Compliance Component

DEFINITION

Name	Contingency Plan Testing, Maintenance and Training
Description	Contingency Plan Testing, Maintenance and Training is the process of testing the plan against test objectives and success criteria, maintaining the plan in a ready state, and training contingency plan personnel.
Rationale	Contingency plans should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. Scheduled reviews and updates ensure new information is documented and contingency measures are revised to maintain the contingency plan in a ready state. Training prepares contingency plan personnel for an actual event to the extent that they are able to execute recovery procedures.
Benefits	• Testing enables plan deficiencies to be identified and addressed • During maintenance, the plan is reviewed for accuracy and completeness • Training familiarizes personnel with the processes and procedures of the contingency plan • Testing helps evaluate the ability of the recovery staff to implement the plan quickly and effectively

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	**Plan Testing.** Testing the plan identifies gaps and omissions. The following areas should be addressed in contingency testing: • System recovery on an alternate platform from backup media • Coordination among recovery teams • Internal and external connectivity • System performance using alternate equipment • Restoration of normal operations

- Notification procedures

The test plan should include a schedule detailing the timeframes for each test and test participants. The test plan should also delineate clear scope, scenario, and logistics. The scenario chosen may be a worst-case incident or an incident most likely to occur. It should mimic reality as closely as possible. There are two basic formats for exercises:

- **Classroom Exercises.** Participants in classroom exercises, often called tabletop, walk through the procedures without any actual recovery operations occurring. Classroom exercises are the most basic and least costly of the two types of exercises and should be conducted before performing a functional exercise.
- **Functional Exercises.** Functional exercises are more extensive than tabletops, requiring the event to be a simulation. Often, scripts are written out for role players pretending to be external organization contacts, or there may be actual interagency and vendor participation. A functional exercise might include actual relocation to the alternate site or system cutover.

It is important that an exercise never disrupt normal operations. Test results and lessons learned should be documented and reviewed by test participants and other personnel as appropriate. Information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the contingency plan. Testing should be performed, as a minimum, on an annual basis.

Plan Maintenance. The plan should be a dynamic document that is updated regularly to remain current with system enhancements. As a general rule, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists. At a minimum, plan reviews should focus on the following elements:

- Operational requirements
- Security requirements
- Technical procedures
- Hardware, software, and other equipment (types, specifications, and amount)
- Names and contact information of team members
- Names and contact information of vendors, including alternate and off-site vendor points-of-contact.
- Alternate and offsite facility requirements
- Vital records (electronic and hardcopy)

Because the IT contingency plan contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled. A copy should also be stored at the alternate site and with the backup media.

Other information that should be stored with the plan includes contracts with vendors (service level agreements and other contracts), software licenses, system user manuals, security manuals, and operating procedures.

Changes made to the plan should be coordinated, communicated and recorded.

Supporting information should be evaluated to ensure that the information is current and continues to meet system requirements adequately. This information includes the following:

- Alternate site contract, including testing times
- Off-site storage contract
- Software licenses
- Memorandums of Understanding or vendor Service Level Agreements
- Hardware and software requirements
- System interconnection agreements
- Security requirements
- Recovery strategy
- Polices that address contingency situations
- Training and awareness materials
- Testing scope

When the Business Impact Analysis is reviewed, updates should be reflected in the plan.

Training. Training prepares recovery personnel for plan activation; improves plan effectiveness and overall agency preparedness. Training for personnel with contingency plan responsibilities should complement testing. Training should be provided at least annually; new hires who will have plan responsibilities should receive training shortly after they are hired. Personnel should be trained to recognize the need to adjust the plan to the circumstances. Recovery personnel should be trained on the following plan elements:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Notification, Activation, Recovery, and Reconstitution Phases)
- Individual responsibilities (Notification, Activation, Recovery, and Reconstitution Phases)

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, alternate, restoration, exercises, storage, backup, reconstitution, BIA.			
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	10/27/2006	*Date Accepted / Rejected*	11/28/2006	
Reason for Rejection				
Last Date Reviewed		*Last Date Updated*		
Reason for Update				