Business Continuity Planning Procedures and Guidelines

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545mai_060106_cd44

Information System Security
Business Continuity Planning Procedures and Guidelines
for System Owners, Information System Security Officers, and System Administrators

1. Introduction

This document defines the procedures and guidelines that you must follow to develop, test, and maintain a USAID information system Business Continuity Plan (BCP). USAID has streamlined them from the guidance provided in NIST Special Publication 800-34, **Contingency Planning Guide for Information Technology Systems**.

2. Business Continuity Planning

Business continuity planning is the process of making certain that business functions, handled by USAID information systems, remain uninterrupted through time. It involves successfully mitigating risks to the system from natural, manmade, or environmental threats, and building resilient systems that can overcome the risks identified during system assessment.

Business continuity planning consists of the following steps:

1. Identifying and prioritizing business critical systems, functions and resources,
2. Identifying critical resources,
3. Identifying potential threats and preventive controls to mitigate risk,
4. Designating responsibilities,
5. Implementing and maintaining the Business Continuity Plan, and
6. Validating the Business Continuity Plan.

Business continuity planning is an on-going, dynamic process that continues throughout the information systems life cycle. See the flowchart on page 4 for a graphic depiction of this process.

2.1 Identifying and Prioritizing Critical Functions, Systems and Processes

Information systems can be very complex, fulfilling many business functions. Your **first step** in business continuity planning is to identify and then to prioritize the USAID critical functions, systems, and processes. As a business continuity planner, you must obtain input from Executive and Functional Managers to determine each system's criticality.

2.2 Identifying Critical Resources

Your **second step** in business continuity planning is to identify the resources that are critical to the information systems that support the functions, systems and processes that you identified in step one. The critical resources that you identified should include everything necessary to support the critical function, system or process. Some examples of critical resources are:

- Servers, workstations, and peripherals,
- Applications and data,
- Media and output,
- Telecommunications connections,
- Physical Infrastructure (e.g. electrical power, environmental controls), and
- Personnel.

2.3 Identifying Potential Threats and Preventive Controls

Your **third step** is to identify the most likely potential threats that could occur, which would interrupt your business or information system's functions. In your Business Continuity Plan, you must identify the *likely* range of threats, since you cannot identify and mitigate all threats. Potential threats fall into three main categories: natural, manmade, and environmental. Some examples for each category are shown in the table below:

Natural Threats	Man-Made Threats	Environmental Threats
Hurricane	Arson	Equipment Failure
Tornado	Theft	Network Failure
Flood	Sabotage	HVAC Failure
Snowstorm	Terrorist Act	Power Failure
Earthquake	Malicious Software Attack	Electrical Fire
Electrical Storm	Human Error	Fire
Monsoon	War	Database Corruption

This table lists some potential threats; each threat is listed by its type.

After you identify potential threats, you must identify preventive controls that can mitigate the identified risks. Within your Business Continuity Plan, you must develop a Plan of Actions and Milestones that details the implementation and testing schedule for the preventive controls. Various preventive controls may apply to your information systems, dependent upon its configuration. Natural and other threats can be mitigated through the careful selection of the business continuity site. Some common measures for manmade and environmental threats are listed below.

- Uninterruptible power supplies or fuel-powered generators,
- Air conditioning systems,
- Fire and smoke detectors and a combustion suppression system,
- Water sensors,

- Heat-resistant and waterproof container for backup media and vital non-electronic records,
- Emergency master system shutdown switch,
- Offsite backup storage of media, non-electronic records, and system documentation,
- Technical security controls, and
- Frequent, scheduled backups.

You must document these preventive controls in your Business Continuity Plan, and you must train the personnel that support your business function, system, or process in "when" and "how" to apply the controls.

2.4 Designate Responsibilities

Your **fourth step** in business continuity planning is to designate responsibility for key activities identified within the Business Continuity Plan. You must identify the personnel designated to perform these key activities and train them to perform their duties, as outlined in the Business Continuity Plan.

2.5 Implement and Maintain the Business Continuity Plan

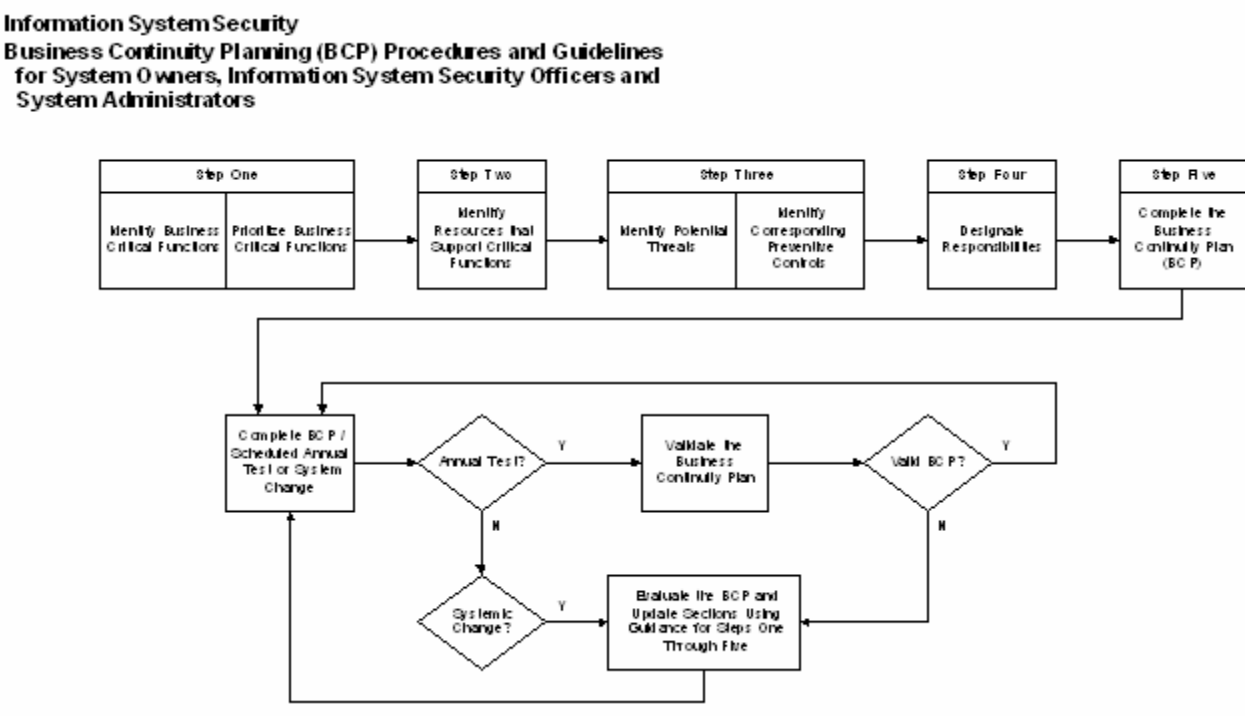
As you take the first four steps, you will populate the sections of the Business Continuity Plan. Once populated, you must keep the Business Continuity Plan up-to-date and securely store it for use during periods whenever business functionality is threatened. Whenever there are changes to the information system, you must update the Business Continuity Plan. You must also validate it annually.

2.6 Validating the Business Continuity Plan

When you test the Business Continuity Plan to validate that it is sufficient, you ***must never disrupt*** normal operation of the information system without the express consent of the System Owner, the CISO, and USAID Executive Management. You must produce test reports and evaluate them with the CISO to determine if the Business Continuity Plan is sufficient to support your business function, system or process. If necessary, you must revise the Business Continuity Plan.

You must submit a copy of the initial BCP to the CISO. When there are subsequent updates, you must submit copies to the CISO. You must submit a **Business Continuity Plan Annual Validation Letter** to the CISO at the conclusion of validation testing. [Note: this document is only available on the USAID intranet. Please contact **ads@usaid.gov** if you need a copy.]

The following flowchart represents the simplified USAID Business Continuity Plan development process, as fully described in NIST Special Publication 800-34, **Contingency Planning Guide for Information Technology Systems.**



The above graphic shows the decisions and steps involved in Business Continuity Planning as described in this document.

References

The **Business Continuity Plan Template** [Note: this document is only available on the USAID intranet. Please contact **ads@usaid.gov** if you need a copy.] can be used for USAID information systems. You can find supplemental guidance in the following documents:

- Federal Preparedness Circular (FPC) 65, **Federal Executive Branch Continuity of Operations**, June 2004.
- NIST Federal Information Processing Standard Publication (FIPS PUB) 87, **Guidelines for ADP Contingency Planning**, March 1981 (superceded by SP 800-34). [Note: this document is only available on the USAID intranet. Please contact **ads@usaid.gov** if you need a copy.]
- NIST Special Publication 800-12, **An Introduction to Computer Security: The NIST Handbook**, Chapter 11, October 1995.
- NIST Special Publication 800-34, **Contingency Planning Guide for Information Technology Systems**, June 2002.
- Presidential Decision Directive (PDD) 63, **Critical Infrastructure Protection**, May 1998.