
Unit 2: Requirements for Continuity Planning

Objectives

At the end of this unit, you should be able to:

1. Describe the requirements of National Security Presidential Directive (NSPD) 51/Homeland Security Presidential Directive (HSPD) 20.
 2. Describe the guidance in Federal Continuity Directive (FCD) 1.
 3. Identify the objectives of Continuity of Operations.
 4. List the roles and responsibilities of the key players in a continuity program.
-

Scope

- Unit Overview and Objectives
 - Purpose and Goals of a Continuity Program
 - Continuity Planning Objectives
 - Legal Basis for Continuity of Operations
 - Continuity Roles and Responsibilities
 - Summary and Transition
-

Time Plan

The suggested time plan for this unit is shown below.

Topic	Time
Unit Overview and Objectives	5 minutes
Purpose and Goals of a Continuity Program	10 minutes
Continuity Planning Objectives	20minutes
Legal Basis for Continuity of Operations	15 minutes
Continuity Roles and Responsibilities	25 minutes
Summary and Transition	5 minutes
Total Time	1 hour 20 minutes

**Unit 2: Requirements for
Continuity Planning**

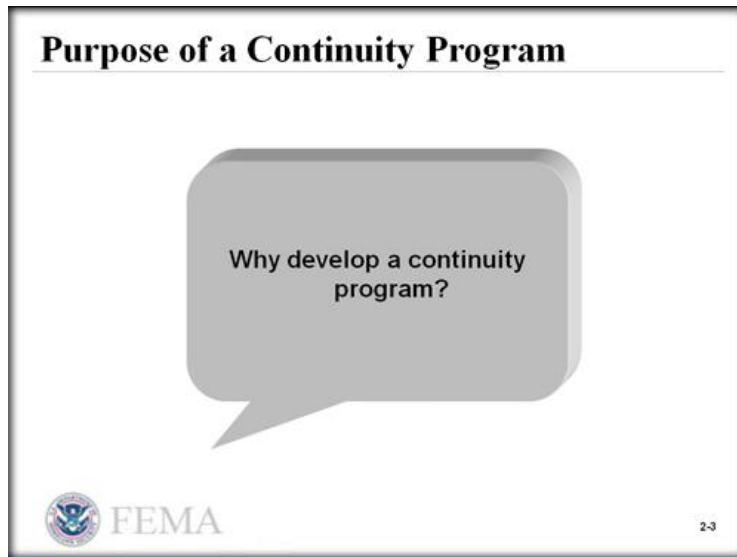


Unit Objectives

- Describe the requirements of NSPD 51/HSPD 20.
- Describe the guidance in FCD 1 and CGC 1.
- Identify the objectives of Continuity of Operations.
- List the roles and responsibilities of the key players in a continuity program.



2-2



Purpose of a Continuity Program

To document and ensure the capability of continuing agency essential functions during a wide range of potential emergencies.

Goals:

- Protect life and property.
- Provide for the continuity of essential services until normal operations can be resumed.



FEMA

2-4

Continuity Planning Objectives

What are some of the objectives realized by planning for Continuity of Operations?



2-5

Continuity Planning Objectives

Continuity planning helps to:

- Ensure continued performance during a continuity situation.
- Reduce loss of life and minimize damage and loss to critical processes and information.
- Ensure successful succession to office.
- Anticipate what might occur in order to mitigate disruptions.
- Ensure that facilities are available during a continuity situation.



2-6

Continuity Planning Objectives

Continuity planning helps to:

- Protect essential facilities, equipment, and vital records.
- Achieve a timely and orderly recovery from a continuity situation.
- Resume full service after an effective reconstitution.
- Maintain a test, training, and exercise program that supports the implementation of continuity plans.



Legal Basis for Continuity of Operations

- Continuity of Operations is a Federal initiative, required by Presidential directive.
- Federal Executive Branch agencies are required to continue their essential functions under a broad range of circumstances.



2-8

Federal directives apply only as guidance to State, local, tribal, and other organizations and entities. Organizations at all levels of government, as well as nongovernmental organizations (NGOs), can benefit from Federal directives and guidance for their continuity planning.

Key Federal Directives/Guidance

- To ensure continuity of essential functions:
[NSPD 51/HSPD 20, issued May 2007](#)
- To provide guidance for continuity of essential functions during all-hazard situations:
[FCD 1, issued February 2008](#)
[CGC 1, issued January 2009](#)



NSPD 51/HSPD 20

- Requires all Federal Executive Branch agencies to incorporate continuity into their daily operations
- Establishes NEFs for all continuity programs
- Assigns categories to each agency in accordance with its national security role and responsibilities
- Designates the National Continuity Coordinator to lead the development of a National Continuity Implementation Plan



FEMA

2-10

NSPD 51/HSPD 20 Requirements

Continuity plans must include:

- Plans to continue performance of PMEFs for 30 days or until normal operations can be resumed.
- Capability to be fully operational at continuity sites within 12 hours after plan activation.
- Orders of succession and delegations of authorities.
- Measures to safeguard and access vital records and resources.
- Provisions for acquiring resources for continued operations.



2-11

NSPD 51/HSPD 20 Requirements

Continuity plans must include:

- Redundant communications capabilities at continuity sites.
- Identification, training, and preparedness of the ERG.
- Reconstitution capabilities.



2-12

NSPD 51/HSPD 20—National Continuity Policy (Unclassified)

UNCLASSIFIED WITH TOP SECRET/CODEWORD ANNEXES

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD 51
HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD 20

Subject: National Continuity Policy

Purpose

(1) This directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. This policy establishes "National Essential Functions," prescribes continuity requirements for all executive departments and agencies, and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

Definitions

(2) In this directive:

- (a) "Category" refers to the categories of executive departments and agencies listed in Annex A to this directive;
- (b) "Catastrophic Emergency" means any incident, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the U.S. population, infrastructure, environment, economy, or government functions;
- (c) "Continuity of Government," or "COG," means a coordinated effort within the Federal Government's executive branch to ensure that National Essential Functions continue to be performed during a Catastrophic Emergency;
- (d) "Continuity of Operations" means an effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies;

NSPD 51/HSPD 20—National Continuity Policy (Unclassified) (Continued)

- (e) "Enduring Constitutional Government," or "ECG," means a cooperative effort among the executive, legislative, and judicial branches of the Federal Government, coordinated by the President, as a matter of comity with respect to the legislative and judicial branches and with proper respect for the constitutional separation of powers among the branches, to preserve the constitutional framework under which the Nation is governed and the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the National Essential Functions during a catastrophic emergency;
- (f) "Executive Departments and Agencies" means the executive departments enumerated in 5 U.S.C. 101, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the United States Postal Service;
- (g) "Government Functions" means the collective functions of the heads of executive departments and agencies as defined by statute, regulation, presidential direction, or other legal authority, and the functions of the legislative and judicial branches;
- (h) "National Essential Functions," or "NEFs," means that subset of Government Functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through Continuity of Operations and Continuity of Government capabilities; and
- (i) "Primary Mission Essential Functions," or "PMEFs," means those Government Functions that must be performed in order to support or implement the performance of NEFs before, during, and in the aftermath of an emergency.

Policy

- (3) It is the policy of the United States to maintain a comprehensive and effective continuity capability composed of Continuity of Operations and Continuity of Government programs in order to ensure the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions.

Implementation Actions

- (4) Continuity requirements shall be incorporated into daily operations of all executive departments and agencies. As a result of the asymmetric threat environment, adequate warning of potential emergencies that could pose a significant risk to the homeland might not be available, and therefore all continuity planning shall be based on the assumption that no such warning will be received. Emphasis will be placed upon geographic dispersion of leadership, staff, and infrastructure in order to increase survivability and maintain uninterrupted Government Functions. Risk management principles shall be applied to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.

NSPD 51/HSPD 20—National Continuity Policy (Unclassified) (Continued)

(5) The following NEFs are the foundation for all continuity programs and capabilities and represent the overarching responsibilities of the Federal Government to lead and sustain the Nation during a crisis, and therefore sustaining the following NEFs shall be the primary focus of the Federal Government leadership during and in the aftermath of an emergency that adversely affects the performance of Government Functions:

(a) Ensuring the continued functioning of our form of government under the Constitution, including the functioning of the three separate branches of government;

(b) Providing leadership visible to the Nation and the world and maintaining the trust and confidence of the American people;

(c) Defending the Constitution of the United States against all enemies, foreign and domestic, and preventing or interdicting attacks against the United States or its people, property, or interests;

(d) Maintaining and fostering effective relationships with foreign nations;

(e) Protecting against threats to the homeland and bringing to justice perpetrators of crimes or attacks against the United States or its people, property, or interests;

(f) Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident;

(g) Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems; and

(h) Providing for critical Federal Government services that address the national health, safety, and welfare needs of the United States.

(6) The President shall lead the activities of the Federal Government for ensuring constitutional government. In order to advise and assist the President in that function, the Assistant to the President for Homeland Security and Counterterrorism (APHS/CT) is hereby designated as the National Continuity Coordinator. The National Continuity Coordinator, in coordination with the Assistant to the President for National Security Affairs (APNSA), without exercising directive authority, shall coordinate the development and implementation of continuity policy for executive departments and agencies. The Continuity Policy Coordination Committee (CPCC), chaired by a Senior Director from the Homeland Security Council staff, designated by the National Continuity Coordinator, shall be the main day-to-day forum for such policy coordination.

NSPD 51/HSPD 20—National Continuity Policy (Unclassified) (Continued)

(7) For continuity purposes, each executive department and agency is assigned to a category in accordance with the nature and characteristics of its national security roles and responsibilities in support of the Federal Government's ability to sustain the NEFs. The Secretary of Homeland Security shall serve as the President's lead agent for coordinating overall continuity operations and activities of executive departments and agencies, and in such role shall perform the responsibilities set forth for the Secretary in sections 10 and 16 of this directive.

(8) The National Continuity Coordinator, in consultation with the heads of appropriate executive departments and agencies, will lead the development of a National Continuity Implementation Plan (Plan), which shall include prioritized goals and objectives, a concept of operations, performance metrics by which to measure continuity readiness, procedures for continuity and incident management activities, and clear direction to executive department and agency continuity coordinators, as well as guidance to promote interoperability of Federal Government continuity programs and procedures with State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate. The Plan shall be submitted to the President for approval not later than 90 days after the date of this directive.

(9) Recognizing that each branch of the Federal Government is responsible for its own continuity programs, an official designated by the Chief of Staff to the President shall ensure that the executive branch's Continuity of Operations and Continuity of Government policies in support of ECG efforts are appropriately coordinated with those of the legislative and judicial branches in order to ensure interoperability and allocate national assets efficiently to maintain a functioning Federal Government.

(10) Federal Government Continuity of Operations, Continuity of Government, and ECG plans and operations shall be appropriately integrated with the emergency plans and capabilities of State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to promote interoperability and to prevent redundancies and conflicting lines of authority. The Secretary of Homeland Security shall coordinate the integration of Federal continuity plans and operations with State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to provide for the delivery of essential services during an emergency.

(11) Continuity requirements for the Executive Office of the President (EOP) and executive departments and agencies shall include the following:

(a) The continuation of the performance of PMEFs during any emergency must be for a period up to 30 days or until normal operations can be resumed, and the capability to be fully operational at continuity sites as soon as possible after the occurrence of an emergency, but not later than 12 hours after continuity activation;

NSPD 51/HSPD 20—National Continuity Policy (Unclassified) (Continued)

- (b) Succession orders and pre-planned devolution of authorities that ensure the emergency delegation of authority must be planned and documented in advance in accordance with applicable law;
 - (c) Vital resources, facilities, and records must be safeguarded, and official access to them must be provided;
 - (d) Provision must be made for the acquisition of the resources necessary for continuity operations on an emergency basis;
 - (e) Provision must be made for the availability and redundancy of critical communications capabilities at continuity sites in order to support connectivity between and among key government leadership, internal elements, other executive departments and agencies, critical partners, and the public;
 - (f) Provision must be made for reconstitution capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations; and
 - (g) Provision must be made for the identification, training, and preparedness of personnel capable of relocating to continuity facilities to support the continuation of the performance of PMEFS.
- (12) In order to provide a coordinated response to escalating threat levels or actual emergencies, the Continuity of Government Readiness Conditions (COGCON) system establishes executive branch continuity program readiness levels, focusing on possible threats to the National Capital Region. The President will determine and issue the COGCON Level. Executive departments and agencies shall comply with the requirements and assigned responsibilities under the COGCON program. During continuity activation, executive departments and agencies shall report their readiness status to the Secretary of Homeland Security or the Secretary's designee.
- (13) The Director of the Office of Management and Budget shall:
- (a) Conduct an annual assessment of executive department and agency continuity funding requests and performance data that are submitted by executive departments and agencies as part of the annual budget request process, in order to monitor progress in the implementation of the Plan and the execution of continuity budgets;
 - (b) In coordination with the National Continuity Coordinator, issue annual continuity planning guidance for the development of continuity budget requests; and
 - (c) Ensure that heads of executive departments and agencies prioritize budget resources for continuity capabilities, consistent with this directive.

NSPD 51/HSPD 20—National Continuity Policy (Unclassified) (Continued)

- (14) The Director of the Office of Science and Technology Policy shall:
- (a) Define and issue minimum requirements for continuity communications for executive departments and agencies, in consultation with the APHS/CT, the APNSA, the Director of the Office of Management and Budget, and the Chief of Staff to the President;
 - (b) Establish requirements for, and monitor the development, implementation, and maintenance of, a comprehensive communications architecture to integrate continuity components, in consultation with the APHS/CT, the APNSA, the Director of the Office of Management and Budget, and the Chief of Staff to the President; and
 - (c) Review quarterly and annual assessments of continuity communications capabilities, as prepared pursuant to section 16(d) of this directive or otherwise, and report the results and recommended remedial actions to the National Continuity Coordinator.
- (15) An official designated by the Chief of Staff to the President shall:
- (a) Advise the President, the Chief of Staff to the President, the APHS/CT, and the APNSA on COGCON operational execution options; and
 - (b) Consult with the Secretary of Homeland Security in order to ensure synchronization and integration of continuity activities among the four categories of executive departments and agencies.
- (16) The Secretary of Homeland Security shall:
- (a) Coordinate the implementation, execution, and assessment of continuity operations and activities;
 - (b) Develop and promulgate Federal Continuity Directives in order to establish continuity planning requirements for executive departments and agencies;
 - (c) Conduct biennial assessments of individual department and agency continuity capabilities as prescribed by the Plan and report the results to the President through the APHS/CT;
 - (d) Conduct quarterly and annual assessments of continuity communications capabilities in consultation with an official designated by the Chief of Staff to the President;
 - (e) Develop, lead, and conduct a Federal continuity training and exercise program, which shall be incorporated into the National Exercise Program developed pursuant to Homeland Security Presidential Directive-8 of December 17, 2003 ("National Preparedness"), in consultation with an official designated by the Chief of Staff to the President;

NSPD 51/HSPD 20—National Continuity Policy (Unclassified) (Continued)

- (f) Develop and promulgate continuity planning guidance to State, local, territorial, and tribal governments, and private sector critical infrastructure owners and operators;
- (g) Make available continuity planning and exercise funding, in the form of grants as provided by law, to State, local, territorial, and tribal governments, and private sector critical infrastructure owners and operators; and
- (h) As Executive Agent of the National Communications System, develop, implement, and maintain a comprehensive continuity communications architecture.
- (17) The Director of National Intelligence, in coordination with the Attorney General and the Secretary of Homeland Security, shall produce a biennial assessment of the foreign and domestic threats to the Nation's continuity of government.
- (18) The Secretary of Defense, in coordination with the Secretary of Homeland Security, shall provide secure, integrated, Continuity of Government communications to the President, the Vice President, and, at a minimum, Category I executive departments and agencies.
- (19) Heads of executive departments and agencies shall execute their respective department or agency continuity plans in response to a localized emergency and shall:
- (a) Appoint a senior accountable official, at the Assistant Secretary level, as the Continuity Coordinator for the department or agency;
- (b) Identify and submit to the National Continuity Coordinator the list of PMEFs for the department or agency and develop continuity plans in support of the NEFs and the continuation of essential functions under all conditions;
- (c) Plan, program, and budget for continuity capabilities consistent with this directive;
- (d) Plan, conduct, and support annual tests and training, in consultation with the Secretary of Homeland Security, in order to evaluate program readiness and ensure adequacy and viability of continuity plans and communications systems; and
- (e) Support other continuity requirements, as assigned by category, in accordance with the nature and characteristics of its national security roles and responsibilities

General Provisions

- (20) This directive shall be implemented in a manner that is consistent with, and facilitates effective implementation of, provisions of the Constitution concerning succession to the Presidency or the exercise of its powers, and the Presidential Succession Act of 1947 (3 U.S.C. 19), with consultation of the Vice President and, as appropriate, others involved. Heads of executive departments and agencies shall ensure that appropriate support is available to the Vice President and others involved as necessary to be prepared at all times to implement those provisions.

NSPD 51/HSPD 20—National Continuity Policy (Unclassified) (Continued)

(21) This directive:

(a) Shall be implemented consistent with applicable law and the authorities of agencies, or heads of agencies, vested by law, and subject to the availability of appropriations;

(b) Shall not be construed to impair or otherwise affect (i) the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals, or (ii) the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President, to the Secretary of Defense, to the commander of military forces, or military command and control procedures; and

(c) Is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person

(22) Revocation. Presidential Decision Directive-67 of October 21, 1998 ("Enduring Constitutional Government and Continuity of Government Operations"), including all Annexes thereto, is hereby revoked.

(23) Annex A and the classified Continuity Annexes, attached hereto, are hereby incorporated into and made a part of this directive.

(24) Security. This directive and the information contained herein shall be protected from unauthorized disclosure, provided that, except for Annex A, the Annexes attached to this directive are classified and shall be accorded appropriate handling, consistent with applicable Executive Orders.

FCD 1 and CGC 1

FCD 1:

- Provides direction to the Federal Executive Branch for developing continuity plans and programs to support continuation of NEFs.
- Identifies three supporting components and 10 primary elements for a viable continuity capability.

CGC 1:

- Mirrors FCD 1 content
- Provides guidance to non-Federal entities



2-13

The ultimate goal of continuity in the Federal Executive Branch is the continuation of National Essential Functions. For non-Federal agencies, continuity planning facilitates the performance of essential functions during all-hazard emergencies or other situations that may disrupt normal operations.

FCD 1 provides direction to the Federal Executive Branch for developing continuity plans and programs. FCD 1 identifies three supporting components and 10 primary elements of a viable continuity capability, which will be described next.

CGC 1 provides guidance to non-Federal entities.

FCD/CGC 1 Support Component 1

Continuity Plans and Procedures:

- Developing effective plans and procedures includes a TT&E program and the operational capability to implement the plans and procedures.
- Establishing planning and procedural objectives and requirements is an essential part of developing a viable continuity plan.



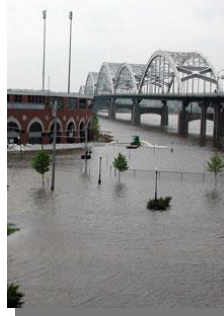
2-14

FCD/CGC 1 Support Component 2

Risk Management:

A structured process for understanding the problems facing an organization:

- What can go wrong?
- How bad can it get? How fast?
- What is the likelihood that the undesired event might occur?
- What would be the impact should it occur?



2-15

The second component identified in FCD 1/CGC 1 is risk management.

A risk (or hazard) analysis model outlines the steps for a risk management process. Refer to the Risk Management Model on the following page.

Steps in the Risk Management Model

1. Inventory the critical functions provided by the organization. The analysis team should leverage the functions identified during the PMEF Identification and Analysis process.
2. Identify the hazards that can impact delivery of the critical functions. This step would include exploring potential natural events, intentional human-caused events, and nonintentional human-caused events that could adversely affect the ability of the organization to perform PMEFs. Natural hazards are those where the occurrence is beyond the control of the organization, including earthquakes, floods, ice storms, winter weather, and external fires. Intentional human-caused hazards are also beyond the direct control of the organization and could include events such as external sabotage and terrorism. Nonintentional human-caused events, such as power outages, fires, explosions, equipment failures, or human errors are generally within the control of the organization.
3. Develop continuity hazard scenarios. All of the assessment steps should be performed within the context of a set of scenarios, each of which is a unique combination of a particular hazard and the organization's PMEF. Within each scenario, the analysis team should consider risks to all four continuity pillars, as appropriate, recognizing that in most cases, all of the pillars must be available in order to deliver the function. The following steps outline the elements of the scenario risk assessment:
 - Determine the risk information needed to assess the risk. Describe the information necessary to assess the risk for each scenario. For each information item, specify the information type, precision, and certainty required, and the analysis resources available.
 - Assess the risk. For each scenario, the analysis team should assess the threat, vulnerability, and consequence, where:
 - a. Threat is the likelihood of a type of attack that might be attempted, or that the scenario will occur.
 - b. Vulnerability is the likelihood that an attacker would succeed with a particular attack type, or that the scenario will result in the expected level of consequence.
 - c. Consequence is the potential impact of a particular attack, or the negative impact of the scenario.

For this effort, consequence should be expressed in terms of failure to deliver the National Essential Functions (NEFs) (see Annex D). When evaluating consequences, the analysis team should consider both short- and long-term impacts for disasters and accidents, as well as intended and unintended effects from intentional attacks.

Depending on the nature of the scenario, the analysis team can use different tools to assess the scenario's risk. For instance, the team may be able to leverage historical accident reporting databases to assess the risk of accident scenarios, while detailed stochastic models may be available for assessing the risk of natural hazard scenarios. For scenarios where historical data or detailed modeling are scarce, subject matter expertise must be leveraged to produce the risk assessment.
 - Identify existing safeguards/countermeasures. For each scenario, the analysis team should identify the existing safeguards that are in place to reduce either the likelihood (e.g., security countermeasures) or consequence (e.g., redundant capabilities) of the hazard.

Steps in the Risk Management Model (Continued)

4. **Evaluation of alternatives.** For many scenarios, the current risk may be considered to be at an acceptable level. For those scenarios where the current level of risk is deemed to be unacceptable, action(s) must be taken to mitigate the risk. These actions must (1) provide a beneficial return on investment, (2) be acceptable to stakeholders, and (3) not cause other significant risk. Critical steps in this phase include:
 - **Developing alternative risk management strategies.** The analysis team should engage the appropriate stakeholders to determine how the risks for each scenario can be managed most effectively. These alternative strategies should be developed completely and documented by addressing all of the critical factors (e.g., cost, schedule).
 - **Assessing the risk impact of the proposed strategies.** The analysis team should reassess the risk of each scenario based on the implementation of each alternative strategy. This step will provide the risk reduction value of each of the alternative strategies.

5. **Management selection.** After alternative strategies have been developed fully, and their risk reduction value has been quantified, the risk management process moves to the management selection phase, where decisionmakers choose the collection of alternatives for implementation. The alternatives will be evaluated based on consideration of all of the previously identified critical factors, including effectiveness (risk reduction), efficiency, and cost effectiveness.

Another critical factor that should be considered is the confidence or belief that the alternative will achieve the projected level of performance. The effect of many of the alternative strategies may be well understood by the organization. For instance, these alternatives may have a proven track record of performance within other similar organizations, or they may have been extensively studied. The performance of other alternatives with less of a history may not be as well understood. The analysis team may believe that these less understood alternatives will achieve a level of satisfactory performance; however, their confidence is at a lower level.

During the management selection phase, decisionmakers need an understanding of both anticipated performance and confidence to ensure that the proper suite of actions is taken. Finally, decisionmakers must recognize that this process is cyclical, and many of the alternatives will be implemented in subsequent cycles because of limitations in resources and time.

Steps in the Risk Management Model (Continued)

6. Implementation and monitoring. Critical steps in this phase include:
- Implementing the chosen mitigation strategies. This step involves the implementation of the mitigation strategies identified during the management selection phase. These strategies should reduce the risk that the organization will be unable to meet the continuity requirements.
 - Developing metrics to measure effectiveness. The analysis team must develop a collection of metrics, both qualitative and quantitative, to measure the organization's ability to meet the continuity requirements. The metrics identified in NSPD 51/HSPD 20, Paragraph 11, for each of the continuity requirements, should serve as a guide in crafting the metrics.
 - Monitoring organizational performance. After the strategies have been implemented and the metrics have been developed, the organization should monitor the effectiveness of the actions taken to manage risk. The goal of the monitoring phase is to verify that the organization is getting the expected results from its risk management decisions. Key inputs into the monitoring phase include testing, training, and exercising. The results of the monitoring step will inform subsequent iterations of the risk management cycle.

Extracted from FCD 1. More information about the Risk Management process is included in the Continuity Planners Course.

FCD/CGC 1 Support Component 3

Budgeting and Acquisition of Resources:

Agencies must align and allocate the budgetary resources necessary to implement and manage the continuity program.



2-16

The third component identified in FCD 1/CGC 1 is budgeting and acquisition of resources.

FCD/CGC 1 Support Component 3

What resources do you need
to consider when you
complete budgeting and
acquisition?



2-17

FCD/CGC 1 Support Component 3

Budgeting and Acquisition of Resources:

- Human capital
- Communications
- Facilities
- Infrastructure (systems, etc.)
- Transportation



2-18

This list is not inclusive. Budgeting and acquisition should include all of the essential elements for a viable continuity program. These elements will be covered next.

FCD/CGC 1 Primary Elements

10 elements ensure a viable continuity program:

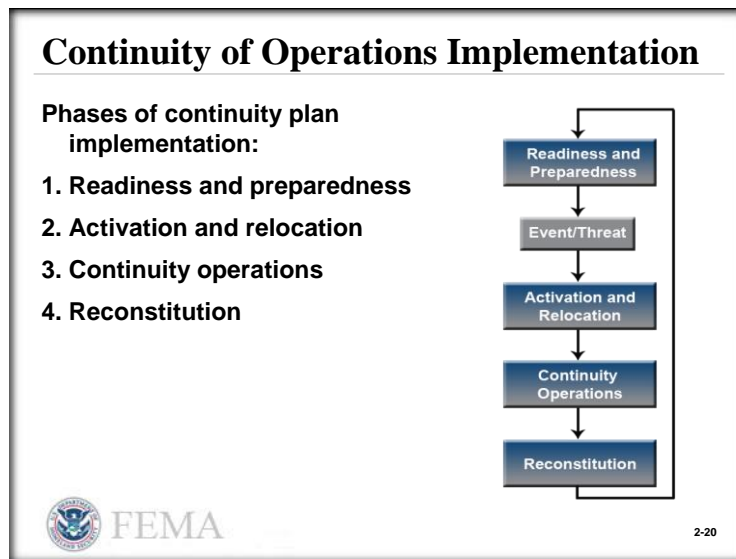
- Essential functions
- Orders of succession
- Delegations of authority
- Continuity facilities
- Continuity communications
- Vital records management
- Human capital
- Tests, training, and exercises
- Devolution of control and direction
- Reconstitution operations



FEMA

2-19

These primary elements for a viable continuity plan will be covered in detail in the next two units.



A continuity plan is implemented to ensure the continuation or rapid resumption of essential functions during a continuity event. Implementation of the continuity plan should be based on a pre-established decisionmaking process that allows for a review of the emergency and a determination of the best course of action based on the agency's readiness posture.

Continuity Roles and Responsibilities

FEMA is:

- The lead agent for continuity planning within the Federal Executive Branch.
- Responsible for issuing guidance to promote the understanding of and compliance with Federal mandates and requirements.

The responsibility for actual continuity planning lies within each Federal agency.

State and local governments should designate their own lead agents for continuity planning.



2-21

Role of Non-Federal Jurisdictions

State, local, territorial, and tribal governments play an integral role in:

- Determining the needs of the public.
- Ensuring that essential functions continue on a daily basis.
- CGC 1 is guidance for non-Federal entities.



2-22

FCD 1 requires that Federal plans and operations are integrated with the emergency and continuity plans and capabilities of State, local, territorial, and tribal governments, and private-sector owners of the Nation's critical infrastructure, to promote interoperability, and prevent redundancies and conflicting lines of authority.

Agency Roles and Responsibilities

- All Federal departments and agencies are responsible for carrying out the direction of NSPD 51/HSPD 20.
- Regardless of government level, continuity planning responsibilities fall to several department/agency levels.



2-23

Role of the Agency Leader

How are agency leaders involved in continuity planning?



2-24

Role of the Agency Leader

Agency leaders establish continuity planning as a priority by:

- Appointing a Continuity Program Manager.
- Ensuring budgetary support.
- Monitoring the progress of the continuity planning effort.



2-25

Role of the Continuity Program Manager

The Continuity Program Manager:

- Oversees the overall development of the continuity plan.
- Serves as the agency's coordinator for Continuity of Operations.
- Is responsible for developing, coordinating, and managing all activities enabling the performance of essential functions during a continuity situation.
- Chairs the agency's internal continuity planning team or CWG.



2-26

Continuity Program Manager Skills

What skill sets are needed by the Continuity Program Manager?

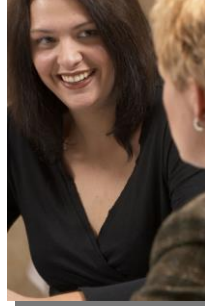


2-27

Continuity Program Manager Skill Sets

Skills that every Continuity Program Manager needs are:

- Business management skills.
- Interpersonal skills.
- Communication skills.
- Facilitation skills.



2-28

The skills that every Continuity Program Manager needs are:

- Business management skills—assessment, data collection, analysis, and development of funding needs and justifications—all concluding with a clear return on investment projection.
- Interpersonal skills—the ability to adapt leadership and communication styles to the individual preferences of those on the planning team.
- Communication skills—both oral and written.
- Facilitation skills—especially the ability to negotiate, to find balance in the middle ground, weigh alternatives, and collect consensus from seemingly opposite positions.

Role of the Continuity Planner

The Continuity Planner manages day-to-day continuity plan development:

- Coordinating with the planning team
- Managing plan development
- Overseeing tests, training, and exercises; corrective action planning; and long-term planning efforts



2-29

Role of the Continuity Planning Team

Members of the continuity planning team should be:

- Selected based on their expertise in specific areas related to the agency's essential functions.
- Assigned specific portions of the continuity plan to research and develop.
- Able to work collaboratively with other team members.



FEMA

2-30

Role of the ERG

Responsibilities of the Emergency Relocation Group (ERG) are to:

- Participate in continuity tests, training, and exercises.
- Prepare office go kits that contain all of the information, supplies, and materials needed initially for continuity plan activation.
- Ensure that they and their families are prepared for an emergency that may require continuity plan activation.
- Report to the continuity facility, or other assigned work area, whenever the continuity plan is activated.



2-31

Summary and Transition

This unit:

- Explained the legal requirements for continuity planning.
- Identified the objectives of Continuity of Operations.
- Described the roles and responsibilities of key players in a continuity program.

Unit 3:

- Will cover elements of a viable continuity program.



2-32

Summary and Transition

Questions?



2-33