Topics:
continuity [2], disaster recovery [3], operations [4]

# Contingency Planning [1]

SS-08-045 Contingency Planning

Issue Date: 3/31/2008

Revision Effective Date: 3/31/2008

## PURPOSE

A computer security event has the potential to disrupt computer operations thereby disrupting critical mission and business functions. The need to maintain security and other regulatory requirements does not go away when an organization is processing in contingency mode. Contingency planning directly supports an organization?s goal of continued operations while maintaining the necessary protection levels.

Contingency planning allows an organization to plan ahead and develop interim measures necessary to recover, restore or maintain critical business and IT operations following or during an emergency or system disruption. Business and IT operations are vulnerable to three classifications of threats:

- **Natural**?e.g., hurricane, tornado, flood, and fire
- **Human**?e.g., operator error, sabotage, implant of malicious code, and terrorist attacks
- **Environmental**?e.g., equipment failure, software error, telecommunications network outage, and electric power failure

This standard outlines the requirements for developing and implementing a plan for continuing or recovering critical operations during and/or after an emergency or disruption.

## STANDARD

Agencies shall identify the potential risks that may adversely impact their critical business functions and develop continuity and recovery strategies and plans designed to ensure the availability of the agencies? essential functions, services and communications in the event of a natural, man-made, or environmental emergency or disruption.

Agency heads shall create and implement a management structure for business continuity within the agency to include a named Business Continuity Coordinator and for directing the development and execution of a viable disaster recovery and business continuity program.

The Business Continuity Coordinator shall:

- Coordinate with internal and external points of contact (POC) associated with the critical business functions to conduct a Business Impact Analysis (BIA).
    - The BIA shall provide information that:
        - Identifies critical business functions, services, and interdependencies
        - Links critical services and functions to support resources (technology, staff and facilities)
        - Characterizes the system requirements, processes, and interdependencies
        - Identifies disruption impacts including financial and non-financial losses
        - Estimates allowable outage times
        - Determines contingency requirements and priorities