CP-2(7) as a control enhancement.

Related Controls: CM-8, RA-9.

References: [SP 800-34], [IR 8179].

CP-3 CONTINGENCY TRAINING

Control:

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

   1. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility;

   2. When required by system changes; and

3. [*Assignment: organization-defined frequency*] thereafter; and

b. Review and update contingency training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Contingency training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, some individuals may only need to know when and where to report for duty during contingency operations and if normal duties are affected; system administrators may require additional training on how to establish systems at alternate processing and storage sites; and organizational officials may receive more specific training on how to conduct mission-essential functions in designated off-site locations and how to establish communications with other governmental entities for purposes of coordination on contingency-related activities. Training for contingency roles or responsibilities reflects the specific continuity requirements in the contingency plan. Events that may precipitate an update to contingency training content include, but are not limited to, contingency plan testing or an actual contingency (lessons learned), assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. At the discretion of the organization, participation in a contingency plan test or exercise, including lessons learned sessions subsequent to the test or exercise, may satisfy contingency plan training requirements.

Related Controls: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

Control Enhancements:

(1) CONTINGENCY TRAINING | SIMULATED EVENTS

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Discussion: The use of simulated events creates an environment for personnel to experience actual threat events, including cyber-attacks that disable websites, ransomware attacks that encrypt organizational data on servers, hurricanes that damage or destroy organizational facilities, or hardware or software failures.

Related Controls: None.

(2) CONTINGENCY TRAINING | MECHANISMS USED IN TRAINING ENVIRONMENTS

Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.

Discussion: Operational mechanisms refer to processes that have been established to accomplish an organizational goal or a system that supports a particular organizational mission or business objective. Actual mission and business processes, systems, and/or facilities may be used to generate simulated events and enhance the realism of simulated events during contingency training.

Related Controls: None.

References: [SP 800-50].

CP-4 CONTINGENCY PLAN TESTING

Control:

a. Test the contingency plan for the system [*Assignment: organization-defined frequency*] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [*Assignment: organization-defined tests*].

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

Discussion: Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related Controls: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.

Control Enhancements:

(1) CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS

Coordinate contingency plan testing with organizational elements responsible for related plans.

Discussion: Plans related to contingency planning for organizational systems include Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans, Crisis Communications Plans, Critical Infrastructure Plans, Cyber Incident Response Plans, and Occupant Emergency Plans. Coordination of contingency plan testing does not require organizations to create organizational elements to handle related plans or to align such elements with specific plans. However, it does require that if such organizational elements are responsible for related plans, organizations coordinate with those elements.

Related Controls: IR-8, PM-8.

(2) CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE

Test the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations.

Discussion: Conditions at the alternate processing site may be significantly different than the conditions at the primary site. Having the opportunity to visit the alternate site and experience the actual capabilities available at the site can provide valuable information on potential vulnerabilities that could affect essential organizational mission and business functions. The on-site visit can also provide an opportunity to refine the contingency plan to address the vulnerabilities discovered during testing.

Related Controls: CP-7.

(3) CONTINGENCY PLAN TESTING | AUTOMATED TESTING

Test the contingency plan using [*Assignment: organization-defined automated mechanisms*].

Discussion: Automated mechanisms facilitate thorough and effective testing of contingency plans by providing more complete coverage of contingency issues, selecting more realistic test scenarios and environments, and effectively stressing the system and supported mission and business functions.

Related Controls: None.

(4) CONTINGENCY PLAN TESTING | FULL RECOVERY AND RECONSTITUTION

Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes

activities for returning systems to fully operational states. Organizations establish a known state for systems that includes system state information for hardware, software programs, and data. Preserving system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission and business processes.

Related Controls: CP-10, SC-24.

(5) CONTINGENCY PLAN TESTING | SELF-CHALLENGE

Employ [*Assignment: organization-defined mechanisms*] to [*Assignment: organization-defined system or system component*] to disrupt and adversely affect the system or system component.

Discussion: Often, the best method of assessing system resilience is to disrupt the system in some manner. The mechanisms used by the organization could disrupt system functions or system services in many ways, including terminating or disabling critical system components, changing the configuration of system components, degrading critical functionality (e.g., restricting network bandwidth), or altering privileges. Automated, on-going, and simulated cyber-attacks and service disruptions can reveal unexpected functional dependencies and help the organization determine its ability to ensure resilience in the face of an actual cyber-attack.

Related Controls: None.

References: [FIPS 199], [SP 800-34], [SP 800-84], [SP 800-160-2].

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2.]

CP-6 ALTERNATE STORAGE SITE

Control:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Discussion: Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related Controls: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

Control Enhancements:

(1) ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE

Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate storage sites are defined in organizational risk assessments and include natural disasters, structural failures, hostile attacks, and errors of

omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(2) ALTERNATE STORAGE SITE | RECOVERY TIME AND RECOVERY POINT OBJECTIVES

Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Discussion: Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution.

Related Controls: None.

(3) ALTERNATE STORAGE SITE | ACCESSIBILITY

Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk. Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

Related Controls: RA-3.

References: [SP 800-34].

CP-7 ALTERNATE PROCESSING SITE

Control:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [*Assignment: organization-defined system operations*] for essential mission and business functions within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Discussion: Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites, access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites

that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

Control Enhancements:

(1) ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE

Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Discussion: Threats that affect alternate processing sites are defined in organizational assessments of risk and include natural disasters, structural failures, hostile attacks, and errors of omission or commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate processing sites based on the types of threats that are of concern. For threats such as hostile attacks, the degree of separation between sites is less relevant.

Related Controls: RA-3.

(2) ALTERNATE PROCESSING SITE | ACCESSIBILITY

Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Discussion: Area-wide disruptions refer to those types of disruptions that are broad in geographic scope with such determinations made by organizations based on organizational assessments of risk.

Related Controls: RA-3.

(3) ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE

Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Discussion: Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site. Organizations establish recovery time objectives as part of contingency planning.

Related Controls: None.

(4) ALTERNATE PROCESSING SITE | PREPARATION FOR USE

Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

Discussion: Site preparation includes establishing configuration settings for systems at the alternate processing site consistent with the requirements for such settings at the primary site and ensuring that essential supplies and logistical considerations are in place.

Related Controls: CM-2, CM-6, CP-4.

(5) ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS

[Withdrawn: Incorporated into CP-7.]

(6) ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE

Plan and prepare for circumstances that preclude returning to the primary processing site.

Discussion: There may be situations that preclude an organization from returning to the primary processing site such as if a natural disaster (e.g., flood or a hurricane) damaged or

destroyed a facility and it was determined that rebuilding in the same location was not prudent.

Related Controls: None.

References: [SP 800-34].

CP-8 TELECOMMUNICATIONS SERVICES

Control: Establish alternate telecommunications services, including necessary agreements to permit the resumption of [*Assignment: organization-defined system operations*] for essential mission and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Discussion: Telecommunications services (for data and voice) for primary and alternate processing and storage sites are in scope for CP-8. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related Controls: CP-2, CP-6, CP-7, CP-11, SC-7.

Control Enhancements:

(1) TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS

(a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

(b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

Discussion: Organizations consider the potential mission or business impact in situations where telecommunications service providers are servicing other organizations with similar priority of service provisions. Telecommunications Service Priority (TSP) is a Federal Communications Commission (FCC) program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. The FCC sets the rules and policies for the TSP program, and the Department of Homeland Security manages the TSP program. The TSP program is always in effect and not contingent on a major disaster or attack taking place. Federal sponsorship is required to enroll in the TSP program.

Related Controls: None.

(2) TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE

Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Discussion: In certain circumstances, telecommunications service providers or services may share the same physical lines, which increases the vulnerability of a single failure point. It is important to have provider transparency for the actual physical transmission capability for telecommunication services.

Related Controls: None.

(3) TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS

Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Discussion: Threats that affect telecommunications services are defined in organizational assessments of risk and include natural disasters, structural failures, cyber or physical attacks, and errors of omission or commission. Organizations can reduce common susceptibilities by minimizing shared infrastructure among telecommunications service providers and achieving sufficient geographic separation between services. Organizations may consider using a single service provider in situations where the service provider can provide alternate telecommunications services that meet the separation needs addressed in the risk assessment.

Related Controls: None.

(4) TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN

(a) Require primary and alternate telecommunications service providers to have contingency plans;

(b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

(c) Obtain evidence of contingency testing and training by providers [*Assignment: organization-defined frequency*].

Discussion: Reviews of provider contingency plans consider the proprietary nature of such plans. In some situations, a summary of provider contingency plans may be sufficient evidence for organizations to satisfy the review requirement. Telecommunications service providers may also participate in ongoing disaster recovery exercises in coordination with the Department of Homeland Security and state and local governments. Organizations may use these types of activities to satisfy evidentiary requirements related to service provider contingency plan reviews, testing, and training.

Related Controls: CP-3, CP-4.

(5) TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING

Test alternate telecommunication services [*Assignment: organization-defined frequency*].

Discussion: Alternate telecommunications services testing is arranged through contractual agreements with service providers. The testing may occur in parallel with normal operations to ensure that there is no degradation in organizational missions or functions.

Related Controls: CP-3.

References: [SP 800-34].

CP-9 SYSTEM BACKUP

Control:

a. Conduct backups of user-level information contained in [*Assignment: organization-defined system components*] [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

b. Conduct backups of system-level information contained in the system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

c. Conduct backups of system documentation, including security- and privacy-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and

d. Protect the confidentiality, integrity, and availability of backup information.

Discussion: System-level information includes system state information, operating system software, middleware, application software, and licenses. User-level information includes information other than system-level information. Mechanisms employed to protect the integrity of system backups include digital signatures and cryptographic hashes. Protection of system backup information while in transit is addressed by MP-5 and SC-8. System backups reflect the requirements in contingency plans as well as other organizational requirements for backing up information. Organizations may be subject to laws, executive orders, directives, regulations, or policies with requirements regarding specific categories of information (e.g., personal health information). Organizational personnel consult with the senior agency official for privacy and legal counsel regarding such requirements.

Related Controls: CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.

Control Enhancements:

(1) SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY

Test backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.

Discussion: Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Related Controls: CP-4.

(2) SYSTEM BACKUP | TEST RESTORATION USING SAMPLING

Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

Discussion: Organizations need assurance that system functions can be restored correctly and can support established organizational missions. To ensure that the selected system functions are thoroughly exercised during contingency plan testing, a sample of backup information is retrieved to determine whether the functions are operating as intended. Organizations can determine the sample size for the functions and backup information based on the level of assurance needed.

Related Controls: CP-4.

(3) SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION

Store backup copies of [*Assignment: organization-defined critical system software and other security-related information*] in a separate facility or in a fire rated container that is not collocated with the operational system.

Discussion: Separate storage for critical information applies to all critical information regardless of the type of backup storage media. Critical system software includes operating systems, middleware, cryptographic key management systems, and intrusion detection systems. Security-related information includes inventories of system hardware, software, and firmware components. Alternate storage sites, including geographically distributed architectures, serve as separate storage facilities for organizations. Organizations may

provide separate storage by implementing automated backup processes at alternative storage sites (e.g., data centers). The General Services Administration (GSA) establishes standards and specifications for security and fire rated containers.

Related Controls: CM-2, CM-6, CM-8.

(4) SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION

[Withdrawn: Incorporated into CP-9.]

(5) SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE

Transfer system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].

Discussion: System backup information can be transferred to alternate storage sites either electronically or by the physical shipment of storage media.

Related Controls: CP-7, MP-3, MP-4, MP-5.

(6) SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM

Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations.

Discussion: The effect of system backup can be achieved by maintaining a redundant secondary system that mirrors the primary system, including the replication of information. If this type of redundancy is in place and there is sufficient geographic separation between the two systems, the secondary system can also serve as the alternate processing site.

Related Controls: CP-7.

(7) SYSTEM BACKUP | DUAL AUTHORIZATION FOR DELETION OR DESTRUCTION

Enforce dual authorization for the deletion or destruction of [*Assignment: organization-defined backup information*].

Discussion: Dual authorization ensures that deletion or destruction of backup information cannot occur unless two qualified individuals carry out the task. Individuals deleting or destroying backup information possess the skills or expertise to determine if the proposed deletion or destruction of information reflects organizational policies and procedures. Dual authorization may also be known as two-person control. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.

Related Controls: AC-3, AC-5, MP-2.

(8) SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION

Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [*Assignment: organization-defined backup information*].

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls: SC-12, SC-13, SC-28.

References: [FIPS 140-3], [FIPS 186-4], [SP 800-34], [SP 800-130], [SP 800-152].

CP-10 SYSTEM RECOVERY AND RECONSTITUTION

Control: Provide for the recovery and reconstitution of the system to a known state within [*Assignment: organization-defined time period consistent with recovery time and recovery point objectives*] after a disruption, compromise, or failure.

Discussion: Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

Related Controls: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

Control Enhancements:

(1) SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING

[Withdrawn: Incorporated into CP-4.]

(2) SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY

Implement transaction recovery for systems that are transaction-based.

Discussion: Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.

Related Controls: None.

(3) SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS

[Withdrawn: Addressed through tailoring.]

(4) SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD

Provide the capability to restore system components within [*Assignment: organization-defined restoration time periods*] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Discussion: Restoration of system components includes reimaging, which restores the components to known, operational states.

Related Controls: CM-2, CM-6.

(5) SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY

[Withdrawn: Incorporated into SI-13.]

(6) SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION

Protect system components used for recovery and reconstitution.

Discussion: Protection of system recovery and reconstitution components (i.e., hardware, firmware, and software) includes physical and technical controls. Backup and restoration components used for recovery and reconstitution include router tables, compilers, and other system software.

Related Controls: AC-3, AC-6, MP-2, MP-4, PE-3, PE-6.

References: [SP 800-34].

CP-11 ALTERNATE COMMUNICATIONS PROTOCOLS

Control: Provide the capability to employ [*Assignment: organization-defined alternative communications protocols*] in support of maintaining continuity of operations.

Discussion: Contingency plans and the contingency training or testing associated with those plans incorporate an alternate communications protocol capability as part of establishing resilience in organizational systems. Switching communications protocols may affect software applications and operational aspects of systems. Organizations assess the potential side effects of introducing alternate communications protocols prior to implementation.

Related Controls: CP-2, CP-8, CP-13.

Control Enhancements: None.

References: None.

CP-12 SAFE MODE

Control: When [*Assignment: organization-defined conditions*] are detected, enter a safe mode of operation with [*Assignment: organization-defined restrictions of safe mode of operation*].

Discussion: For systems that support critical mission and business functions—including military operations, civilian space operations, nuclear power plant operations, and air traffic control operations (especially real-time operational environments)—organizations can identify certain conditions under which those systems revert to a predefined safe mode of operation. The safe mode of operation, which can be activated either automatically or manually, restricts the operations that systems can execute when those conditions are encountered. Restriction includes allowing only selected functions to execute that can be carried out under limited power or with reduced communications bandwidth.

Related Controls: CM-2, SA-8, SC-24, SI-13, SI-17.

Control Enhancements: None.

References: None.

CP-13 ALTERNATIVE SECURITY MECHANISMS

Control: Employ [*Assignment: organization-defined alternative or supplemental security mechanisms*] for satisfying [*Assignment: organization-defined security functions*] when the primary means of implementing the security function is unavailable or compromised.

Discussion: Use of alternative security mechanisms supports system resiliency, contingency planning, and continuity of operations. To ensure mission and business continuity, organizations can implement alternative or supplemental security mechanisms. The mechanisms may be less effective than the primary mechanisms. However, having the capability to readily employ alternative or supplemental mechanisms enhances mission and business continuity that might otherwise be adversely impacted if operations had to be curtailed until the primary means of implementing the functions was restored. Given the cost and level of effort required to provide such alternative capabilities, the alternative or supplemental mechanisms are only applied to critical security capabilities provided by systems, system components, or system services. For example, an organization may issue one-time pads to senior executives, officials, and system administrators if multi-factor tokens—the standard means for achieving secure authentication—are compromised.

Related Controls: CP-2, CP-11, SI-13.

Control Enhancements: None

References: None.