COMPLIANCE COMPONENT

DEFINITION	
Name	Contingency Planning Process
Description	Contingency Planning Process is 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	• Identifies fundamental planning principles and practices to help personnel develop and maintain effective IT contingency plans 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	
Specify the Domain Name	Security
Specify the Discipline Name	Operational Controls
Specify the Technology Area Name	Contingency Planning
Specify the Product Component Name	

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

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	The contingency planning process describes the process to develop and maintain an effective information system contingency plan. The five steps in the process are: 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. • 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: o Roles and responsibilities o 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

- As information system contingency plans are developed during the Initiation phase of the System Development Life Cycle (SDLC), they should be coordinated with related organization-wide policies and programs, including information system security, physical security, human resources, system operations, and emergency preparedness functions. Information system contingency activities should be compatible with program requirements for these areas, and recovery personnel should coordinate with representatives from each area to remain aware of new or evolving policies, programs, or capabilities. The Contingency Plan must be written in coordination with other plans associated with each target system as part of organization-wide resilience strategy. Such plans include the following:
  - Information system security plans;
  - Facility-level plans
  - Organization-level plans

2. **Conduct the business impact analysis (BIA).** The BIA helps to identify and prioritize critical systems and components.

   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. Three steps are typically involved in accomplishing the BIA:

   - Determine mission/business processes and recovery criticality - Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission.
   - Identify resource requirements - Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
   - Identify recovery priorities for system resources - Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

3. **Identify preventive controls.** Measures taken to mitigate the effects of system disruptions can increase system availability.
   - 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.

   - 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. **Create contingency strategies.** Contingency strategies are created to cover the full range of backup, recovery, contingency planning, testing, and ongoing maintenance. The following should be considered when creating a contingency strategy:
    - Backup and Recovery - a means to restore system operations quickly and effectively following a service disruption. The methods and strategies should address disruption impacts and allowable downtimes identified in the BIA and should be integrated into the system architecture during the Development/Acquisition phase of the SDLC.
    - Backup Methods and Offsite Storage - System data should be backed up regularly. Policies should specify the minimum frequency and scope of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. Data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. It is good business practice to store backed-up data offsite. When selecting backup methods, agencies should consider the following:
        - Geographic area
        - Accessibility
        - Security
        - Environment
        - Cost
    - Alternate Sites – The different types of alternate sites to be considered are:
        - Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities, when needed.
        - Warm Sites are partially equipped office spaces that contain some or all the system hardware, software, telecommunications, and power sources.
        - Hot Sites are facilities appropriately equipped to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.
        - Mobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.
        - Mirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.
    - Equipment Replacement - If the information system is damaged or destroyed or the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. Three basic strategies exist to prepare for equipment replacement.
        - Vendor agreements - As the contingency plan is being developed, SLAs with hardware, software, and support vendors may be made for emergency maintenance service.
        - Equipment inventory - Required equipment may be purchased in advance and stored at a secure offsite location, such as an alternate site where recovery operations will take place (warm or mobile site) or at another location where they will be stored and then shipped to the alternate site.

- Existing compatible equipment - Equipment currently housed and used by the contracted hot site or by another organization within the organization may be used.

- Cost Considerations - The cost of each type of alternate site, equipment replacement, and storage option should be weighed against budget limitations.
- Roles and Responsibilities - Each team should be trained and ready to respond in the event of a disruptive situation requiring plan activation. Recovery personnel should be assigned to specific teams that will respond to the event, recover capabilities, and return the system to normal operations.

5. **Develop an IT contingency plan -** The contingency plan should contain detailed guidance and procedures for restoration. There are five main components of the contingency plan, as listed below:
    - **Supporting Information** - includes an introduction and concept of operations section providing essential background or contextual information that makes the contingency plan easier to understand, implement, and maintain.
    - **Activation and Notification Phase** - initial actions taken once a system disruption or outage has been detected or appears to be imminent. This phase includes activities to notify recovery personnel or teams, conduct an outage assessment, and activate the plan.
    - **Recovery Phase** - Formal recovery operations begin after the Contingency Plan has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation at an alternate system, or relocation and recovery at an alternate site. It is feasible that only system resources identified as high priority in the BIA will be recovered at this stage.
    - **Reconstitution Phase** - Recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. This phase consists of two major activities: validating successful recovery and deactivation of the plan.
    - **Plan Appendices** - Contingency plan appendices provide key details not contained in the main body of the plan. Common contingency plan appendices include the following:
        - Contact information for contingency planning team personnel;
        - Vendor contact information, including offsite storage and alternate site POCs;
        - BIA;
        - Detailed recovery procedures and checklists;
        - Detailed validation testing procedures and checklists;
        - 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;
        - Alternate mission/business processing procedures that may occur while recovery efforts are being done to the system;
        - Contingency Plan testing and maintenance procedures;

	○ System interconnections (systems that directly interconnect or exchange information); and ○ Vendor SLA's, reciprocal agreements with other organizations, and other vital records.
Document Source Reference #	NIST Special Publication 800-34, *Contingency Planning Guide for Federal Information Systems,* Rev. 1 (May, 2010) NIST Special Publication 800-53, *Security and Privacy Controls for information Systems and Organizations*, *CP – Contingency Planning.* Rev. 5 (Dec. 2020)

Compliance Sources			
Name	NIST Special Publication 800-34, *Contingency Planning Guide for Federal Information Systems,* Rev. 1 (May, 2010)	*Website*	NIST 800-34, Rev 1 Contingency Planning Guide for Federal Information Systems
Contact Information	inquiries@nist.gov		
Name	NIST Special Publication 800-53, *Security and Privacy Controls for information Systems and Organizations*, *CP – Contingency Planning.* Rev. 5 (Dec. 2020)	*Website*	SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC (nist.gov)
Contact Information			

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

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

COMPONENT SUB-CLASSIFICATION		
Sub-Classification	Date	Additional Sub-Classification Information
☐ *Technology Watch*		
☐ *Variance*		
☐ *Conditional Use*		

Rationale for Component Classification	
Document the Rationale for Component Classification	

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 Approved / Rejected*	11/28/2006
Reason for Rejection			
Last Date Reviewed	1/10/2024	*Last Date Updated*	1/12/2024
Reason for Update	Vitality		