Compliance Component

DEFINITION	
Name	Contingency Plan Development, Documentation and Technical Considerations
Description	Contingency Plan Development, Documentation and Technical Considerations are a coordinated strategy involving plans, procedures and technical measures that enable the recovery of IT systems, operations and data after a disruption.
Rationale	Information Technology (IT) resources are essential to an organization's success. Therefore, it is critical that the services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing plans, procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster.
Benefits	• Provides guidance to help personnel evaluate information systems and operations to determine contingency requirements and priorities. • Identifies fundamental planning principles and practices to help personnel develop and maintain effective IT contingency plans. • Provides established plans, procedures and technical measures that can enable a system to be recovered quickly and effectively following a service disruption or disaster. • Provides a structured approach to aid planners in developing cost-effective solutions that accurately reflect business requirements and integrate contingency planning principles into all aspects of IT operations.

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Operational Controls
List the Technology Area Name	Contingency Planning TA
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	Contingency planning refers to interim measures to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods. 1. **Develop the contingency planning policy statement.** A formal policy including business and IT functions provides the authority and guidance necessary to develop an effective contingency plan. a. To be effective and to ensure that personnel fully understand the agency's contingency planning requirements, the contingency plan must be based on a clearly defined policy. The contingency planning policy statement should include the agency's business objectives and establish the organizational framework and responsibilities for contingency planning. Key policy elements are as follows: • Roles and responsibilities • Scope as applies to the type(s) of platform(s) and organization functions subject to contingency planning • Resource requirements • Training requirements • Exercise and testing schedules • Plan maintenance schedule • Frequency of backups and storage of backup media 2. **Conduct the business impact analysis (BIA).** The BIA helps to identify and prioritize critical systems and components. a. The purpose of the BIA is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components. Results from the BIA should be incorporated into the analysis and strategy development efforts for the organization. A BIA should: • Identify IT resources critical to business • Record disruption impacts and allowable outage times • Record recovery priorities 3. **Identify preventive controls.** Measures taken to mitigate the effects of system disruptions can increase system availability and reduce contingency life cycle costs. a. In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption. A wide variety of preventive controls are available, depending on system type and configuration; some common measures are listed below:

- Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls)
- Gasoline or diesel-powered generators to provide long-term backup power
- Air-conditioning systems with adequate excess capacity to permit failure of certain components, such as a compressor
- Fire suppression systems
- Fire and smoke detectors
- Water sensors in the computer room ceiling and floor
- Plastic tarps that may be unrolled over IT equipment to protect it from water damage
- Heat-resistant and waterproof containers for backup media and vital non-electronic records
- Emergency master system shutdown switch
- Offsite storage of backup media, non-electronic records, and system documentation
- Technical security controls, such as cryptographic key management and least-privilege access controls
- Frequent, scheduled backups

b. Preventive controls should be documented in the contingency plan, and personnel associated with the system should be trained on how and when to use the controls. These controls should be maintained in good condition and included in routine testing to ensure their effectiveness in an emergency.

4. **Develop recovery strategies.** Recovery strategies must ensure that the system may be recovered quickly and effectively following a disruption.

   a. The recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. The following should be considered:

      - Backup methods including offsite storage and should consider
        - Geographic area
        - Accessibility
        - Security
        - Environment
        - Cost

- Alternate Sites. The following table provides considerations for choosing a site.

Alternate Site Criteria Selection

Site	Cost	Hardware Equipment	Telecom-munications	Setup Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial/Full	Medium	Fixed
Hot Site	Medium/High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	High	Full	Full	None	Fixed

- Equipment replacement and should consider:
  - Vendor agreements
  - Equipment inventory
  - Existing compatible equipment
- Roles and responsibilities
- Overall cost

5. **Develop an IT contingency plan.** The contingency plan should contain detailed guidance and procedures for restoration. The following sections should be included:

   a. Supporting information
      - Introduction
        - Purpose
        - Applicability
        - Scope
        - References and requirements
        - Record of changes
      - Concept of operations
        - System description
        - Line of succession
        - Responsibilities

   b. Notification and Activation Phase. Describes the process of notifying recovery personnel and performing a damage assessment and includes:
      - Notification procedures
      - Damage assessment and should address
        - Cause of the emergency or disruption
        - Potential for additional disruptions or damage
        - Area affected by the emergency
        - Status of physical infrastructure (e.g., structural integrity of computer room, condition of electric

power, telecommunications, and heating, ventilation, and air-conditioning [HVAC])

- Inventory and functional status of IT equipment (e.g., fully functional, partially functional, and nonfunctional)
- Type of damage to IT equipment or data (e.g., water damage, fire and heat, physical impact, and electrical surge)
- Items to be replaced (e.g., hardware, software, firmware, and supporting materials)
- Estimated time to restore normal services

- Plan activation. Criteria may be based on:
  - Safety of personnel and extent of damage to the facility
  - Extent of damage to system (e.g., physical, operational, or cost)
  - Criticality of the system to the organization's mission (e.g., critical infrastructure protection asset)
  - Anticipated duration of disruption.

c. Recovery Phase. Discusses a suggested course of action for recovery teams and personnel to restore IT operations at an alternate site or using contingency capabilities and includes:
   - Sequence of recovery activities
   - Recovery procedures. Procedures should be assigned to the appropriate recovery team and typically address the following actions:
     - Obtaining authorization to access damaged facilities or geographic area
     - Notifying internal and external business partners associated with the system
     - Obtaining necessary office supplies and work space
     - Obtaining and installing necessary hardware components
     - Obtaining and loading backup media
     - Restoring critical operating system and application software
     - Restoring system data
     - Testing system functionality including security controls
     - Connecting system to network or other external

systems

- Operating alternate equipment successfully

d. Reconstitution Phase. Outlines actions that can be taken to return the system to normal operating conditions at the permanent site. The following major activities occur in this phase:
    - Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies
    - Installing system hardware, software, and firmware. This activity should include detailed restoration procedures similar to those followed in the Recovery Phase
    - Establishing connectivity and interfaces with network components and external systems
    - Testing system operations to ensure full functionality
    - Backing up operational data on the contingency system and uploading to restored system
    - Shutting down the contingency system
    - Terminating contingency operations
    - Securing, removing, relocating or destroying all sensitive materials at the contingency site
    - Arranging for recovery personnel to return to the permanent facility

e. Plan appendices. Common contingency plan appendices include the following:
    - Contact information for contingency planning team personnel
    - Standard operating procedures and checklists for system recovery or processes
    - Equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations. Details should be provided for each entry, including model or version number, specifications, and quantity
    - Vendor contact information, including offsite storage and alternate site points of contact
    - Vendor Service Level Agreements, reciprocal agreements with other organizations, and other vital records
    - Description of, and directions to (including alternate routes), the alternate site
    - Transportation arrangements e.g. use of privately owned vehicles or alternate transportation

	• The BIA, conducted during the planning phases, contains valuable information about the interrelationships, risks, prioritization, and impacts to each element of the system. The BIA should be included as an appendix for reference to help determine when the plan should be activated
Document Source Reference #	NIST Special Publication 800-34

Standard Organization			
Name		*Website*	
Contact Information			

Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	inquiries@nist.gov		

KEYWORDS	
List all Keywords	Recovery, disaster, disruption, business impact analysis, BIA, preventative, alternate site.

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☒ *Current*	☐ *Twilight*	☐ *Sunset*

Rationale for Component Classification	
Document the Rationale for Component Classification	

Conditional Use Restrictions	
Document the Conditional Use Restrictions	

Migration Strategy	
Document the Migration Strategy	

Impact Position Statement	
Document the Position Statement on Impact	

CURRENT STATUS				
Provide the Current Status)	☐ *In Development*	☐ *Under Review*	☒ *Approved*	☐ *Rejected*

AUDIT TRAIL			
Creation Date	11/28/2006	*Date Accepted / Rejected*	11/28/2006

Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			