Business Continuity and Emergency Preparedness Planning

Vandita Zachariah, MA, MBA, CIA
HHSC Internal Audit Division
May 21, 2010

Overview

- Define key terms and list essential elements of business continuity planning.
- Identify important governance processes necessary for effective business continuity and emergency preparedness.
- Describe the main functional units of a NIMS-compliant incident command structure.
- List types of training useful for personnel to gain an understanding of business continuity and emergency preparedness.
- Discuss the importance of coordination among essential business functions before, during, and after emergencies.

Key Definitions

Business Continuity

Ongoing processes to ensure necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies, recovery plans, and continuity of services.

Emergency Management

Ongoing processes to prevent, mitigate, prepare for, respond to, and recover from an incident that threatens life, property, operations, or the environment.

Key Definitions

Preparedness

Activities, tasks, programs, and systems developed and implemented prior to an emergency used to support the prevention of, mitigation of, response to, and recovery from emergencies.

Risk Analysis

Identifying and monitoring hazards, assessing the likelihood of their occurrence, and the vulnerability of people, property, environment, and the entity itself.

Key Definitions

Business Impact Analysis

BIA is used to identify business processes that are integral to keeping the business unit functioning in a disaster and to determine how soon these integral processes should be recovered following a disaster.

Business Continuity Plans

Documents describing roles, responsibilities, and actions necessary to resume critical business functions in the event of a disruption.

Key Definitions

Exercises and Tests

Exercises and tests include regularly scheduled practice (drills) of the emergency management program and business continuity plans.

The purpose of exercises and tests is to improve the organization's performance in an actual event.

Emergency Management

TDEM Roles and Responsibilities

- Texas Governor's Executive Order RP-32 created the Governor's Division of Emergency Management (now called the Texas Division of Emergency Management) and defined the responsibilities for a coordinated approach to safeguarding the citizens and infrastructure of Texas.
- Based on this directive, TDEM developed the State of Texas Emergency Management Plan (Plan).
- Roles and responsibilities are coordinated through the State Operations Center under the leadership and guidance of the Texas Division of Emergency Management.

Emergency Management

Agency Roles and Responsibilities

- Establish planning processes and emergency management programs to assist in mitigation, preparedness, response, and recovery at the state and federal level (FEMA, CDC).
- Each state agency providing vital public services is required to develop a continuity of operations plan and establish processes to ensure that the plan is regularly updated.
- Agencies prepare and submit plans to the Texas Division of Emergency Management.

Business Continuity Management

- Assess mission critical activities for areas of risk and mitigation of risk (including identifying likely risks that may disrupt essential business functions).
- Analyze the potential impact of extended service interruptions, including systems.
- Identify recovery needs and resource requirements.
- Define and establish resource needs in developing and maintaining business continuity plans.
- Test (exercise) and maintain business continuity plans.

Business Continuity Management

Key Elements of Business Impact Analysis

- List key contacts, contact information, and primary/secondary locations.
- Estimate tolerable interruption of service.
- List essential IT systems.
- Estimate effect on operations due to unmanageable production backlog.
- Plan to control backlog of transactions.
- Identify production deadlines.
- Identify telecom services (LAN, Internet, email) required to maintain service level needed.

Business Continuity Management

Key Elements of Business Impact Analysis

- Estimate length of time operations can continue without IS or network availability
- List and prioritize critical recovery activities to be performed in first 12 hours of an emergency/disaster.
- Identify office equipment and supplies needed to re-establish functionality and when items will be needed.
- List vital and confidential information and their location.
- List critical contractors and external organizations, including contact information.

Business Continuity Management

Business Continuity Plans

- Personnel authorized to develop, approve, and implement plans.
- Decision-making authorities for response and recovery.
- Alternate facilities.
- Employee and service provider contact information.
- Operating procedures for mission-critical functions.
- Integration of Business Continuity and Disaster Recovery plans.
- Manual operations necessary when IT resources are unavailable.
- Vital data interdependencies.
- Location of vital documents and files.

Business Continuity Management

Communication and Coordination

- Prioritize and repurpose available resources (alternate sites, technology resources, equipment, and supplies)
- Consider and integrate key interdependencies among and between business operations and support services (including IT)
- Coordinate with administrative and technology support services, including human resources, facilities, procurement, and management of resources

Business Continuity Management

Tests and Exercises

- Test essential and interrelated business processes.
- Determine the frequency and scope of tests based on the complexity of business processes and impact of business process on the organization.
- Periodic review (annual or more frequent).
- Establish methods to track issues and gaps uncovered during tests and after action assessments.
- Identify deficiencies and establish procedures to take corrective actions.
- Update plans.

After Action Assessment and Reporting

Policy and procedures considerations include:

- Types of events or the extent and length of disruptions for which after action assessments should be performed.
- Identify personnel who are responsible for identifying, documenting, collecting, and assessing response and recovery activities, collecting, and considering information during assessment and reporting.
- Identify reporting elements (strengths, specific improvements, recommendations for achieving needed improvements, and follow up actions, as necessary.
- Timelines for preparation and finalization of after action reports, including management review and approvals.
- Timelines and responsibilities for business units to identify necessary changes to key business processes and update plans.

Governance

- Formation of an oversight committee with clear authority, objectives, roles, and responsibilities.
- Development and implementation of agency policy and (minimum) standards for business continuity and emergency management.
- Establishment of an Incident Command Structure, aligned with FEMA's National Incident Management System guidelines to effectively respond to emergencies and disasters.
- Development of a training program to increase employee awareness of relevant business continuity and emergency preparedness topics.

Key Considerations for Policy

- Require development and approval of plans from appropriate level of management and staff.
- Include risk assessment for business operations and information resources.
- Define the functional level for which business continuity plans should be developed.
- Specify key roles and responsibilities of personnel involved in continuity planning, response, and recovery.
- Require integration of plans within and among dependent functional areas and contractors.
- Define requirements for plan testing.
- Identify requirements for after action assessments and reporting.
- Include requirements for plan updates

Incident Command Structure (FEMA NIMS)

- Incident Commander
- Command Staff
  - Public Information Officer
  - Safety Officer
  - Liaison Officer
- General Staff
  - Planning Section
  - Operations Section
  - Logistics Section
  - Finance/Administration Section

Training

- Provide new employee orientation.
- Perform evacuation drills based on established schedules.
- Identify relevant courses based on roles and responsibilities (Entry-level, Field Supervisors, Middle Management and EOC staff, Command and General Staff).
- Establish method to assess training needs, verify course completion, track and record training courses.
- Ensure business continuity specialists and managers seek professional certifications.

Training

Concepts for New employee orientation

- Employee roles and responsibilities related to business continuity.
- Information about threats, hazards, and protective actions.
- Emergency reporting, response, evacuation, shelter procedures.
- Business unit specific information.
- Emergency shutdown procedures.

Training

Selected Courses Offered by FEMA

- IS 700 NIMS An Introduction
- ICS 100 Introduction to the Incident Command System
- ICS 400 Advanced ICS
- IS 701 NIMS Multiagency Coordination System
- IS 703 NIMS Resource Management
- IS-704 NIMS Communication and Information Management
- P-Level courses are position-specific

FEMA Training Guidelines

FEMA Training Guidelines for Incident Command System Duties	**700**	**800**	**100**	**200**	**300**	**400**
	Independent Study (IS)			*Classroom*		
Entry Level (IS-700 and IS-100)	X		X			
First Line, Single Resource, Field Supervisors (IS-700, IS-100, IS/ICS 200)	X		X	X		
Middle Management such as Strike Team Leaders, Division Supervisors, and Emergency Operations Center Staff (IS-700, IS-800, ICS-100, IS/ICS-200, ICS-300)	X	X	X	X	X	
Command and General Staff such as Area, Emergency, and Emergency Operations Center Managers (IS-700, IS-800, ICS-100, IS/ICS-200, ICS-300, ICS-400)	X	X	X	X	X	X

Training

Business Continuity

- Certified Business Continuity Professional
- Master Business Continuity Professional

DRII The Institute for Continuity Management (www.drii.org)

Audit Topics To Consider

- Governance
  - Oversight Committee roles and responsibilities
  - Policy and procedures
  - Incident command structure for managing emergencies/disasters
  - Training
- Plan Development
  - Business Risk Analysis
  - Security Risk Analysis
  - Business Impact Analysis (mission critical functions)

Audit Topics To Consider

- Plan Coordination and Integration
  - Disaster Recovery Plans
  - Communication and Coordination (HR, IT, facilities management, key contractors)
- Plan Maintenance
  - Periodic review and update
  - Tests and Exercises
  - After Action Assessment and Reporting

Some Useful Resources

- FEMA Emergency Management Guide for Business and Industry, A Step-by-Step Approach to Emergency Planning, Response, and Recovery for Companies of All Sizes http://www.fema.gov/business/guide/toc.shtm
- NFPA 1600 (National Fire Protection Agency) Standard on Disaster/Emergency Management and Business Continuity Programs http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf
- Global Technology Audit Guide – Business Continuity Management, Institute of Internal Auditors