Disaster/Emergency Management & Business Continuity Auditor Training

BCLE-AUD (NFPA 1600)

National Fire Protection Association

DRI International

Copyright © DRI International and National Fire Protection Association, All Rights Reserved
This page left blank intentionally.
Instructor Introduction

Insert instructor introduction notes here
  ▪ Background
  ▪ Education
  ▪ Experience in the BCM field
  ▪ Etc…

Housekeeping

  ▪ Fire Alarm & Exits
  ▪ Breaks & Lunch
  ▪ Cell Phones & PDAs
  ▪ Audio or Video Recording
  ▪ Restrooms
  ▪ Attendance
  ▪ Tent Cards
  ▪ The “Parking Lot”
Introductions & Experience

- What organization do you represent?
- What is your role?
- What is your experience in emergency management and business continuity?
- What is your auditing experience?

Objectives

- Learn the elements of an disaster/emergency management and business continuity program as defined by NFPA1600 “Standard on Disaster/Emergency Management and Business Continuity Programs”
- Understand audit concepts as documented in The Institute of Internal Auditors International Professional Practices Framework (IPPF)
- Learn how to use the audit framework and NFPA 1600 to audit a preparedness program and determine conformity to the standard
- Prepare you for the CBCA/CBCLA qualifying examination

Program Agenda

**Day 1**
- Introduction
- Auditing basics
- Program management
- Planning process
- Risk assessment
- Business impact analysis

**Day 2**
- Prevention & mitigation
- Resource management
- Operational procedures
- Communications & warning
- Incident management
- Emergency operations/response
Program Agenda

Day 3
- Business continuity and Information technology disaster recovery planning
- Crisis communications and public information
- Employee assistance and support

Day 4
- Training and education
- Testing & exercises
- Program improvement
- Reporting audit findings & recommendations
- Examination review

Day 5
- DRI International CBCA/CBCLA Qualifying Examination
  Begins: 8:00 AM
  Ends: 10:30 AM

How to Use NFPA 1600
- Introduction
  - Important Notices and Disclaimers
  - Additional Notices and Disclaimers
- Standard
  - Chapters 1 – 9
  - Annex A (Explanatory Material)
  - Annex B (Resources)
  - Annex C (Conformity Self-Assessment)
  - Annex D (Plan-Do-Check-Act Cycle)
  - Annex E (Standards Crosswalk)
  - Annex F (Management System Standard)
  - Annex H (Awareness and Preparedness for Emergencies at the Local Level)
  - Annex I (Family Preparedness)
  - Annex J (Informational References)
Terminology

3.3.1 *All-Hazards.* An approach for prevention, mitigation, preparedness, response, continuity, and recovery that addresses a full range of threats and hazards, including natural, human-caused, and technology-caused.

3.3.2 *Business Continuity.* An ongoing process to ensure that the necessary steps are taken to identify the impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.

3.3.8 *Crisis Management.* The ability of an entity to manage incidents that have the potential to cause significant security, financial, or reputational impacts.

3.3.10 *Disaster/Emergency Management.* An ongoing process to prevent, mitigate, prepare for, respond to, maintain continuity during, and recover from an incident that threatens life, property, operations, or the environment.

Audit Guide

- Ordered to follow NFPA 1600’s chapters and sections
- Will be used for class exercises
- Reference for your future audits

Title IX of Public Law 110-53
“PS-PREP”
Voluntary Certification Program

- Establish and implement a voluntary private sector preparedness accreditation and certification program
- Designate an officer responsible for the accreditation and certification program
- Support the development and updating of voluntary preparedness standards
- Develop and promote a program to certify the preparedness of private sector entities that voluntarily choose to seek certification

PS-PREP Program

U.S. Dept. of Homeland Security

ANAB (ANSI-ASQ National Accreditation Board)

Certifying Bodies

Certify Compliant PS Preparedness Programs

Private Sector Entities

Seek certification by demonstrating conformity to selected standard

PS-PREP Designated* Standards

* DHS Secretary Napolitano announced the adoption of the following standards for the PS-Prep program on June 15, 2010:
Auditing Basics

“Audit”

“systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled”

ISO/DIS 19011

“Internal Auditing”

“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

International Professional Practices Framework, Institute of Internal Auditors
Audit Definitions

**Audit Criteria**
"set of policies, procedures or requirements"
Audit criteria are used as a reference against which audit evidence is compared. If the audit criteria are selected from legal or other requirements, the audit finding is termed compliance or non-compliance.

**Audit Evidence**
"records, statements of fact or other information, which are relevant to the audit criteria and verifiable"
Audit evidence may be qualitative or quantitative.

**Audit Findings**
"results of the evaluation of the collected audit evidence against audit criteria"
Audit findings may indicate conformity, nonconformity, and opportunities for improvement or good practices.

**Audit Conclusion**
"outcome of an audit, after consideration of the audit objectives and all audit findings"

ISO/DIS 19011

Types of Audits

**First Party**
Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the organization itself for management review and other internal purposes and may form the basis for an organization's self-declaration of conformity.

**Second Party**
External audits include second and third party audits. Second party audits are conducted by parties having an interest in the organization, such as customers, or by other persons on their behalf.

**Third Party**
Third party audits are conducted by independent auditing organizations, such as regulators or those providing registration or certification.

ISO/DIS 19011

Auditing Standards & Guidance

- Institute of Internal Auditors
  - “Internal Auditors Professional Framework”
- International Organization for Standards
  - ISO 19011 “Guidelines for auditing management systems”
- Information Systems Audit and Control Association (ISACA)
- U.S. Government Accountability Office
- Federal Information Security Management Act (FISMA)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - Guidance on internal controls and enterprise risk management

ISO/DIS 19011
**Internal Auditors Professional Framework**

Institute of Internal Auditors (IIA)
- **Mandatory Guidance**
  - Definition of internal auditing
  - Code of Ethics
  - Standards
- **Strongly Recommended Guidance**
  - Practice Advisories
  - Position Papers
  - Practice Guides
- **Professional Certifications**
  - Certification in Control Self Assessment
  - Certified Financial Services Advisor
  - Certified Government Auditing Professional

**Government Auditing Standards**

- Commonly called the “Yellow Book”
- Yellow Book standards apply to U.S. federal financial audits, performance or operations audits and other audit related activities
- Federal regulations require that both federal and non-federal auditors comply with Yellow Book standards for audits of federal organizations, programs and functions

**Information Technology**

- ISACA
  - IT Audit and Assurance Standards, Guidelines, Tools and Techniques
  - COBIT IT governance framework and toolset
- FISMA
  - Risk Management Framework; Security Assessment; Controls
- NIST Computer Security Division
  - Special Publications
**Auditing & Governance**

- Governance begins with the board of directors and its committees.
- Day to day governance is executed by the management of the organization.
- Internal and external parties such as auditors provide management and the board of directors with assurances regarding the effectiveness of the governance activities.

**Risk Management & Controls**

<table>
<thead>
<tr>
<th>Risk Management</th>
<th>Effective Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational objectives support and align with the organization’s mission.</td>
<td>Reliability and integrity of financial and operational information.</td>
</tr>
<tr>
<td>Significant risks are identified and assessed.</td>
<td>Effectiveness and efficiency of operations.</td>
</tr>
<tr>
<td>Appropriate risk responses are selected that align risks with the organization’s risk appetite.</td>
<td>Safeguarding of assets.</td>
</tr>
<tr>
<td>Relevant risk information is captured and communicated on a timely basis enabling staff, management and the board to carry out their responsibilities.</td>
<td>Compliance with laws, regulations and contracts.</td>
</tr>
</tbody>
</table>

**Auditor Attributes**

- **Independence.** Independent… free from conditions that threaten the ability to carry out responsibilities in an unbiased manner.
- **Objectivity.** Highest level of professional objectivity gathering, evaluating, and communicating information. Balanced assessment of all relevant circumstances not unduly influenced by their own interests or others.
- **Confidentiality.** Respect the value and ownership of information received; no disclosure without appropriate authority unless legal or professional obligation to do so.
- **Proficiency and Professional Due Care.** Apply the knowledge, skills, and experience needed.
Required Knowledge

- Risk, resilience, security, preparedness, crisis management, emergency management, business continuity, and IT disaster recovery planning
- Principles of risk identification, analysis and evaluation, and risk communication
- Asset protection and physical security
- Loss prevention, deterrence, and risk mitigation
- Incident response, crisis management, crisis communications
- Emergency operations/response; business continuity

Phases of Engagement

- Planning
  - Objectives & Scope
  - Resource Allocation
  - Work program
  - Identifying Information
  - Analysis & Evaluation
  - Documenting Information

- Performance
  - Criteria for Communications
  - Quality
  - Disseminating

- Communicating Results

Engagement Planning

Objectives
- 1st, 2nd or 3rd party audit
- What is to be achieved by the engagement
- What is the deliverable
- Who is the audience

Scope
- Areas to be audited
- Must be sufficient to satisfy the objectives
- Includes:
  - Organizational and functional units
  - Facilities to survey
  - Documents
  - Interviews
  - Witnessing of training, drills, testing, exercises
Resource Allocation

- Appropriate and sufficient resources to achieve the objective of the engagement
- Nature and complexity of each resource to be engaged
- Time constraints
- Resource availability

Work Program

Develop and document work programs that achieve the engagement objectives:

- Procedures for identifying, analyzing, evaluating and documenting information
- Plan, timetable, status reporting
- Supervision of work performed

Engagement Planning

- Select the audit team; assign responsibilities
- Determine audit methods
- Request program documents
- Research standards and regulations
- Identify sites to visit
- Schedule interviews
- Prepare for on-site activities
Performing the Engagement

- **Identify information**: sufficient, reliable, relevant and useful to achieve objectives.
- **Analyze and evaluate**: Base conclusions and results on appropriate analysis and evaluations.
- **Document information**: to support conclusions and engagement results.

Performing the Engagement

**Identify information: Program Documentation**

- Facility information
- Policy statement
- Program objectives, development plan, schedule, budget, and milestones
- Program committee/steering committee (rosters, agendas, meeting minutes, action items, communications with management)
- Finance & administration framework and procedures
- Records management policies and practices:
  - Program reviews and audits
  - Corrective action procedures, plans and status reports

Research Regulatory Requirements

<table>
<thead>
<tr>
<th>Regulations</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire prevention code</td>
<td>Construction</td>
</tr>
<tr>
<td>Life Safety Code®</td>
<td>Height (e.g., high-rise)</td>
</tr>
<tr>
<td>Occupational safety &amp; health</td>
<td>Size</td>
</tr>
<tr>
<td>Environmental</td>
<td>Use or Occupancy</td>
</tr>
<tr>
<td>Hazardous materials</td>
<td>Hazards</td>
</tr>
<tr>
<td>Industry specific</td>
<td>Hazardous processes</td>
</tr>
<tr>
<td>Information security</td>
<td>Location</td>
</tr>
<tr>
<td></td>
<td>Proximity to waterways</td>
</tr>
<tr>
<td></td>
<td>Scope of emergency response operations</td>
</tr>
</tbody>
</table>
Performing the Engagement

Identifying Information

- Interviews with employees and other persons;
- Observations of activities
- Documents, such as policies, objectives, plans, procedures, specifications, drawings, contracts etc.
- Records, such as minutes of meetings, audit reports, records of exercise programs and the results, plan summaries, business impact analyses reports etc.

ISO 19011 C.2

Performing the Engagement

Analyze and Evaluate

- Is the information provided complete? (all expected content is contained in the document);
  - correct (the content is compliant to other reliable sources such as standards and regulations);
  - consistent (the document is consistent in itself and to related documents);
  - current (the content is up to date).
- Does the information reviewed cover the audit scope and is it capable of providing sufficient information to support the audit objectives?
- Specific care is needed for information security due to applicable regulations on protection of data (in particular for information, which lies outside the audit scope but is also contained in the document).

Conducting Interviews

- Interview persons from levels and functions performing activities or tasks within the scope of the audit;
- Conduct during normal working hours and, where practical, at the normal workplace;
- Put the person at ease prior to and during the interview;
- Explain the reason for the interview and any note taking;
- Initiate by asking the persons to describe their work;
- Avoid questions that bias the answer (i.e., leading questions);
- Summarize results and review with the interviewed person;
- Thank the person interviewed.
Site Visits

- Ensure that the audit team is using PPE properly.
- Adapt audit team size and number of guides and observers to avoid interference of operational processes.
- Do not touch or manipulate any equipment, unless explicitly permitted, even when competent and/or licensed.
- If taking pictures, seek management authorization in advance and consider security and confidentiality. Avoid photographing persons without their permission.
- If taking copies of documents of any kind, ask for permission in advance and consider confidentiality and security matters.
- When taking notes, avoid collecting personal information unless required by the audit objectives and/or audit criteria.

Engagement Supervision & Conduct

- Engagement supervision (IPPF 2340-1)
  - Engagements must be properly supervised to ensure objectives are achieved, quality is assured and staff is developed.
- Audit conduct (ISO 19011-6.4)
  - Opening meeting
- Document Review (ISO 19011 C.3)
- Conduct Interviews (ISO 19011 C.7)
- Conduct site visits (ISO 19011 C.6)
  - Collection and verification of information
  - Communications during the audit

Communicating the Results

- Criteria for communications
  - Include objectives, scope, conclusions, recommendations, and action plans.
  - Include relevant information to support the conclusions and engagement results.
  - Include overall opinion and/or conclusions where appropriate.
  - Identity and comply with limitations on distribution.
- Quality of Communications
  - Accurate, objective, clear, concise, constructive, complete and timely.
  - Minimize the risk of misinterpretation.
  - Correct errors promptly.
- Disseminating results
  - Outcomes of the engagement must be communicated timely to the appropriate parties.
  - More on this on Day 4.
Discussion

1. What is auditing?
2. What is internal auditing?
3. Discuss the following types of audits:
   a. First Party
   b. Second Party
   c. Third Party
4. Name some prominent regulations and standards that can be used in audits.
Program Administration

1.1* Scope. This standard shall establish a common set of criteria for all hazards disaster/emergency management and business continuity programs, hereinafter referred to as “the program.”

1.2* Purpose. This standard provides the fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity, and recovery.

1.3* Application. This document shall apply to public, not-for-profit, and nongovernmental organizations (NGOs) and to private entities.
4.1 Leadership and Commitment

4.1.1 The entity leadership shall demonstrate commitment to the program to prevent, mitigate the consequences of, prepare for, respond to, maintain continuity during, and recover from incidents.

4.1.2 The leadership commitment shall include the following:
1. Policies, plans, and procedures to develop, implement, and maintain the program
2. Resources to support the program
3. Reviews and evaluations to ensure program effectiveness
4. Correction of deficiencies

4.1.3 The entity shall adhere to policies, execute plans, and follow procedures developed to support the program.

Leadership and Commitment

Interviews/Surveys/Documents
- Interviews
  - Entity leadership
  - Program coordinator
  - Team members
- Survey
  - Facility survey
- Documents
  - Program documents
  - Program budget
  - Policy statement
  - Training, drill, testing, and exercise records

Evidence of Conformity
- Policy statement signed by senior leader and widely disseminated
- Sufficient funds budgeted
- Periodic communication involves senior leadership
- Senior leadership attendance at key activities

4.2 Program Coordinator

The program coordinator shall be appointed by the entity’s leadership and authorized to develop, implement, administer, evaluate, and maintain the program.
4.3 Program Committee

4.3.1* A program committee shall be established by the entity in accordance with its policy.

4.3.2 The program committee shall provide input for, and/or assist in the coordination of the preparation, development, implementation, evaluation, and maintenance of the program.

4.3.3* The program committee shall include the program coordinator and others who have the expertise, the knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and shall solicit applicable external representation.

Internal Participants

- Management
- Legal
- Environmental Health & Safety (EHS)
- Human Resources
- Public Relations or Public Affairs
- Regulatory Affairs
- Risk Management
- Finance
- Labor Relations
- Operations
- Facilities or Property Management
- Engineering
- Security
- Medical
- Information Technology
- Purchasing, Supply Chain, & Distribution
- Quality
- Employees
- Audit
**External Representation**

- Law enforcement
- Fire Department
- Rescue service
- Emergency Medical Services
- Hazardous Materials contractor
- Local Emergency Planning Committee (LEPC)
- Emergency Management Agency
- Public Health
- Public Works
- Contractors
- Vendors
- Customers
- Others

**Program Committee**

**Interviews/Surveys/Documents**
- Interviews
  - Program coordinator
  - Program committee members
- Documents
  - Company organization chart
  - Meeting minutes
  - Communications between team members
  - Communications with external representatives

**Evidence of Conformity**
- Program committee membership documented and current?
- Committee reflect the entity’s organization?
- Include required institutional and technical knowledge?
- Periodic meetings held?
- Communications between committee members related to achieving program goals?

**4.4 Program Administration**

1. Executive policy, including vision, mission statement, roles and responsibilities, and enabling authority
2. Program scope, goals, objectives, and method of program evaluation
3. Program plans and procedures that include the following:
   a. Anticipated cost
   b. Priority
   c. Time schedule
   d. Resources required
4. Applicable authorities, legislation, regulations, and industry codes of practice as required by Section 4.5
5. Program budget and schedule, including milestones
6. Records management practices as required by Section 4.8
Program Administration

Interviews/Surveys/Documents
- Interviews
  - Senior management
  - Program Coordinator
- Documents
  - Policy statement
  - Mission & vision statement
  - Program plans (roles, responsibilities, goals, objectives)
  - Program evaluation
  - Program development plan
  - Budget

Evidence of Conformity
- Policy statement with vesting of authority
- Goals and objectives of program consistent with mission & vision
- Roles and responsibilities defined
- Program development plan with schedule supporting budget

4.5 Laws and Authorities

4.5.1* The program shall comply with applicable legislation, policies, regulatory requirements, and directives.
4.5.2* The entity shall establish and maintain a procedure(s) to comply with applicable legislation, policies, regulatory requirements, and directives.
4.5.3* The entity shall implement a strategy for addressing the need for revisions to legislation, regulations, directives, policies, and industry codes of practice.

Laws & Authorities (USA)

- Occupational Safety & Health (OSHA) Standards
  - Emergency Action Plan
  - Means of Egress
  - Medical Services & First Aid; Blood borne Pathogens
  - Permit-Required Confined Spaces
  - Process Safety Management
  - Hazardous Waste (HAZWOPER)
  - Fire brigades
- Fire codes
  - "Model Codes" (NFPA 1, International Fire Code)
  - State or local fire prevention code
- Life safety codes
- Americans with Disabilities
- Environmental
  - Emergency Planning and Community “Right to Know”
  - Chemical Accident Prevention
  - Risk Management Plan
  - Spill Prevention Control & Countermeasures
  - Oil Pollution Prevention (more)
- Homeland Security
- Local ordinances
- Industry Regulations
Laws & Authorities: Industries

- Banking
  - Federal Financial Institutions Examination Council (FFIEC) BCP Handbook
  - Electronic Funds Transfer Act
- Securities
  - NASD Rules 3510 and 3520
  - NYSE Rule 446 Business Continuity
  - NFA Compliance Rule 2-38
- Insurance
  - National Association of Insurance Commissioners' Guidelines on Information Technology (IT)
- All Industries
  - Cyber security (protection of customer information)

- Health Care
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - HITECH Act of 2009 – Health Information Technology for Economic and Clinical Health Act
  - Pharmaceuticals
  - U.S. FDA Good Manufacturing Practices, Computerized Systems Used in Clinical Trials
- Electric Utility Industry
  - Federal Electric Reliability Council's (FERC) Security Standards
  - North American Electric Reliability Council's (NERC) Security Guidelines

Laws & Authorities

Interviews/Surveys/Documents

- Interviews
  - Program coordinator
  - Regulatory affairs
  - Legal

- Documents
  - Prevention & mitigation plans
  - EHS program
  - IT security
  - BCP and IT DRP plans
  - Organizational statements (Emergency response plan)
  - Crisis communications plan (mandatory reporting, recall)
  - Incident reports
  - Training, drill, testing, and exercise documents

Evidence of Conformity

- Applicable Federal, state, and local laws, regulations, and ordinances are referenced in the plan
- Requirements have been identified and addressed in the plans
  - Plans and procedures
  - Resources
  - Training, drills, exercises
  - Reporting
- Reporting requirements and triggers specified

4.6 Finance and Administration

4.6.1 The entity shall develop financial and administrative procedures to support the program before, during, and after an incident.

4.6.2 There shall be a responsive finance and administrative framework that does the following:
   (1) Complies with the entity's program requirements
   (2) Is uniquely linked to response, continuity, and recovery operations
   (3) Provides for maximum flexibility to respond quickly to incidents, manage, and apply funds in a nonemergency environment and in an emergency situation to ensure the timely delivery of assistance

4.6.3 Procedures shall be created and maintained for expediting fiscal decisions in accordance with established authorization levels, accounting principles, governance requirements, and fiscal policies.

4.6.4 Financial and administrative procedures shall include the following:
   (1) Responsibilities for program finance authority, including reporting relationships to the program coordinator
   (2) Procurement procedures
   (3) Payroll
   (4) Accounting systems to track and document costs
   (5) Management of funds from external resources
   (6) Crisis management procedures that coordinate authorization levels and appropriate control measures
   (7) Documenting financial expenditures incurred as a result of an incident and for compiling claims for future cost recovery
   (8) Identifying and accessing alternative funding sources
   (9) Managing budgeted and specially appropriated funds
**Finance and Administration**

<table>
<thead>
<tr>
<th>Interviews/Surveys/Documents</th>
<th>Evidence of Conformity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interviews</td>
<td>Budget specifically for program</td>
</tr>
<tr>
<td>Program coordinator</td>
<td>Defined roles &amp; responsibilities</td>
</tr>
<tr>
<td>CFO, Treasurer, Accounting Manager</td>
<td>Documented authorization levels and procedures for expedited approvals</td>
</tr>
<tr>
<td>Risk or insurance manager</td>
<td>Risk management/insurance procedures for claims management</td>
</tr>
<tr>
<td>Documents</td>
<td>Documented accounting procedures; pre-established accounts</td>
</tr>
<tr>
<td>Program documents (crisis management, ERP, BCP)</td>
<td>Oversight controls to prevent fraud</td>
</tr>
<tr>
<td>Accounting procedures</td>
<td>Risk management or insurance claims reporting and accounting procedures</td>
</tr>
</tbody>
</table>

**Evidence of Conformity**

- Budget specifically for program
- Defined roles & responsibilities
- Documented authorization levels and procedures for expedited approvals
- Risk management/insurance procedures for claims management
- Documented accounting procedures; pre-established accounts
- Oversight controls to prevent fraud

**4.7 Records Management**

4.7.1 The entity shall develop, implement, and manage a records management program to ensure that records are available to the entity following an incident.

4.7.2 The program shall include the following:

1. Identification of records (hard copy or electronic) vital to continue the operations of the entity
2. Backup of records on a frequency necessary to meet program goals and objectives
3. Validation of the integrity of records backup
4. Implementation of procedures to store, retrieve, and recover records onsite or offsite
5. Protection of records
6. Implementation of a record review process
7. Procedures coordinating record access

**Records Management**

<table>
<thead>
<tr>
<th>Interviews/Surveys/Documents</th>
<th>Evidence of Conformity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interviews</td>
<td>Records management practices specified?</td>
</tr>
<tr>
<td>Program coordinator</td>
<td>Records kept for required time period?</td>
</tr>
<tr>
<td>Person responsible for records management</td>
<td>Document controls specified?</td>
</tr>
<tr>
<td>Survey</td>
<td>Access controls enforced?</td>
</tr>
<tr>
<td>Records storage area or site</td>
<td>Required confidentiality maintained?</td>
</tr>
<tr>
<td>Documents</td>
<td></td>
</tr>
<tr>
<td>Program documents</td>
<td></td>
</tr>
</tbody>
</table>
5.1 Planning Process

5.1.1* The program shall follow a planning process that develops strategies, plans, and required capabilities to execute the program.

5.1.2 Strategic planning shall define the entity’s vision, mission, and goals of the program.

5.1.3 A risk assessment and a business impact analysis (BIA) shall develop information to prepare prevention and mitigation strategies.

5.1 Planning Process (continued)

5.1.4 A risk assessment, a BIA, and a resource needs assessment shall develop information to prepare emergency operations/response, crisis communications, continuity, and recovery plans.

5.1.5 Crisis management planning shall address issues that threaten the strategic, reputational, and intangible elements of the entity.

5.1.6 The entity shall include key stakeholders in the planning process.
Strategic Planning

- Vision
- Mission
- Program goals
  - Prevention & mitigation
  - Emergency response
  - Business continuity
  - Crisis communications

6.1 Common Plan Requirements

6.1.1* Plans shall address the health and safety of personnel.

6.1.2 Plans shall identify and document the following:
   1. Assumptions made during the planning process
   2. Functional roles and responsibilities of internal and external agencies, organizations, departments, and positions
   3. Lines of authority
   4. The process for delegation of authority
   5. Lines of succession for the entity
   6. Liaisons to external entities
   7. Logistics support and resource requirements

6.1.3* Plans shall be individual, integrated into a single plan document, or a combination of the two.

6.1.4* The entity shall make sections of the plans available to those assigned specific tasks and responsibilities therein and to key stakeholders as required

Crisis Management Planning

Addresses issues that threaten the brand, organizational image, reputation, and intangible elements of the entity.

Crisis Management. The ability of an entity to manage incidents that have the potential to cause significant security, financial, or reputational impacts. [NFPA 1600 3.3.8]
## Auditing the Planning Effort

<table>
<thead>
<tr>
<th>Interviews/Surveys/Documents</th>
<th>Evidence of Conformity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interviews</td>
<td>Program goals and objectives align with strategic goals and objectives of the entity</td>
</tr>
<tr>
<td>• Program coordinator</td>
<td>• “All Hazards” approach</td>
</tr>
<tr>
<td>• Senior management</td>
<td>• “Common plan requirements” met within each plan document</td>
</tr>
<tr>
<td>• Planners</td>
<td></td>
</tr>
<tr>
<td>• Communications</td>
<td></td>
</tr>
<tr>
<td>Documents</td>
<td></td>
</tr>
<tr>
<td>• Strategic planning</td>
<td></td>
</tr>
<tr>
<td>• Capital budget</td>
<td></td>
</tr>
<tr>
<td>• All plans</td>
<td></td>
</tr>
</tbody>
</table>

BCLE-AUD Slide 4-7
5.2* Risk Assessment

The entity shall conduct a risk assessment to develop required strategies and plans.

5.2.1* The entity shall identify hazards and monitor those hazards and the likelihood of their occurrence.

5.2.2* Hazards to be evaluated shall include the following:

1. Natural hazards (geological, meteorological, and biological)
2. Human caused events (accidental and intentional)
3. Technologically caused events (accidental and intentional)

5.2.2.1* The entity shall identify hazards and monitor those hazards and the likelihood of their occurrence.

5.2.3* The entity shall conduct an analysis of the impact of the hazards identified in 5.2.2 on the following:

1. Health and safety of persons in the affected area
2. Health and safety of personnel responding to the incident
3. Continuity of operations
4. Property, facilities, assets, and critical infrastructure
5. Safety of the entity's services
6. Supply chain
7. Environment
8. Economic and financial condition
9. Regulatory and contractual obligations
10. Reputations of or confidence in the entity

5.2.5 The risk assessment shall evaluate the adequacy of existing prevention and mitigation strategies.

Risk Assessment Process

<table>
<thead>
<tr>
<th>Identify Hazards</th>
<th>Assets at Risk</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire</td>
<td>People</td>
<td>Casualties</td>
</tr>
<tr>
<td>Explosion</td>
<td>Property</td>
<td>Property damage</td>
</tr>
<tr>
<td>Natural hazards</td>
<td>including</td>
<td>Business interruption</td>
</tr>
<tr>
<td>Hazardous spills or releases</td>
<td>buildings, critical infrastructure</td>
<td>Loss of customers</td>
</tr>
<tr>
<td>Terrorism</td>
<td>Safety systems</td>
<td>Financial loss</td>
</tr>
<tr>
<td>Workplace violence</td>
<td>Technology</td>
<td>Environmental contamination</td>
</tr>
<tr>
<td>Utility outage</td>
<td>Information Technology</td>
<td>Loss of confidence in the organization</td>
</tr>
<tr>
<td>Mechanical breakdown</td>
<td>Business</td>
<td>Fines and penalties</td>
</tr>
<tr>
<td>Supplier failure</td>
<td>Regulatory and contractual obligations</td>
<td>Lawsuits</td>
</tr>
<tr>
<td>Cyber attack</td>
<td>Environment</td>
<td></td>
</tr>
</tbody>
</table>

Hazard Identification | Vulnerability Assessment | Impact Analysis
Risk Assessment

Analyze the impacts of identified hazards on:

- Health and safety of persons in the affected area and responding personnel
- Property, facilities, assets, and critical infrastructure
- Continuity of operations/delivery of services
- Supply chain
- Environment
- Economic and financial condition
- Regulatory and contractual obligations
- Reputation or confidence in the entity

Evaluate potential effects of regional, national, or international incidents that could have cascading impacts.

Hazards: Natural Hazards

Geological
- Earthquakes
- Landslide
- Subsidence/Sinkhole
- Tsunami
- Volcano

Meteorological
- Flooding
- Hurricanes
- Lightning
- Tornadoes
- Dam Failure
- Severe Winter Storm
- Arctic freeze

Hazards: Natural Hazards

- Biological Hazards
- Pandemic Disease
- Foodborne Illnesses

© 2013, National Fire Protection Association and DRI, International, All Rights Reserved
Version 4.0
Hazards: Human-Caused Events

- **Fire & Explosion**
- **Explosion**
- **Fire**
- **Wildfire**

**Buildings & Equipment**

- Structural Failure or Collapse
- Entrapment
- Mechanical Breakdown

---

Hazards: Human-Caused Events

**Transportation Incidents**

- Motor Vehicle
- Railroad
- Watercraft
- Aircraft
- Pipeline

**Hazardous Materials**

- Hazmat spill or release (on and off-site)
- Natural Gas Leak
- Nuclear Power Plant Incident
- Radiological incident

---

Hazards: Human-Caused Events

**Supply Chain Interruption**

- Loss of Shipping or Transportation
- Vendor failure (single or sole source provider)
- Loss of Key Customer

**Utility Interruption or Failure**

- Telecommunications
- Electrical Power
- Water
- Gas
- Steam
- HVAC
- Pollution control system
- Sewerage system
- Other critical infrastructure
Hazards: Human-Caused Events

Human Caused Intentional Acts
- Arson
- Labor Strike
- Demonstrations
- Civil Disturbance (Riot)
- Bomb Threat
- Lost Person
- Child Abduction
- Kidnap
- Extortion
- Hostage Incident
- Workplace Violence
- Robbery
- Sniper Incident
- Crime or Theft
- Sabotage or Vandalism

Terrorism
- Chemical
- Biological
- Radiological
- Nuclear
- Explosives

Hazards: Human-Caused Events

Employment Practices
- Privacy
- Discrimination
- Harassment

Liability
- Product Liability or Warranty
- Professional Liability
- Contractual Liability
- Directors & Officers Liability
- Libel or Slander
- Fraud
- General Liability
- Automobile Liability

Hazards: Technological

Computer Systems
- Outages
- Hardware failure
- Data corruption, deletion, or theft
- Loss of network connectivity (Internet or intranet)
- Loss of electronic data interchange or eCommerce
- Loss of domain name server (DNS)
- Virus, worm, Trojan horse
- Power surge, lightning
- Host site interdependencies

Water damage
- Cyber terrorism
- Hacking
- Computer fraud
- Loss of encryption
- Denial of service
- Improper system use by employee
- Telecommunications interruption or failure
- Internet service provider
- Electricity brownout or blackout
**Example Probability of Occurrence**

- **Low:** Less than 10% annual probability or on average less than once every 10 years
- **Medium:** Greater than or equal to 10% annual probability or on average at least once every 10 years
- **High:** 100% annual probability of occurrence (expected to occur on average once each year)

**Probability of Occurrence**

- Probabilities of some natural hazards available from government sources
- Entity must assign relative probabilities
- For each hazard there are many combinations of probability and severity
- Probabilities of some threats (e.g., pandemic flu and terrorism) are hard to quantify

**Assets at Risk**

- **People**
  - Employees
  - Visitors, guests, contractors
  - Neighbors/community
  - Emergency responders
- **Property**
  - Buildings
  - Machinery & Equipment
  - Computer Systems
  - Raw materials/finished goods
  - Property on premises of others
  - Vital records, drawings, data
- **Intellectual Property**
- **Utilities**
- **Critical Infrastructure**
**Assets at Risk**

- Business Operations
  - Manufacturing processes
  - Delivery of services
  - Administrative services
  - Research & development
  - Supply chain
- Environment
  - Air, Water, & Ground
- Entity
  - Economic and financial condition
  - Licenses, Patents, Trademarks
  - Reputation and image
  - Regulatory and contractual obligations
  - Relationships

**Vulnerability Assessment**

- Vulnerability is a weakness, an inadequately protected exposure, or susceptibility to damage or harm.
- A vulnerability assessment is a process to identify, evaluate, and assess:
  - Susceptibility of a site to natural or manmade hazards
  - Weaknesses in buildings, systems, equipment, management programs, and the capabilities of people
  - Lack of, or inadequate protection of, a hazard
  - Dependencies and interdependencies

**Severity of Impacts**

- How do you measure severity of impacts?
- Impact is relative to the size and resources of the entity
- Interview senior management and experts within the organization to obtain their opinion on the relative impact of various scenarios
Auditing Risk Assessment

Interviews/Surveys/Documents
- Interviews
  - Program coordinator
  - Internal experts (EHS, security, IT, facilities, operations, supply chain, etc.)
  - Internal Audit
  - Risk management
- Surveys
  - Observations of site, facility, data center, hazardous processes
- Documents
  - Risk assessments
  - Process hazard analysis
  - Risk management plan
  - Loss prevention reports (internal, insurer, consultant)

Evidence of Conformity
- Risk assessment considers “all hazards”
- Probabilities are estimated
- Vulnerabilities are identified
- Impacts of hazards are estimated
  - People
  - Buildings
  - Operations
  - Environment
- Image and reputation
- Evaluates effects of regional, national, or international incidents
- Risk assessment used to develop overall program

Discussion

1. What is “All Hazards”?
2. What does a Risk Assessment determine?
3. Define “Vulnerability”.
4. Describe the “Risk Assessment Process”.

© 2013, National Fire Protection Association and DRI, International, All Rights Reserved
Version 4.0
5.3* Business Impact Analysis

5.3.1 The entity shall conduct a business impact analysis (BIA).
5.3.2 The BIA shall evaluate the potential impacts resulting from interruption or disruption of individual functions, processes, and applications.
5.3.3* The BIA shall identify those functions, processes, infrastructure, systems, and applications that are critical to the entity and the point in time (recovery time objective (RTO)) when the impact of the interruption or disruption becomes unacceptable to the entity.
5.3.4* The BIA shall identify dependencies and interdependencies across functions, processes, and applications to determine the potential for compounding impact in the event of an interruption or disruption.
5.3.5 The BIA shall identify those functions, processes, infrastructure, systems, and applications that are critical to the entity and the point in time (recovery point objective (RPO)) that defines the potential gap between the last backup of information and the time of the interruption or disruption.
5.3.6 The BIA shall be used in the development of recovery strategies and plans to support the program.

BIA Process

- Identify Business Functions
  - Functions
  - Processes
  - Applications & Data

- Identify Interdependencies
  - Internal
  - External

- Identify & Analyze Impacts of Interruption/Disruption
  - Financial
  - Customer
  - Contractual
  - Reputation
  - Regulatory

- Determine Recovery Time Objectives
  - Point in time when impact(s) of the interruption or disruption becomes unacceptable

- Determine Resource Requirements
  - Staff
  - Workspace
  - Machinery & Equipment
  - Information Technology
  - Vital Records
Business Functions

Groups of related activities that enable the entity to produce its product(s) or provide its service(s).

Interdependencies

- Supply chain
- Process diagram
- Distribution
- Information Technology
  - Order receipt
  - Order processing
  - Voice
  - Data
  - Manufacturing control

Impacts: Quantitative & Qualitative

**Quantitative**
- Property damage
- Revenue loss
- Cash flow
- Accounts receivable
- Market share
- Stock price
- Fines
- Legal liability
- Extra expenses

**Qualitative**
- Human resources
- Morale
- Stakeholder confidence
- Image and reputation
- Financial community credibility
Impacts of Interruption/Disruption

- Financial
  - Lost revenue
  - Deferred revenue
  - Increased costs
- Operational
  - Availability of automated systems and information
  - Reduced productivity and efficiency
  - Increased administrative costs
  - Management attention redirected to continuity and recovery
- Contractual
  - Penalties
  - Loss of bonuses
- Customer
  - Customer relationships
  - Lost market share
  - Reputation or confidence in the entity

Recovery Time Objective (RTO)

The recovery time objective is the period of time within which systems, applications, or functions must be recovered after an outage (e.g., one business day).

A.5.3.3 RTOs are often used as the basis for the development of recovery strategies and as a determinant as to when to implement the recovery strategies during a disaster situation.
**Data Recovery Point Objective**

A.5.3.5 The RPO is the point in time from which data are recovered, "the last good backup offsite at the time of the event."

---

**Resource Requirements**

- Personnel
- Facilities
  - Alternate workspace
  - Data center hot site
- Machinery & equipment
- Information technology
- Vital records

---

**Vital Records**

3.3.27 Information critical to the continued operation or survival of an entity.

Includes records required to be kept for legal reasons
Paper Records

- Paper Records
  - Work in process
  - Desks
  - Notebooks
  - File cabinets
- Backup Options:
  - Scanning
  - Photocopy
  - Microfilm/Fiche
  - Offsite storage

Auditing the BIA

<table>
<thead>
<tr>
<th>Interviews/Surveys/Documents</th>
<th>Evidence of Conformity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interviews</td>
<td>Systematic identification of functions, processes, and applications</td>
</tr>
<tr>
<td>C Suite (COO, CFO, CIO)</td>
<td>Analysis of potential impacts</td>
</tr>
<tr>
<td>Department heads</td>
<td>Determination of recovery time objectives</td>
</tr>
<tr>
<td>Business process managers</td>
<td>Identification of resource requirements</td>
</tr>
<tr>
<td>Program Coordinator</td>
<td>Identification of lost data potential</td>
</tr>
<tr>
<td>Business continuity team</td>
<td></td>
</tr>
<tr>
<td>IT Disaster recovery team</td>
<td></td>
</tr>
<tr>
<td>Surveys</td>
<td></td>
</tr>
<tr>
<td>Manufacturing processes</td>
<td></td>
</tr>
<tr>
<td>Documents</td>
<td></td>
</tr>
<tr>
<td>Business process flowchart</td>
<td></td>
</tr>
<tr>
<td>Questionnaires and worksheets</td>
<td></td>
</tr>
<tr>
<td>BIA report</td>
<td></td>
</tr>
<tr>
<td>IT Disaster recovery plan</td>
<td></td>
</tr>
</tbody>
</table>

Evaluating the BIA Process

- What were the assumptions?
- What criteria was defined?
- What method was used?
  - Questionnaires
  - Interviews
  - Workshop
- Who was interviewed?
- How were results validated?
- Who approved final BIA results?
Evaluating the BIA Process

- How were the potential financial and non-financial impacts quantified and evaluated?
- What were the requirements for identification of qualitative impacts?
- What was the scale to define and prioritize impacts?
- Did management agree with the thresholds and criticality scale?

Evaluating the BIA Report

- "Criticality" Rating
- Recovery Time Objectives (RTO)
- Interdependencies - Internal and external
- Resource requirements
  - Minimum staff levels
  - Workspace
  - Information technology including supporting infrastructure
  - Electronic information
  - Vital Records

Discussion

1. Define and describe "RTO".
2. Define and describe "RPO".
3. Define qualitative and quantitative impacts.
4. Describe the "BIA Process".

© 2013, National Fire Protection Association and DRI, International, All Rights Reserved
Version 4.0
6.2 Prevention

6.2.1 The entity shall develop a strategy to prevent an incident that threatens life, property, and the environment.

6.2.2 The prevention strategy shall be kept current using the information collection and intelligence techniques.

6.2.3 The prevention strategy shall be based on the results of hazard identification and risk assessment, an analysis of impacts, program constraints, operational experience, and a cost-benefit analysis.

6.2.4 The entity shall have a process to monitor the identified hazards and adjust the level of preventive measures to be commensurate with the risk.

Prevention Methods

- Fire prevention
- Injury & illness prevention programs
  - Safety/accident prevention
  - Occupational health
  - Immunizations, isolation, or quarantine
- Physical & operational security
  - Deterrence operations
  - Surveillance and security operations
- Provision of protective systems or equipment for physical risks
- Computer/cyber security
Auditing Prevention Strategies

**Interviews/Surveys/Documents**
- Interviews
  - Program coordinator
  - EHS manager
  - Risk manager
  - Human resources
  - IT manager
  - Facility, operations, engineering, fleet managers
- Survey
- Documents
  - Risk assessment
  - Business impact analysis
  - Insurance loss prevention reports
  - Insurance claims
  - OSHA logs

**Evidence of Conformity**
- Do strategies address:
  - Life safety
  - Property protection
  - Environmental protection?
- Are there prevention strategies to address the identified hazards?
- Is there a process to collect information and intelligence to adjust preventive measures?
- Is there an ongoing process to monitor hazards—in real time—if required?

6.3 Mitigation

6.3.1 The entity shall develop and implement a mitigation strategy that includes measures to be taken to limit or control the consequences, extent, or severity of an incident that cannot be prevented.

6.3.2 The mitigation strategy shall be based on the results of hazard identification and risk assessment, an analysis of impact, program constraints, operational experience, and cost-benefit analysis.

6.3.3 The mitigation strategy shall include interim and long-term actions to reduce vulnerabilities.

Hazard Mitigation

- Compliance with building codes
- Hazard avoidance through land-use practices
- Removal or elimination of the hazard
- Segregation of hazard
- Modification of characteristics of hazard
- Control of rates of release of the hazard
- Protective systems or equipment for physical risks
- Hazard warning and communication
- Redundancy or duplication of essential personnel, critical systems, equipment
Financial Risk Mitigation

- Insurance is financial risk mitigation
- Lines of coverage:
  - Property damage
  - Business interruption (time element)
  - Contingent business interruption
  - Liability
- Endorsements:
  - Extra expense
  - Extended period of indemnity

Is insurance coverage aligned with risk assessment and BIA?

Auditing Mitigation Strategies

Interviews/Surveys/Documents
- Interviews
  - Program coordinator
  - Strategic planner
  - EHS manager
  - Risk manager
  - Human resources
  - IT manager
  - Facility, operations, engineering, supply chain, field managers
- Survey
- Facilities
- Documents
  - Risk assessment
  - Business impact analysis
  - EHS program documents
  - Insurance loss prevention reports
  - Capital budget

Evidence of Conformity
- Do strategies address protection of life, property, and the environment?
- Are there strategies to mitigate potential impacts?
- Has money been budgeted short-term and long-term?

Discussion

1. Discuss some of the prevention methods used in Business Continuity and Emergency Management.
2. What is “mitigation”?
3. What are “mitigation strategies”?
Resource Management
6.7.7 Resource management shall include the following tasks:
(1) Establishing processes for describing, taking inventory of, requesting, and tracking resources
(2) Resource typing or categorizing by size, capacity, capability, and skill
(3) Mobilizing and demobilizing resources in accordance with the established IMS
(4) Conducting contingency planning for resource deficiencies
6.7.8 A current inventory of internal and external resources shall be maintained.
6.7.9 Donations of human resources, equipment, material, and facilities shall be managed.

Resource Requirements
4.4.1(5)(c) … entity shall have … program plans and procedures that include … resources required
6.1.2(7) Plans shall identify…logistics support and resource requirements.

What are the program goals and objectives?
- Protect the health and safety of people
- ____________________________________________
- ____________________________________________

What are the hazards impacting the entity?
Processes to describe, inventory, request, track resources
Activating these processes prior to and during an incident
Dispatching resources prior to and during an incident
Deactivating or recalling resources during or after incidents
Contingency planning for shortfalls of resources
Logistics Procedures

- Locate, acquire, store, distribute, maintain, test, and account for
- Services, personnel, resources, materials, and facilities
- Procured or donated to support the program.

Resource Inventory

6.7.8 A current inventory of internal and external resources shall be maintained.
- Funding
- Trained staff, expert knowledge
- Facilities
- Information technology
- Equipment
- Materials and supplies
- Information and intelligence

Materials & Supplies

- Consumable
- Timely re-supply needed to meet goals and objectives
- Procurement strategies
  - Purchase in advance
  - Quick ship contracts
  - Procure at the time of disaster
  - Risk management
- Examples
  - Extra batteries, battery meters, and chargers
  - Food, water, etc.
  - Medical or first aid supplies
  - Fuel
  - Salvage covers
  - Cleanup supplies
  - Paper, pens, pencils
  - Checks
  - Paper Forms
Resource Requirements: Fire

Goals
- Prevent fires
- Protect life
- Minimize property damage
- Prevent business interruption
- Prevent environmental contamination
- Protect image & reputation
- Comply with regulations

Selected Resources
- Fire protection engineer
- Detection & suppression systems
- Occupant notification system
- Means of egress (exits)
- Evacuation team
- Fire brigade
- Crisis communications team
- Mutual Aid
- Emergency response plan
- Business continuity plan
- Alternate facilities
- Hazardous materials containment
- Funding

Resource Requirements: Power Outage

Goals
- Protect people
- Protect property
- Continue partial or full business functions
- Protect the environment

Selected Resources
- Trained personnel
- Emergency lighting
- Communications capability
- Supplies for sheltering
- Uninterruptible power supplies
- Generators
- Fuel supply for 72 hours

Mutual Aid/Assistance

5.4.5* Agreements. The need for mutual aid/assistance or partnership agreements shall be determined; if needed, agreements shall be established and documented.

The need for mutual aid/assistance should be determined for:
- Private-Private Partnerships
- Public-Private Partnerships
- Public-Public Partnerships
Donations

6.7.9 Donations of human resources, equipment, material, and facilities shall be managed.

Auditing Resource Management

Interviews/Surveys/Documents
- Interviews
  - Program coordinator
  - Team leaders and members
  - Public services (fire, hazmat, police, health, emergency medical)
  - Purchasing or procurement
- Surveys
  - Facilities (alternate workspace—offices, call center, data center, manufacturing, etc.)
  - IT (hardware, networking, applications, data)
  - Vital records
  - Systems (detection, alarm, communication, and suppression; etc.)
  - Life safety (exits, lighting, signs, etc.)
  - Equipment, materials, and supplies
- Documents
  - Budget
  - Rosters and contact lists
  - Plans (Emergency response, business continuity, communications, DRP)
  - Resource inventory
  - Partnership/mutual aid agreements
  - Vendor contracts (quick ship, hot site, etc.)

Evidence of Conformity
- Needs assessment conforming to 6.7.5 has been completed
- Needs assessment is based on risk assessment
- Current resource inventory maintained
- Verification that resources identified in plan documents are available within required time frame
- Resources have required capabilities
- Resources are in reliable conditions
- Logistics procedures to execute program
- Procedures for donations management
6.5 Warning, Notifications, and Communications

6.5.1* The entity shall determine its warning, notification, and communications needs.

6.5.2* Warning, notification, and communications systems shall be reliable, redundant, and interoperable.

6.5.3* Emergency warning, notification, and communications protocols and procedures shall be developed, tested, and used to alert stakeholders potentially at risk from an actual or impending incident.

6.5.4 Procedures shall include issuing warnings through authorized agencies if required by law as well as the use of prescribed information bulletins or templates.
Auditing Communications & Warning

**Interviews/Surveys/Documents**

- Interviews
  - Program coordinator
  - Teams (emergency response, business continuity, crisis communications)
  - Security and building management staff
- Surveys
  - Early warning systems
  - Audibility and intelligibility of warning systems
- Documents
  - Plan documents
  - Inspection, testing, and maintenance records
  - Training records

**Evidence of Conformity**

- Systems, protocols, and procedures for early notification and warning
- Warning system audible and intelligible by all building occupants
- Reliable means to alert:
  - Team members
  - Public emergency services
  - Contractors and vendors
- Ability to communicate with employees, stakeholders, others
- Effective communication within and between:
  - Teams
  - Management
  - Public agencies
  - Contractors and vendors
- Systems and equipment tested; personnel trained

---

**6.6 Operational Procedures**

6.6.1 The entity shall develop, coordinate, and implement operational procedures to support the program.

6.6.2* Procedures shall be established and implemented for response to and recovery from the impact of hazards identified in 5.2.2.

6.6.3* Procedures shall provide for life safety, property conservation, incident stabilization, continuity, and protection of the environment under the jurisdiction of the entity.

6.6.4 Procedures shall include the following:

1. Control of access to the area affected by the incident
2. Identification of personnel engaged in activities at the incident
3. Accounting for personnel engaged in incident activities
4. Mobilization and demobilization of resources

6.6.5 Procedures shall allow for concurrent activities of response, continuity, recovery, and mitigation.

---

Auditing Operational Procedures

**Interviews/Surveys/Documents**

- Interviews
  - Program coordinator
- Documents
  - Emergency response
  - Business continuity
  - Crisis communications

**Evidence of Conformity**

- Plans address:
  - Hazard scenarios (risk assessment)
  - Business impacts (BIA)
- Roles and responsibilities defined by incident management system
- Procedures for situation analysis, needs assessment, and incident action plan development included
- Connectivity, coordination, and communications between plans:
  - Emergency response
  - Business continuity
  - Crisis communications
6.7 Incident Management

6.7.1* The entity shall develop an incident management system to direct, control, and coordinate response and recovery operations.

6.7.2 The incident management system shall describe specific organizational roles, titles, and responsibilities for each incident management function.

6.7.3 The entity shall establish procedures and policies for coordinating mitigation, preparedness, response, continuity, and recovery activities.

6.7.4 The entity shall coordinate the activities specified in 6.7.3 with stakeholders.

6.7.5 Procedures shall include a situation analysis that incorporates a damage assessment and a needs assessment to identify resources to support activities.

6.7.6* Emergency operations/response shall be guided by an incident action plan or management by objectives.

Incident Management System

The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents.

6.7.1.1* Emergency Operations Center

6.7.1.1.1* The entity shall establish primary and alternate EOCs capable of managing response, continuity, and recovery operations.

6.7.1.2* The EOCs shall be permitted to be physical or virtual.

6.7.1.3 On activation of an EOC, communications and coordination shall be established between incident command and the EOC.
Emergency Operations Center

- Physical location or virtual facility
- Permanent or established when needed (in accordance with plan)
- Primary and alternate EOCs should be located so they are not impacted by the same event.
- Reliable communications capability—with backups.
- Staffed by a wide variety of personnel from internal departments and external agencies

Centralized management center to facilitate policy making, coordination and overall direction of the response and recovery efforts
- Communications/information clearinghouse for information collection, analysis, sharing, dissemination
- Resource dispatching and tracking
- Providing direction and control, and warning

EOC Resources
- Tables, chairs, easels (with markers), projection screen
- Telephones (landline, cell, satellite) with speakerphones for meeting rooms
- Plan documentation in hard copy (emergency response, business continuity, crisis communications, crisis management, contact/telephone lists, resource inventory, etc.)
- Computers (desktop and or laptop) with access to plan documentation, software tools, LAN, WAN, Internet
- Computer projection unit, access to photocopiers
- AM/FM radio, television with recording capability
- Food, water with utensils
Incident Command Assignments

- Incident Commander
- Command Staff
- General Staff

Incident Commander

- Person in charge of the organization's on-scene response
- Maintain command until public agencies arrive and assume command, or when relieved at start of next operational period
- Establish the Incident Command Post at a safe location inside or outside depending upon the nature and location of the incident
- Assess the situation (conducts a Situation Analysis)
- Order warning of persons at risk or potentially at risk to take appropriate protective actions
- Notify or verify internal teams, departments, public agencies, regulators, contractors, and suppliers have been notified
- Appoint General Staff and Command Staff officers as needed

- Brief General and Command Staff on current organization and activities; assign tasks; schedule planning meeting
- Determine the incident objectives and strategy; identify information needed or required by others; ensure planning/strategy meetings are held and attend as needed
- Coordinate activities with the EOC; identify priorities and activities; provide impact assessment for business continuity and senior management
- Review requests for resources; confirm who has authority to approve procurement; approve all requests for resources as required
- Provide information to and coordinate with crisis communications or media relations team
- Terminate the response and demobilize resources when the situation has been stabilized
**Command Staff**

**Information Officer**
- Notify spokespersons and Crisis Communications Team
- Develop information for use in media briefings
- Obtain IC’s and management approval for all news releases
- Conduct periodic media briefings
- Arrange for tours, interviews, and/or briefings
- Monitor and forward media useful information

**Safety Officer**
- Identify and assess hazardous situations; prevent accidents
- Prepare safety plan; ensure messages communicated
- Stop unsafe acts; correct unsafe conditions

**Liaison Officer**
- Point of contact with outside agencies and companies
- Monitors operations to identify inter-organizational problems

**Operations Section**

- Manage all tactical operations during the incident
- Assist in the development of the operations portion of the Incident Action Plan
- Ensure safe tactical operation for all responders (in conjunction with any assigned Safety Officer)
- Request additional resources to support tactical operations
- Expedite appropriate changes in the operations portion of the Incident Action Plan
- Maintain close communication with the Incident Commander

**Planning Section**

- Conduct and facilitate planning meetings
- Supervise preparation of the Incident Action Plan
- Determine need for technical experts from within the company or outside as well as specialized resources to support the incident
- Coordinate with business continuity and senior management teams
- Assemble information on alternative strategies and plans
- Assess current and potential impacts on people, property, environment
- Compile and display incident status information
Logistics Section

- Provides resources to stabilize the incident and support the personal, systems, and equipment:
  - Workspace or facilities for incident management staff
  - Media briefing center
  - Transportation
  - Communications equipment
  - Food, water, shelter, and medical care
- Ensures Incident Command Post and other facilities have been established as needed
- Assesses communications needs and facilitates communications between teams/personnel/agencies
- Attends planning meetings; provides input to Incident Action Plan
- Provides updates on resources (availability, response time, deployment)
- Estimates and procures resources for the next operational period

Finance/Administration Section

- Manages all financial aspects of the incident
- Provides financial and cost analysis information as requested
- Create accounts for claims and costs; coordinates with Logistics
- Tracks worker time and costs for material and supplies
- Documents claims for damage, liability, and injuries
- Notifies risk management/insurance to initiate claims reporting
- Provides incurred and forecasted costs at planning meetings
- Provides oversight of financial expenditures, new leases, contracts and assistance agreements to comply with corporate governance

Incident Command Assignments

- Command:
  - Incident Commander
  - Safety
  - Public Information
  - Liaison
- Sections:
  - Operations
    - Evacuation/SHP
    - Fire
    - Security
    - HazMat
    - Rescue
    - Property Conservation
  - Planning
    - Strategic Analysis
    - Information Management
    - Public Information
    - Technical Support
  - Logistics
    - Facilities
    - Communications
    - Planning
    - Equipment & Supplies
    - Food & Water
    - Shelter
    - Medical
  - Finance & Administration
    - Time & Cost Accounting
    - Compensation
    - Claims
    - Procurement

© 2013, National Fire Protection Association and DRI, International, All Rights Reserved
**Incident Reporting**

- Develop criteria for reporting incidents
- Report incidents to local/division/business unit/corporate mgt.
- Regulatory authorities: OSHA, EPA, SERC, etc.
- Insurance companies
- Complete required incident report and investigation

**Incident Briefing**

- Incident command assignments: Internal, External (public agencies on scene)
- Incident facilities: Command Post, EOC
- Incidents details: What, Where, Hazards & impacts, Overall incident status

**Incident Action Plan**

- Who should be notified to respond or warned to take protective action?
- What protective actions are warranted?
- What actions are required to stabilize or manage the incident?
- What resources are needed? What is the status of resources ordered?
Incident Response Example

Unified Command

Auditing Incident Management
6.8 Emergency Response

6.8.1* Emergency operations/response plans shall assign responsibilities for carrying out specific actions in an emergency.

6.8.2* The plan shall identify actions to be taken to protect people, including those with access and functional needs, property, operations, the environment, and the entity.

6.8.3* The plan shall identify actions for incident stabilization.

6.8.4 The plan shall include the following:

1. Protective actions for life safety in accordance with 6.8.2
2. Warning, notifications, and communication in accordance with Section 6.5
3. Crisis communication and public information in accordance with Section 6.4
4. Resource management in accordance with 6.7.7
5. Donation management in accordance with 6.7.9

Evacuation Plan

- Building/Site Population
  - Number of occupants, areas with high density
  - Procedures and equipment for evacuating persons with disabilities
- Means of Egress System
  - Number, capacity, and arrangement of exits and areas of refuge or rescue assistance
  - Type and limitations of warning system
  - Primary and secondary evacuation routes and assembly areas
- Evacuation Team
  - Organized evacuation team with defined roles and responsibilities
- Evacuation Plan
  - Decision matrix for full, partial, or adapted evacuation based on building construction, occupancy, hazards, and protection
  - Prepared scripts for emergency announcements
- Training & Drills
  - Training members of the Evacuation Team
  - Evacuation instructions provided to all occupants
  - Evacuation drills conducted at least annually or as required by regulations
**Evacuation Team**

- **Evacuation Team Leader**
- **Floor Plan**
- **Exit Routes**
  - Number
  - Capacity
  - Arrangement
  - Illumination
  - Signs
  - Unobstructed
- **Warning System**
- **Floor Diagrams**
- **Evacuation Team**
- **Ability to evacuate or protect persons with disabilities**
- **Assembly Areas**
- **Ability to account for evacuees**
- **Drills conducted as required**

**Auditing the Evacuation Plan**

- **Exit Routes**
  - Number
  - Capacity
  - Arrangement
  - Illumination
  - Signs
  - Unobstructed
- **Warning System**
- **Floor Diagrams**
- **Evacuation Team**
- **Ability to evacuate or protect persons with disabilities**
- **Assembly Areas**
- **Ability to account for evacuees**
- **Drills conducted as required**

**Lockdown**

- **Employed when there is a security threat or suspected threat:**
  - Act of violence in progress
  - Intruder inside or believed to be inside the building
  - “Secure and hold” (moving everyone inside and locking exterior doors) would be employed if the threat was outside the building (e.g., disturbance outside, police chasing a bank robbery suspect)
- **Lockdown Capability**
  - Ability to broadcast “lockdown” throughout the building(s) from a safe location
  - Audible and intelligible announcements
  - Scripts and training for announcements
  - Training and drills for occupants to barricade themselves in a safest room
  - Access to surveillance cameras by police to identify location of an nature of threat
**Shelter-In-Place**

- Temporary protective action
  - Exterior airborne hazard
  - Safer to remain inside
  - Insufficient time to evacuate
- Warning from public emergency services and by Emergency Alert System receiver
- Personnel move to safer locations within the building.
  - Above the ground floor
  - Minimal vents and doors to close
  - Interior rooms and offices are preferable to offices or large spaces on the outside or with exterior windows or doors
- Location of control and procedures for shutting down air handling units, fans, and outside air intakes documented
  - Controls marked “Shelter-in-Place Shutoff.”
  - Time to shutdown determined
- Awareness training for occupants; drills for building management staff who shutdown air handling systems

**Sheltering**

- Tornado
  - Emergency alert system receiver
  - Weather monitoring
  - Distinct warning sound
  - Tornado shelters
- Other sheltering scenarios
  - Weather
  - Transportation interruption
  - Blackout (e.g., August 2003)

**Persons with Special Needs**

- Identify persons with temporary or permanent disabilities or special needs:
  - Mobility
  - Sight
  - Hearing
  - Cognitive
- Address
  - Evacuation and sheltering
  - Assist devices
  - Designated aides
  - Coordination with public emergency services
Medical Emergency Plan

- On-site medical capability only required if not in “near proximity” to medical capability
- Medical Emergency Plan
  - Current roster of persons certified in first aid, CPR, and use of Automated External Defibrillator
  - Procedures for prompt notification of public emergency services
  - Procedures for any site-specific chemical exposure
  - Coordination with other emergency plans
- Training and Certification
  - Perform CPR and use Automated External Defibrillator
  - First aid training that includes “universal precautions” to prevent exposure to bloodborne pathogens
- Resource Inventory
  - First aid kits with “Universal Precautions” kits
  - Treatment for any site-specific hazards
  - Automated External Defibrillators

Firefighting

- Minimum Requirements
  - Fire Prevention Code
  - Local ordinances
- If a Fire Brigade has been organized:
  - OSHA 1910.156, Fire Brigades (minimum)
  - NFPA 600, Standard on Industrial Fire Brigades
  - NFPA 1081, Industrial Fire Brigade Member Professional Qualifications

HazMat “Emergency Response”

Responses to incidental releases of hazardous substances where the substance can be absorbed, neutralized, or otherwise controlled at the time of release by employees in the immediate release area, or by maintenance personnel are not considered to be emergency responses within the scope of this standard.

“Emergency response” is an effort by employees from outside the immediate release area or by other designated responders (i.e., mutual aid, fire dept., etc.) to an occurrence which results, or is likely to result, in an uncontrolled release of a hazardous substance.
HazMat Plan

- Type, location, and quantity of all hazardous material documented
- Scenarios for hazardous materials spills or releases identified; procedures for each scenario
- Material Safety Data Sheets compiled for all hazardous materials
- Hazard Communication “Right to Know” program in place (OSHA 1910.1200)
- Hazmat information documented on Pre-Incident Planning Form
- Evacuation routes reviewed to determine how evacuees must be redirected

Organizational Statement

- Required for:
  - Fire brigades
  - Hazardous materials response teams
- Defines
  - Functions of ERT
  - Command structure
  - Personnel, equipment, and training
- Has it been approved by management in accordance with the policy statement?

Rescue Plan

- Confined spaces, stacks, cranes, process structures, waterfront, entrapment, and other works areas that may require rescue or extrication have been identified
- Confined spaces reviewed to determine if any are “permit-required”
- Fire Department (or rescue service)
  - Review confined spaces and rescue scenarios
  - Identifies their rescue capabilities and ability to extract confined space entrants
  - Conducts exercises to validate capability
  - Is on-site when authorized entry to permit-required confined spaces
- Confined spaces and other rescue scenarios documented on Pre-Incident Planning Form
- Conformity to NFPA 1670 “Standard on Operations and Training for Technical Search and Rescue Incidents” suggested
Natural Hazards

- Plan for hazards identified in risk assessment:
  - Earthquake
  - Flood, flash flood
  - Hurricane
  - Landslide or subsidence
  - Lightning
  - Severe thunderstorm
  - Tornado
  - Severe winter storm
- Protective actions for life safety
- Property conservation

Security Threats Hazards

- Plans for threats or acts of violence:
  - Missing person
  - Abduction/kidnapping
  - Fights, assaults, sexual assaults
  - Protests, civil unrest
  - Trespasser, intruder
  - “Active shooter”
- Protective actions
  - “secure and hold”
  - lockdown

Suspicious Package

- Detection
- Isolation
- Protective actions
  - Evacuation
  - Washing exposed skin that was in contact
  - Shutdown of HVAC
- Communication and coordination with first responders
Bomb Threat Plan

- Protocol for bomb threats developed after consultation with local law enforcement
- Decision matrix to:
  - Evacuate immediately
  - Search and evacuate only if a suspicious item is found, or
  - Do nothing.
- Procedures to direct occupants to exit routes away from device; routes inspected for safety before use
- If there is a search team:
  - Defined roles and responsibilities aligned with search zones (marked floor plans)
  - Room search tags
- Bomb Threat Checklist distributed
- Caller ID, recording, and tracing capabilities and procedures identified
- Training for all who may receive threats

Utility Outage Plan: Electricity

- Critical systems identified:
  - Communication systems
  - Life safety (illumination of exit travel paths, alarm system)
- Emergency Power Supplies:
  - Identify emergency power supplies and equipment it powers
  - Evaluate fuel supply capacity and expected run time under full load
  - Verify equipment is properly inspected, tested, and maintained with fuel level at least ¾ full
  - Identify systems and equipment that must be turned off before power is restored to prevent surge damage

Utility Outage Plan: Other

- Plans for the loss of:
  - Water supplies and building pumps
  - Sanitary systems
  - HVAC systems
- Elevator emergencies including service emergency contact
- Diagrams and operating instructions of the following compiled:
  - Electrical disconnects
  - Domestic potable water
  - Fire protection (pumps, sprinkler risers, sectional control valves)
  - Steam lines
  - Natural gas meter and main shutoff
  - Oil tanks
Property Conservation
- Clean up and restore facility after damage has occurred
- Prepare facility for forecast event (e.g., storm)
- Resources (personnel, equipment, materials, supplies)

Coordination with Public Agencies
- Pre-incident planning of buildings, utility systems, fire protection and life safety systems, and occupancy hazards
- Review and coordination of emergency procedures with their tactical operations

<table>
<thead>
<tr>
<th>Agency</th>
<th>Plan to be Reviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire Dept</td>
<td>Local or county</td>
</tr>
<tr>
<td>Local Emergency Planning Team</td>
<td>Local or regional</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td>Local, county, or state</td>
</tr>
<tr>
<td>Emergency Medical Services</td>
<td>Ambulance, paramedics, fire dept., private service</td>
</tr>
<tr>
<td>Emergency Management</td>
<td>Local or county</td>
</tr>
</tbody>
</table>

Pre-Incident Planning
- Surveys by public emergency services
- Compilation of information (NFPA 1620 defines process)
- Accessible to emergency responders
### Auditing Emergency Response Plan

<table>
<thead>
<tr>
<th>Interviews &amp; Surveys</th>
<th>Documents to Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Interviews</td>
<td>- Emergency response plan(s)</td>
</tr>
<tr>
<td>- Emergency response team leaders and members</td>
<td>- Evacuation plan</td>
</tr>
<tr>
<td>- Security</td>
<td>- Lockdown procedures</td>
</tr>
<tr>
<td>- Human resources</td>
<td>- Shelter-In-Place plan</td>
</tr>
<tr>
<td>- EHS</td>
<td>- Shelter plan (e.g., tornado)</td>
</tr>
<tr>
<td>- Survey</td>
<td>- Threat-specific procedures</td>
</tr>
<tr>
<td>- Exit routes, assembly areas</td>
<td>- Interruption/disruption of utilities</td>
</tr>
<tr>
<td>- Hazards (inside and outside)</td>
<td>- Pre-Incident Plan</td>
</tr>
<tr>
<td>- Security</td>
<td>- Property conservation</td>
</tr>
<tr>
<td>- Fire detection, alarm, communications, and suppression systems</td>
<td>- Resource inventory</td>
</tr>
<tr>
<td>- Building command center</td>
<td>- Rosters</td>
</tr>
<tr>
<td>- Incident command post</td>
<td>- Systems, equipment, materials, supplies</td>
</tr>
<tr>
<td>- Emergency Operations Center</td>
<td>- Records</td>
</tr>
<tr>
<td></td>
<td>- Training</td>
</tr>
<tr>
<td></td>
<td>- Drills</td>
</tr>
<tr>
<td></td>
<td>- Exercises</td>
</tr>
<tr>
<td></td>
<td>- Incident reports</td>
</tr>
</tbody>
</table>

### Evidence of Conformity

- Addresses hazards and impacts identified during risk assessment
- Plans and procedures to protect
  - Life safety including persons with special needs
  - Property
  - Operations
  - Environment
- Plans and procedures to stabilize an incident
- Assigned responsibilities for carrying out specific actions
- Incident management system
- Sufficient resources (e.g., trained personnel, systems, equipment, materials, and supplies) to safely execute plans

### Evidence of Regulatory Compliance

<table>
<thead>
<tr>
<th>Minimum requirements</th>
<th>Regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Protective actions for life safety</td>
<td>- OSHA regulations</td>
</tr>
<tr>
<td>- Medical capability if not in “near proximity” to medical services</td>
<td>- Environmental regulations</td>
</tr>
<tr>
<td>- Hazardous materials response capability if regulated facility</td>
<td>- Fire prevention code</td>
</tr>
<tr>
<td>- Rescue capability required for permit-required confined spaces</td>
<td>- Life safety code</td>
</tr>
<tr>
<td>- Regulatory compliance if fire brigade organized (conform to national standards recommended)</td>
<td>- Homeland security ordinances</td>
</tr>
<tr>
<td>- Environmental protection for regulated facilities</td>
<td></td>
</tr>
</tbody>
</table>
6.1 Common Plan Requirements

6.1.1* Plans shall address the health and safety of personnel.

6.1.2 Plans shall identify and document the following:
   (1) Assumptions made during the planning process
   (2) Functional roles and responsibilities of internal and external agencies, organizations, departments, and positions
   (3) Lines of authority
   (4) The process for delegation of authority
   (5) Lines of succession for the entity
   (6) Liaisons to external entities
   (7) Logistics support and resource requirements

6.1.3* Plans shall be individual, integrated into a single plan document, or a combination of the two.

6.1.4* The entity shall make sections of the plans available to those assigned specific tasks and responsibilities therein and to key stakeholders as required.

Discussion

1. What is "property conservation"?
2. What is the purpose of emergency response procedures?
3. Discuss the following types of emergency response plans:
   a. Evacuation
   b. Shelter-In-Place
   c. Sheltering
   d. Lockdown
6.9 Business Continuity & Recovery

6.9.1* The continuity plan shall include recovery strategies to maintain critical or time-sensitive functions and processes identified during the business impact analysis.

6.9.2 The continuity plan shall identify stakeholders that need to be notified; critical and time-sensitive applications; alternative work sites; vital records, contact lists, functions, and processes that must be maintained; and personnel, procedures, and resources that are needed while the entity is recovering.

6.9.3* The recovery plan shall provide for restoration of functions, services, resources, facilities, programs, and infrastructure.

6.6 Operational Procedures

6.6.1 The entity shall develop, coordinate, and implement operational procedures to support the program.

6.6.2* Procedures shall be established and implemented for response to and recovery from the impact of hazards identified in 5.2.2.

6.6.3* Procedures shall provide for life safety, property conservation, incident stabilization, continuity, and protection of the environment under the jurisdiction of the entity.

6.6.4 Procedures shall include the following:

(1) Control of access to the area affected by the incident
(2) Identification of personnel engaged in activities at the incident
(3) Accounting for personnel engaged in incident activities
(4) Mobilization and demobilization of resources

6.6.5 Procedures shall allow for concurrent activities of response, continuity, recovery, and mitigation.
Terminology

Business Continuity
The identification and protection of business processes required to maintain an acceptable level of operations in the event of sudden, unexpected, or not so unexpected, interruptions of these processes and their supporting resources.

IT Disaster Recovery
The documented procedures for the continuation or recovery of the technology that supports the entity.

Business Continuity Planning Process

Business Impact Analysis
1. Conduct BIA questionnaire using senior management’s recovery objectives.
2. Conduct BIA workshop with business representatives.
3. Distribute BIAs and receive completed forms from business representatives.
4. Review BIA questionnaires.
5. Conduct follow-up interviews with business unit representatives.

Recovery Strategies
- Identify and document resource requirements based on BIAs.
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities.
- Explore options (operations and IT).
- Define strategy options.
- Select recovery strategies with management approval.
- Implement strategies.

Plan Development
- Develop plan framework.
- Organize recovery teams.
- Develop relocation plans.
- Write business continuity and IT disaster recovery procedures.
- Document manual workarounds.
- Assemble plan; validate; gain management approval.

Testing & Exercises
- Develop testing, exercise, and maintenance requirements.
- Train staff on BCP plan.
- Conduct orientation exercises.
- Conduct testing and document test results.
- Update BCP Plan to incorporate lessons learned from testing and exercises.

Recovery Strategies
Recovery strategies are driven by the recovery time objectives (RTO) developed during the Business Impact Analysis (BIA).
- Surviving site
- Dedicated alternate
- Non-dedicated alternate
- Manual Workarounds
- Displacement
- Telecommuting (work from home)
- Internal Alternate Site in Dual Usage Space
- Reciprocal/mutual aid agreements
- External suppliers
Surviving Site Strategy

- Used when an organization operates in more than one geographic location
- Used to support business operations with short recovery windows like call centers
- Workload is split between two or more sites. When one site becomes unavailable, the surviving site(s) take on all of the workload
- Service levels may drop but function does not stop operating
- Service level issues may be addressed by staff reassignment, triage of work so most important work is addressed first, auto attendant asking customer to call back if request is not urgent, extending work hours to accommodate load, hiring temporary staff and so forth

Dedicated Alternate Sites

- Built by the entity to recover operations
- Commonly used by large organizations with short recovery windows and unique recovery requirements; not easily implemented
- Expensive solution but utilized when loss potential is significant justifying the recovery costs
- Very hard sell to have space and technology sitting there waiting for the “big one”
- Recovery time for this strategy is dependent on the distance between the impacted site and the recovery location and the method used to equip the site at time of disaster

Non-Dedicated Alternate Strategy

- Used where an organization has more than one facility
- Facility designated as recovery site has excess space that can be utilized by recovery staff
- Recovery time is determined by the distance between the two sites and whether the space to be occupied is equipped with the resources needed to support recovery or if it must be equipped at the time of disaster
- The logistics of moving staff and workload is very important to document as part of the plan documentation
- Changes in workload as a result of the disaster must also be documented
- Facility information (stacking plans, phone and network capacity, etc.) must be tracked to ensure availability of space when needed
**Manual Workarounds**

- Continue business operations in the absence of technology
- Fill time gaps
- Process to develop manual workarounds
  - Decompose automated process
  - Establish manual intervention points
  - Establish control logs

**Displacement**

- Used where an organization has more than one facility
- Facility designated as recovery site will displace staff performing non-time-sensitive functions to make room for recovery staff
- Recovery time is determined by the distance between the two sites and whether the space to be occupied is equipped with all the resources needed to support recovery or if changes must be made ATOD
- The logistics of moving staff and workload is very important to document as part of the plan documentation
- Changes in workload as a result of the disaster must also be documented
- Facility information (stacking plans, etc) and employee info must be tracked to ensure availability of space when needed

**Telecommuting (Work From Home)**

- Used when the entity has the capability to support staff working from home through remote connectivity
- Can be used in combination with other strategies to reduce alternate site requirements
- Functions to work from home should be carefully chosen
- Unless organization will provide requirements, staff should be surveyed to determine the following:
  - Have assigned laptop or home computer with high-speed connection (dial-up is too slow in many circumstances)
  - Peripherals (e.g., printer, fax or fax software)
  - Employee can connect with required security (VPN)
  - Suitable office-type work environment
  - Awareness and ability to ensure information security and privacy, proprietary waste disposal, etc.
- Strategy unavailable if the home has been impacted by the same event as the office
Internal Alternate Site In Dual Usage Space

- Used where an organization operates in more than one location and has dual usage space that can be equipped to support business operations.
- Locations to consider include cafeterias, conference rooms, training rooms.
- Requires up front costs to prepare sites for work like network cabling, additional power outlets, excess capacity on phone switch, network to support additional users.
- Equipment to populate the space can be stored on site or provided through a drop ship agreement or purchased at time of disaster.
- Recovery time for this strategy is dependent on the distance between the impacted site and the recovery location and the method used to equip the site at time of disaster.

Reciprocal/Mutual Aid Agreements

- An agreement entered into by two like organizations to support each other by providing facilities to each other for use in the event of a disaster.
- Requires up front negotiations between the parties to define clearly what space or equipment may be used, for how long, and under what circumstances.
- Requires parties to carefully consider issues like network connectivity, phone capacity, privacy, intellectual property, costs to operate, impact to each others operations, expense to re-tool.
- Agreement need to be periodically reviewed to make certain nothing has changed to prevent its practical use.
- Recovery time for this strategy is dependent on the distance and the start up time to use the facility.

External Suppliers

- Contracted alternate sites with recovery vendors.
- Vendor provides business environment and commonly used technology (computers, printers, fax machines, telephones).
- Unique equipment may need to be provided by the entity.
- Seats and technology sold to multiple customers of recovery provider with the assumption that not everyone will experience a disaster at the same time.
- Some vendors provide dedicated space at additional cost.
- Space and technology can be provided in physical building where recovery staff would travel to or through Mobile Units which are delivered and set up wherever you specify.
- Generally a less expensive solution than internal dedicated space or dual usage space.
- Recovery time for this strategy is dependent on the distance between the impacted site and the recovery location and the specific services contracted for.
Technology Recovery Strategies

- **Dual Data Center** – this strategy is employed for applications which cannot accept any downtime without impacting business.
- **Internal Hot site** – this site is standby ready with all necessary technology and equipment necessary to run the applications recovered there.
- **External Hot Site** - This strategy has equipment on the floor waiting for recovery but the environment must be re-built for the recovery.
- **Warm Site** – A leased or rented facility that is usually partially configured with some equipment, but not the actual computers.
- **Cold Site** – A cold site is a shell or empty data center space

Data Back-up Strategies

- **Replication** – Synchronous or Asynchronous
- **Tape Backups**
  - Full – point in time full copy of all data
  - Incremental – copy of only the data that has changed since the last back-up
  - Differential – copy of everything that has changed since the last FULL back-up

How the data is backed up and where it is stored will have a significant impact on the amount of time it takes to recover.

Dual Data Center/High Availability

- This strategy is employed for applications which cannot accept any downtime without impacting business.
- Applications are split between two geographically dispersed data centers and either load balanced between the two centers or hot swapped to the two centers (active/active – active/passive)
- The surviving data center must have enough head room to carry the full production load in either case
### Hot Site Strategies

**Hot Site**
A fully equipped data center space with information technology on the floor. No technology must be purchased or acquired at the time of a disaster.

**External Hot Site**
A hot site owned/operated by an external organization such as a commercial recovery vendor or third party.

**Internal Hot Site**
A hot site owned/operated by an organization actually performing recovery operations.

### Warm Site

- A leased or rented facility or owned space that is unoccupied
- Usually partially configured with some equipment
  - Cooling
  - Cabling
  - Networks
- Servers, mainframe equipment etc are delivered to the site at time of disaster

### Cold Site

- A cold site is a shell or empty data center space with no technology on the floor
- All technology must be purchased or acquired at the time of disaster
Technology Recovery Times

- High Availability Solutions
- Hot Site with Remote Replication
- Remote replication of data
- Virtual tape system
- Tapes and Trucks

- Cold Site
- Warm Site

<table>
<thead>
<tr>
<th></th>
<th>Maximum</th>
<th>Minimum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours</td>
<td>0</td>
<td>50</td>
</tr>
<tr>
<td>Weeks</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Manufacturing Strategies

- Retooling to change production from one item to another
  - Cost
  - Time
- Proximity may impact shipments to/from:
  - Customers
  - Suppliers

- Business relocation:
  Switching production from damaged or unavailable site to another owned or controlled site
  - Available capacity will probably limit production
  - Prioritization of production—which items are produced first?
    - By profit margin - SKU prioritization
    - By customer relationship
## Margins by Manufacturing Plant

<table>
<thead>
<tr>
<th>Plant</th>
<th>Domestic P Cases</th>
<th>Domestic $ Margin</th>
<th>Region P Cases</th>
<th>Region $ Margin</th>
<th>Total P Cases</th>
<th>Total $ Margin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11,977</td>
<td>332,991</td>
<td>638</td>
<td>17,737</td>
<td>12,615</td>
<td>350,728</td>
</tr>
<tr>
<td>2</td>
<td>6,919</td>
<td>101,730</td>
<td>1,228</td>
<td>18,056</td>
<td>8,147</td>
<td>119,785</td>
</tr>
<tr>
<td>3</td>
<td>19,227</td>
<td>180,205</td>
<td>2,232</td>
<td>20,919</td>
<td>21,459</td>
<td>201,125</td>
</tr>
<tr>
<td>4</td>
<td>12,239</td>
<td>150,219</td>
<td>11,037</td>
<td>135,465</td>
<td>23,276</td>
<td>285,685</td>
</tr>
<tr>
<td>5</td>
<td>609</td>
<td>46,464</td>
<td>375</td>
<td>28,593</td>
<td>984</td>
<td>75,057</td>
</tr>
</tbody>
</table>

Sub-Total - US Sourced: 1,045,330
Total: 11,871

## SKU Prioritization

<table>
<thead>
<tr>
<th>Product</th>
<th>Conv. Cases (%)</th>
<th>Net Sales (%)</th>
<th>Margin (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>93</td>
<td>96</td>
<td>99</td>
</tr>
<tr>
<td>B</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>C</td>
<td>55</td>
<td>60</td>
<td>63</td>
</tr>
<tr>
<td>D</td>
<td>86</td>
<td>89</td>
<td>91</td>
</tr>
<tr>
<td>E</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>F</td>
<td>64</td>
<td>81</td>
<td>88</td>
</tr>
<tr>
<td>G</td>
<td>79</td>
<td>83</td>
<td>88</td>
</tr>
<tr>
<td>H</td>
<td>81</td>
<td>90</td>
<td>100</td>
</tr>
<tr>
<td>I</td>
<td>96</td>
<td>94</td>
<td>97</td>
</tr>
<tr>
<td>J</td>
<td>49</td>
<td>47</td>
<td>49</td>
</tr>
<tr>
<td>K</td>
<td>70</td>
<td>72</td>
<td>76</td>
</tr>
</tbody>
</table>

## Customer Prioritization

<table>
<thead>
<tr>
<th>Customer</th>
<th>% Sales</th>
<th>% Margin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>20</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>18</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>30</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>12</td>
</tr>
</tbody>
</table>
**Pre-Loss Strategies**

**Increase Product Inventory**
- Is there existing excess storage capacity anywhere?
- Is it possible to obtain additional storage space?
- Does the product have a limited shelf life?
- What is the potential loss if excess capacity is wasted?
- How much excess inventory and storage space would be needed to provide sufficient impact?

**Contractual Risk Mitigation**
- Do contracts regularly have Force Majeure clauses?
- What impact on sales, price, customer relationship, etc. would using this strategy have?
- Are contractual terms legally sound and defensible?

**Insurance**
- What is the existing business insurance (BI) insurance cover?
- What are the limits of coverage?
- What are the options and costs to increase or decrease the cover?
- What effect will relying on insurance have on customer relationships, product placement, long-term survivability?
- Are there insurance premium savings to offset costs to improve resilience?

Preparatory strategies may fill gaps of execution strategies, change the acceptable level of recovery, or be the only possible strategy.

**Evaluating Recovery Strategies**

<table>
<thead>
<tr>
<th>Strategy Option</th>
<th>Execution Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use existing inventory/stock in transit</td>
<td>Is there existing inventory in a warehouse, in transit, or anywhere else?</td>
</tr>
<tr>
<td>Shift production within site or company or sub-contract manufacturer</td>
<td>Is it possible to manufacture the product at another location, either internal or at a third party?</td>
</tr>
<tr>
<td>Increase manufacturing output</td>
<td>Is there a substitute product available?</td>
</tr>
<tr>
<td>Product reallocation (customer prioritization)</td>
<td>Can customers be prioritized; deliveries suspended?</td>
</tr>
<tr>
<td>Limit order quantity</td>
<td>Can the allowable quantity that a customer can order be limited?</td>
</tr>
<tr>
<td>Reduce unit quantity</td>
<td>Can order quantity of product be reduced so that reduced orders can be filled?</td>
</tr>
<tr>
<td>Suspension or discontinuation (consider product lifecycle)</td>
<td>Are any products at the end of their lifecycle?</td>
</tr>
<tr>
<td>Make a customer strategic partner</td>
<td>Is it possible to purchase the product anywhere?</td>
</tr>
<tr>
<td>Repurchase/buy back product</td>
<td>Can your relationship with your customers allow you to partner with them?</td>
</tr>
</tbody>
</table>

Negative Answers Eliminate Strategies

**Evaluating Recovery Strategies**

- Cash costs and opportunity costs
- Proximity issues
- Capacity issues
- Quality issues (customer satisfaction/acceptance)
- Product packaging issues
- Product capability issues
- Availability/reliability
- Longer term consequences of decision
- Regulatory issues
**Strategy Cost/Benefit Analysis**

![Diagram showing cost vs. recovery time for different recovery options: Internal Recovery, Commercial Hot Site, Warm Site, Cold Site, No Recovery Strategy.]

**Business Continuity Plan**

- **Scope, objectives and assumptions**
- **Incident detection and reporting**
- **Alerting and notifications**
  - Business continuity team
  - IT disaster recovery team
  - Management
  - Contractors and vendors
- **Incident management**
  - Plan activation
  - Emergency operations center activation
  - Damage assessment (coordination with emergency plan); situation analysis
  - Development and approval of an incident action plan
- **Plan execution**
  - Recovery strategies and alternate site locations for business operations and technology that meet the RTO and RPO set by the Business Impact Analysis
  - Detailed procedures for continuation or resumption of business processes
  - Detailed procedures for the recovery of technology
- **Roles and responsibilities**
  - Human resource management and support
  - Financial management and support
  - Crisis Communication plan—communications with stakeholders

**Scope Statement**

- **Sets the boundaries for the plan**
- **Clarifies what is included and excluded:**
  - "The scope of the plan covers all units located in location X only."
  - "Plans do not include restoration of the location X facility."
**Objectives**

**Plan Objectives**
- “To maintain client services and customer relations.”
- “To minimize the impacts of an incident by executing strategies to sustain minimum levels of critical functions.”
- “To satisfy legal and regulatory requirements.”

**Recovery Objectives**
- Satisfy client commitments
- Maintain reputation
- Sustain revenue
- Maintain cash flow
- Maintain financial controls
- Maintain staff commitment
- Reducing operational risk
- Satisfy regulatory requirements

**Plan Assumptions**
- An assumption is “something that is taken for granted or advanced as fact.” Examples:
  - “The recovery facility will not be affected by the same disaster as the one that strikes location X.”
  - “The plan assumes that loss or unavailability of personnel will not significantly impact execution of the plan.”
  - “Total duration of an outage will be no more than X weeks.”
  - “All Recovery Plans will be securely stored and immediately accessible at their respective recovery sites.”

**Auditing the Business Continuity Plan**

**Interviews/Surveys**
- Interviews
  - Senior leadership (strategy selection)
  - Program Coordinator
  - BCP Steering Committee
  - IT Disaster Recovery Team Leader
  - Function/business unit planners
- Surveys
  - Business operations
  - Emergency Operations Center
  - Recovery site(s)
  - Alternate workspace

**Evidence of Conformity**
- Management has approved recovery strategies
- Recovery strategies can achieve RTOs
- Required resources are available to achieve RTOs
- Team leaders demonstrate knowledge of plans and incident management
- Team members are knowledgeable about their responsibilities
- Secure copies of business continuity plans are available at or accessible from the EOC and recovery site(s)
Auditing the Business Continuity Plan

Documents to Review
- Business Impact Analysis (BIA) report
- Business Continuity Plan(s)
  - Plan activation, escalation, incident management procedures
  - Relocation strategy and procedures
  - Recovery strategies
  - Manual workarounds
  - Plan maintenance schedule
- IT Disaster Recovery Plan(s)
  - Technology recovery (infrastructure, connectivity, hardware, applications)
  - Data backup methods, schedules, and location
  - Data restoration
- Resource Requirements
  - Resource inventory
  - GAP analysis
  - Reciprocal/mutual aid agreements
  - Contracts for alternate workspace, equipment, and services
  - Testing and Exercises

Evidence of Conformity
- Recovery strategies have been designed to recover critical functions identified by BIA within RTOs:
  - Business functions and processes
  - Critical and time-sensitive applications
  - Alternative work sites
  - Vital records and information
- Stakeholder communications addressed

6.1 Common Plan Requirements
6.1.1* Plans shall address the health and safety of personnel.
6.1.2 Plans shall identify and document the following:
  (1) Assumptions made during the planning process
  (2) Functional roles and responsibilities of internal and external agencies, organizations, departments, and positions
  (3) Lines of authority
  (4) The process for delegation of authority
  (5) Lines of succession for the entity
  (6) Liaisons to external entities
  (7) Logistics support and resource requirements
6.1.3* Plans shall be individual, integrated into a single plan document, or a combination of the two.
6.1.4* The entity shall make sections of the plans available to those assigned specific tasks and responsibilities therein and to key stakeholders as required.
Discussion

1. Describe the steps in the "Business Continuity Planning Process".
2. Discuss the relationship between cost of recovery strategies and recovery window?
3. Describe the following technology strategies:
   a. Hot Site
   b. Warm Site
   c. Cold Site
6.4 Crisis Communications & Public Information

6.4.1* The entity shall develop a plan and procedures to disseminate information to and respond to requests for information from the following audiences before, during, and after an incident:

1. Internal audiences, including employees
2. External audiences, including the media, functional needs populations, and other stakeholders

6.4.2* The entity shall establish and maintain a crisis communications or public information capability that includes the following:

1. Central contact facility or communications hub
2. Physical or virtual information center
3. System for gathering, monitoring, and disseminating information
4. Procedures for developing and delivering coordinated messages
5. Protocol to clear information for release

6.5 Warning, Notifications, and Communications

6.5.1* The entity shall determine its warning, notification, and communications needs.
6.5.2* Warning, notification, and communications systems shall be reliable, redundant, and interoperable.
6.5.3* Emergency warning, notification, and communications protocols and procedures shall be developed, tested, and used to alert stakeholders potentially at risk from an actual or impending incident.
6.5.4 Procedures shall include issuing warnings through authorized agencies if required by law as well as the use of prescribed information bulletins or templates.
Challenges & Pitfalls

- How an entity communicates has a direct impact on how the public, employees, and other “stakeholders,” perceive the organization’s handling of the situation.
- If the entity slow to explain what happened, rumors and speculation will flourish—the public may perceive the situation was handled badly.
- Conversely, organizations that communicate quickly and openly about a situation are often perceived more positively.
- The public expects an organization to begin communicating effectively within minutes of an incident.

Coordination of Information

- Information flow is bi-directional—collection and dissemination
- Must be a central process to collect information about the incident and coordinate the outflow of information to stakeholders.
- Capability to collect inquiries and analyze those inquiries to help forecast emerging issues and the likely information needs of stakeholders.
- Pre-scripted communications should be developed for each audience so they can understand “what it means for me” and “what the organization is doing about it.”

Move from Reactive to Strategic

- Quickly move away from responding to requests for information
- Provide information that protects the public and the organization
- Communicate more proactively—deliver positive messages to key audiences
- Assign resources to develop a communications strategy
Crisis Communications Plan

- Disseminate and respond to requests for:
  - Pre-incident
  - Incident
  - Post-incident information
- to and from the following:
  - Internal audiences, including employees
  - External audiences, including the media and special needs populations

Scalable Communications Structure

- **Limited incident** with no outside attention:
  - One person posting emails or updating company intranet
- **Major incident** that draws international attention:
  - Spokespersons for on-camera requests and press conferences
  - Writers drafting statements and developing frequently asked questions for the website and call center
  - Telephone operators to staff the call center
  - Media monitors monitoring the media or coordinating with outsourced media monitors
  - Team coordinating employee statements
  - Website team updates the intranet
  - Human Resources team contacts victim families
  - Labor Relations team keeps labor union updated

Crisis Communications

- A central contact facility
- Pre-scripted information bulletins
- A method to coordinate information for release
- Protective action guidelines
- Procedures to advise the public of threats
Communications with Stakeholders

- Neighbors next door
- Special needs population
- Emergency services
- Community at large
- Employees
- Victims and their families
- Regulatory bodies
- News media
- Customers
- Company management/Board of Directors
- Government authorities
- Investment community
- Activist groups
- Vendors

Audit the crisis communications plan to see who is assigned to speak with each stakeholder.

Evaluate how the entity will ensure that the information given to each group is accurate and consistent with information disseminated to others.

Pre-Incident Communications

- Community relations builds public understanding of a company’s values, capabilities and risks
- The more obvious the risks associated with company operations, the greater the need for risk communications
- When the community feels threatened:
  - Establish a two-way dialog
  - Identify their fears, concerns and information needs
  - Fulfill those needs to their satisfaction
  - Monitor community and media reaction
  - Address new questions and concerns as they arise
  - Meet with the community in smaller groups
- Community relations includes:
  - Response planning
  - Risk communications
  - Community outreach efforts during and after an incident

Auditing the Crisis Communications Plan

Interviews/Surveys/Documents

- Interviews
  - Senior management
  - Public affairs/relations/Corporate communications
  - Program coordinator
  - Team leaders (ER/BCP)
  - Public relations firm on call
- Surveys
  - Communications facility
- Documents
  - Crisis management plan
  - Crisis communications plan
  - Product recall plan
  - Public relations plan

Evidence of Conformity

- Central contact facility
- Scalable communications organization
- Pre-scripted bulletins matched to risk assessment
- List of internal and external audiences and who will contact them
- Protocols and procedures for coordination flow of information and clearing for release
- Protocols and procedures for warning: coordination with public officials as required
Discussion

1. What is Crisis Communications?
2. In a command center organized around the ICS, who is responsible for:
   • Developing messages for the media?
   • Communicating with external organizations?
   • Final approval for all messages?
6.10* Employee Assistance & Support

6.10.1* The entity shall develop a strategy for employee assistance and support to include the following:

1. **Communications procedures**
2. **Contact information**, including emergency contact outside anticipated hazard area
3. **Accounting for persons** affected, displaced, or injured by the incident
4. Temporary, short-term, or long-term housing, and feeding and care of those displaced by an incident
5. **Mental health and physical well-being** of individuals affected by the incident
6. **Pre-incident and post-incident awareness**

6.10.2 The strategy shall be flexible for use in all incidents.

6.10.3* The entity shall promote family preparedness education and training for employees.

**Communications & Accounting**

- **Communications capability** (to/from home & work)
  - Landline and cellular telephone
  - Electronic mail
  - Text
  - Voice messaging
  - Call center
- **Contact list**
- **System to account for personnel**
Employee & Family Assistance

- **Situation Analysis**
  - Personnel accounting
  - Human impact assessment
  - Resource needs assessment

- **Family Assistance**
  - Communications
  - Call center
  - Family assistance center
  - Liaisons to families
  - Claims and benefits administration

- **Trauma response**
  - Medical & psychological

Auditing Employee Assistance & Support

**Interviews/Surveys/Documents**

- Interviews
  - Human Resources
  - Crisis Communications
  - Information Technology

- Documents
  - Employee Assistance Plan (aka human impact plan)
  - Up to date employee lists with work, home, and emergency contact information
  - Protocols and procedures for communications

**Evidence of Conformity**

- Documented policies, protocols, and procedures
- Communications capability with up to date contacts
- Accounting system
- Arrangements with professional services to provide health care and mental health services
- Plan for logistics
- Employee awareness program

Employee & Family Assistance

Interviews/Surveys/Documents

- Interviews
  - Human Resources
  - Crisis Communications
  - Information Technology

- Documents
  - Employee Assistance Plan (aka human impact plan)
  - Up to date employee lists with work, home, and emergency contact information
  - Protocols and procedures for communications

Auditing Employee Assistance & Support

**Interviews/Surveys/Documents**

- Interviews
  - Human Resources
  - Crisis Communications
  - Information Technology

- Documents
  - Employee Assistance Plan (aka human impact plan)
  - Up to date employee lists with work, home, and emergency contact information
  - Protocols and procedures for communications

**Evidence of Conformity**

- Documented policies, protocols, and procedures
- Communications capability with up to date contacts
- Accounting system
- Arrangements with professional services to provide health care and mental health services
- Plan for logistics
- Employee awareness program
7. Training & Education

7.1 Curriculum. The entity shall develop and implement a competency-based training and education curriculum that supports all employees who have a role in the program.

7.2 Goal of Curriculum. The goal of the curriculum shall be to create awareness and enhance the knowledge, skills, and abilities required to implement, support, and maintain the program.

7.3 Scope and Frequency of Instruction. The scope of the curriculum and the frequency of instruction shall be identified.

7.4 Incident Management System Training. Personnel shall be trained in the entity’s incident management system (IMS) and other components of the program to the level of their involvement.

7.5 Recordkeeping. Records of training and education shall be maintained as specified in Section 4.7.

7.6 Regulatory and Program Requirements. The curriculum shall comply with applicable regulatory and program requirements.

7.7 Public Education. A public education program shall be implemented to communicate the following:

1. The potential impact of a hazard
2. Preparedness information
3. Information needed to develop a preparedness plan

Training and Education Curriculum

Establish and maintain an ability to execute the disaster/emergency management program. Curriculum identifies the “what”—the “courses” or subject areas. The standard and regulations define:

- Who needs training
- When—the frequency of training
### Incident Management System

- Basic concepts of the incident command system
- Incident command—passing of command to higher authority
- Unification of command between private and public sectors
- How the ICS structure expands or contracts to meet the needs of an incident
- Position within the ICS structure, reporting relationships, and responsibilities
- Incident command post operations
- Incident briefing and incident action planning
- Resource needs for managing an incident
- Communications protocols and procedures
- Communications with media and stakeholders
- Criteria and procedures for activation of the emergency operations center and the roles and responsibilities of persons operating within the EOC

### Senior Management

- Role in the program
- Crisis management and communications plans and procedures
- Concept of operations for incident management
- Coordination with division, business unit, and site plans and teams
- Media relations
**All Employees**

- Environmental, health, and safety policies, procedures, and acceptable practices; including hazards of materials and processes to which they are exposed
- Policies, procedures, and practices for physical and information (cyber) security
- Vital records identification and protection
- Protective actions for life safety (e.g., evacuation, shelter-in-place, and lockdown)
  - Understand the emergency alarm system
  - Identifying occupants who need special assistance with evacuation
  - Location of primary and secondary exits
  - Location of assembly areas and procedures for accounting for all employees
- Understand the emergency alarm system
- Identifying occupants who need special assistance with evacuation
- Location of primary and secondary exits
- Location of assembly areas and procedures for accounting for all employees

**All Employees**

- Emergency response procedures related to the hazards they may encounter in the workplace (e.g., reporting an emergency, medical emergency, bomb threat, chemical spill, suspicious package, etc.)
- Evacuation drills at least annually, more frequently if local fire prevention or homeland security codes require
- Awareness of the business continuity plan
- Crisis communications—authorized spokesperson(s)
- Employee assistance and support

**Emergency Organization**

- Train members of emergency response teams in accordance with their duties and applicable regulations and standards.
- Evacuation team
  - Evacuation of the building
  - Assembly area supervision
  - Accounting of evacuees
- Fire: commensurate with duties and functions members will perform (e.g., use of fire extinguishers, or as fire brigade member)
- Hazardous Materials:
  - Hazmat team training (NFPA 471, 472 and OSHA 1910.120)
  - Employees need training in hazards and compatibility of chemicals and procedures for fire, leak, or spill (Hazard Communication)
- Medical: certify first responders to provide first aid, CPR/AED and universal precautions to prevent exposure to bloodborne pathogens
- Rescue: train confined space entrants in emergency procedures and rescuers as authorized entrants
- Facilities: Operation, shutdown of building communications, warning, utility (shelter-in-place), and process systems
Regulations: Which are applicable?

- OSHA 1910.120, “HAZWOPER” Hazardous Waste Operations and Emergency Response
- OSHA 1910.146, Permit-Required Confined Spaces
- OSHA 1910. Subpart K - Medical & First Aid
- OSHA 1910. Subpart L - Fire Protection
- OSHA 1910.1200, Hazard Communication
- Environmental regulations (state and U.S. EPA)
- Local, county, or state codes, “homeland security” regulations

Regulations: Which are applicable?

- NFPA 1, Fire Code or International Fire Code
- NFPA 472, Responders to Hazardous Materials Incidents
- NFPA 600, Standard on Industrial Fire Brigades
- NFPA 601, Standard for Security Services in Fire Loss Prevention
- NFPA 1006, Rescue Technician Professional Qualifications
- NFPA 1081, Fire Brigade Member Professional Qualifications
- NFPA 1670, Training for Technical Search and Rescue Incidents,
- Industry regulations, standards, accreditation requirements, and industry practices
- Business continuity professional practices (DRI)

Business Continuity & IT Team

- Damage assessment
- Declaration of an incident
- Plan activation and escalation
- Alerting
- EOC activation
- Business/technology relocation
- Business/technology recovery strategies
- Data restoration
- Return to “normal” operations
**Crisis Communications Team**

**Subject Areas**
- Crisis communications plan and their roles and responsibilities
- Public awareness (if there are off-site consequences of hazards on-site)
- Communicating with:
  - Customers
  - Community
  - News media
  - Regulators
  - Employees and families
  - Other stakeholders

**Who**
- Media spokespersons
- Community relations
- Call center operators
- Human resources
- Others assigned to communicate with stakeholders

**Auditing Training & Education**

**Interviews/Surveys/Documents**
- Interviews
  - Sample of team members
  - Interview selected employees
  - Trainers
- Documents
  - Training required by EHS, security, other programs
  - Training records
  - Records/evaluations of drills and exercises
  - Certification records (e.g., CPR, CBCP, etc.)
  - Applicable regulations

**Evidence of Conformity**
- Demonstrated knowledge of program policies, procedures, and practices
- Identification of regulations and means to track completion of required training
- Training in incident management system
- Public awareness training (if public at risk)
Testing and Exercises

8.1 Program Evaluation
8.1.1 The entity shall evaluate program plans, procedures, training, and capabilities and promote continuous improvement.
8.1.2 The entity shall evaluate the program based on post-incident analyses, lessons learned, and operational performance in accordance with Chapter 9.
8.1.3 Exercises and tests shall be documented.

8.2 Exercise and Test Methodology
8.2.1 Exercises shall provide a standardized methodology to practice procedures and interact with other entities (internal and external) in a controlled setting.
8.2.2 Exercises shall be designed to assess the maturity of program plans, procedures, and strategies.
8.2.3 Tests shall be designed to demonstrate capabilities.

8.3 Design of Exercises and Tests.
Exercises shall be designed to do the following:
(1) Ensure the safety of people, property, operations, and the environment involved in the exercise or test
(2) Evaluate the program
(3) Identify planning and procedural deficiencies
(4) Test or validate recently changed procedures or plans
(5) Clarify roles and responsibilities
(6) Obtain participant feedback and recommendations for program improvement
(7) Measure improvement compared to performance objectives
(8) Improve coordination among internal and external teams, organizations, and entities
(9) Validate training and education
(10) Increase awareness and understanding of hazards and the potential impact of hazards on the entity
(11) Identify additional resources and assess the capabilities of existing resources, including personnel and equipment needed for effective response and recovery
(12) Assess the ability of the team to identify, assess, and manage an incident
(13) Practice the deployment of teams and resources to manage an incident
(14) Improve individual performance
Goals of Testing and Exercises

- Train personnel; clarify roles and responsibilities
- Reinforce knowledge of procedures, facilities, systems, and equipment
- Improve individual performance as well as organizational coordination and communications
- Evaluate policies, plans, procedures, and the knowledge and skills of team members
- Reveal weaknesses and resource gaps
- Comply with local laws, codes, and standards
- Gain recognition for the emergency management and business continuity program

Test Categories

- **Element** - exercises a single part of a plan; e.g., contact clients with recovery status.
- **Segment** - tests a full segment of the plan; e.g., A/P application, call center transfer, etc.
- **Process** - tests the integration of plans supporting a process; e.g. Full billing cycle - systems restoration, user input, create bills, fold & stuff envelopes, send to mail facility.

Test Schedule

<table>
<thead>
<tr>
<th>Business Unit Name</th>
<th>Process Name</th>
<th>Contact Name</th>
<th>Contact Telephone</th>
<th>Test Category</th>
<th>Test Type</th>
<th>Description</th>
<th>Scheduled Date</th>
<th>Actual Date</th>
<th>Objective Met (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Element</td>
<td>Mobilization</td>
<td>Call team members to confirm phone numbers</td>
<td>January 12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Segment</td>
<td>Mobilization</td>
<td>Recovery team members report to recovery site</td>
<td>January 20</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Process</td>
<td>Tabletop</td>
<td>Billing Cycle</td>
<td>January 29, 1:00 to 3:00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Test schedule should be determined based on program needs and regulations
- Tests should be designed to test new or changed procedures
- Tests should be designed and conducted to validate IT disaster recovery plans, procedures, scripts, and hardware/software compatibility
**Types of Exercises**

- Walkthroughs, workshops or orientation seminars
- Tabletop exercises
- Functional exercises
- Full-scale exercises

Post-incident critiques often find that experience gained during recent exercises is the single most dependable predictor of the ability to respond effectively to an emergency.

---

**Exercise Design Process**

1. Review Plan
2. Needs Assessment
3. Assess Capabilities
4. Exercise Scope
5. Purpose Statement
6. Develop Schedule
7. Send Exercise Directive
8. Organize Design Team
9. Organize Evaluation Team
10. Prepare Objectives
11. Write Messages
12. Finalize Exercise Enhancements
13. Develop Evaluation Format
14. Conduct Exercise
15. Conduct “Hot Wash”
16. Write “After Action Report”
17. Conduct Follow-Up Activities

---

**8.4 Exercise and Test Evaluation**

8.4.1 Exercises shall evaluate program plans, procedures, training, and capabilities to identify opportunities for improvement.

8.4.2 Tests shall be evaluated as either pass or fail.

8.4.3 Exercise and Test Methodology

8.2.1 Exercises shall provide a standardized methodology to practice procedures and interact with other entities (internal and external) in a controlled setting.

8.2.2 Exercises shall be designed to assess the maturity of program plans, procedures, and strategies.

8.2.3 Tests shall be designed to demonstrate capabilities.
Exercise Evaluation & Reporting

- Was a formal after-action review with the team members conducted?
  - Compare test results with test objectives
  - Note discrepancies
  - Document action items and due dates
- Were exercise results and action items documented and reported to Senior Management?
- Were on action items followed up till complete?
- Was program documentation updated as needed?
Discussion

1. What is a Tabletop exercise?
2. What is a Walkthrough exercise?
3. Describe the “Exercise Design Process”.
4. How frequently should test and exercises be conducted?
Program Improvement
Disaster/Emergency Management & Business Continuity Auditor Training

9.1* Program Reviews

9.1.1 The entity shall improve effectiveness of the program through evaluation of the implementation of changes resulting from preventive and corrective action.

9.1.2 Evaluations shall be conducted on a regularly scheduled basis and when the situation changes to challenge the effectiveness of the existing program.

9.1.3 The program shall be re-evaluated when a change in any of the following impacts the entity’s program:
   (1) Regulations
   (2) Hazards and potential impacts
   (3) Resource availability or capability
   (4) Entity’s organization
   (5) Funding changes
   (6) Infrastructure, including technology environment
   (7) Economic and geographic stability
   (8) Entity operations

9.1.4 Reviews shall include post-incident analyses, reviews of lessons learned, and reviews of program performance.

9.1.5 The entity shall maintain records of its reviews and evaluations. In accordance with the records management practices developed under Section 4.7.

9.1.6 Documentation, records, and reports shall be provided to management for review and follow-up.

Program Maintenance Schedule

<table>
<thead>
<tr>
<th>BCP Components</th>
<th>Quarterly</th>
<th>Semi-Annually</th>
<th>Annually</th>
<th>Unscheduled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Management</td>
<td>Requested and approved by Steering Committee</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
</tr>
<tr>
<td>Application Management</td>
<td>Requested and approved by Steering Committee</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
</tr>
<tr>
<td>Telecommunication</td>
<td>Requested and approved by Steering Committee</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
</tr>
<tr>
<td>IT Reliability</td>
<td>Requested and approved by Steering Committee</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
</tr>
<tr>
<td>Test Records</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
</tr>
<tr>
<td>Telephone Setup</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
</tr>
<tr>
<td>Net Reliability</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
<td>Requested, but for non-BP changing events</td>
</tr>
</tbody>
</table>
### Program Reviews

- Regularly scheduled evaluation of plans, procedures, and capabilities through periodic reviews, testing, and exercises
- Performance evaluations
- Conducted if there is a trigger (see 8.1.3)
- Post-incident analyses
- Lessons learned

### Triggers for Program Review

- Regulatory changes
- New or changed processes
- New hazards identified; vulnerability to hazards changes
- Tests, drills, or exercises identify weaknesses
- Post incident critiques identify issues
- Funding or budget level changes
- New product or service launched or withdrawn
- Company, division, or business unit acquired, integrated, or divested
- Significant changes to critical suppliers or supply chain
- Significant increase in the workforce population on-site
- Significant changes to site, buildings, or layouts
- Changes to surrounding infrastructure

### Post Incident Critiques

- Formal critique should have been completed for all incidents involving personal injury, property damage, interruption to operations, or contamination of the environment
- Incident Commander is responsible for initiation of the formal critique process, preparing a summary report, and ensuring that all involved in the incident receive a copy of the summary
- Have items resulting from the critique been acted on:
  - Address deficiencies in teams, plans, and procedures
  - Further implement or coordinate plans and procedures among organizations, departments, agencies, or teams
  - Upgrade the capabilities of resources including personnel, systems, and equipment for prevention, mitigation, response, and recovery
Lessons Learned

- Provide invaluable information to develop plans, procedures, and training
- Sources
  - Professional journals
  - Speeches and presentations at the meetings of professional societies
  - Federal government
  - Trade associations
  - Internet mailing lists
- Copies to Program Coordinator, Program Committee, ER/BC teams, and management

Auditing Program Reviews

Interviews/Surveys/Documents

- Interviews
  - Program coordinator
  - Team leaders
  - Environmental, health and safety, security
  - Operations and facilities management
  - Information Technology
- Surveys
  - Facility conditions, practices, changes, etc.
- Documents
  - Incident reports and post incident critiques
  - Evaluation reports and action items from training, drills, and exercises
- Prior program reviews or audits; determine if identified deficiencies have been corrected
- Risk assessment; monitoring of existing hazards and identification of new hazards
- Change management; program, process, procedure, equipment, or technology
- Change management; program, process, procedure, equipment, or technology
- Change management; program, process, procedure, equipment, or technology
- Change management; program, process, procedure, equipment, or technology
- Change management; program, process, procedure, equipment, or technology

Evidence of Conformity

- Program has been reviewed annually or more recently if any triggers have occurred
- Reviews compare capabilities to program objectives
- Post-incident critiques conducted; lessons learned disseminated
- Action item taken on identified deficiencies
- Team rosters and contact information are current
- Resource inventory (e.g., systems, equipment, materials, and supplies) including records of inspection, testing, and maintenance
- Communication with senior leaders regarding program status
- Records of reviews maintained

9.2 Corrective Action

9.2.1* The entity shall establish a corrective action process.

9.2.2* The entity shall take corrective action on deficiencies identified.

9.3 Continuous Improvement. The entity shall effect continuous improvement of the program through the use of program reviews and the corrective action process.
Auditing the Corrective Action Program

Interviews/Surveys/Documents
- Interviews
  - Program coordinator
  - Facilities and operations
  - Environmental, health and safety (EHS)
- Surveys
  - Facility (review high priority action items)
- Documents
  - Corrective action process
  - Corrective action logs

Evidence of Conformity
- There is a prioritized corrective action process:
  1. Hazards to health and safety
  2. Hazards and or impacts to property, operations, the environment, or the entity (e.g., reputation or image)
  3. Regulatory compliance
  4. Good practice
- Description of action to correct the identified deficiency
- Responsibility assigned; due date for each item
- Resources needed to correct the problem identified
- Approval for necessary resources solicited from mgmt.
- Outstanding issues tracked
- Management updated regularly
Reporting Audit Findings & Recommendations

Observations: Imminent Hazards
- Hazards or practices that could result in serious injury, property damage, business interruption, or environmental contamination
- Report immediately to senior management
- Promptly follow with formal communication

Closing Conference
- Attendees
  - Senior management
  - Program coordinator(s)
  - Selected audit participants
  - Audit team
- Present preliminary findings
- Identify incomplete or missing information
- Address information gaps or conflicting information
- Confirm reporting requirements

© 2013, National Fire Protection Association and DRI, International, All Rights Reserved
### Report Content

- Entity audited
- Location(s)
- Date(s)
- Audit team
- Entity managers and staff
- Observers
- Executive Summary
- Purpose
- Scope
  - Interviews (names, titles)
  - Surveys (facility name)
  - Documents reviewed
- Criteria
- Limitations
- Statement on conformity and or statement on compliance
- Findings
- Recommendations
- Action plan

### Findings & Recommendations

- Corroborate interviews with observations and/or documents
- Connect findings to audit criteria

### Findings & Recommendations

<table>
<thead>
<tr>
<th>Findings</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify the criteria</td>
<td>Regulatory requirement</td>
</tr>
<tr>
<td>Specify the nonconformity and or noncompliance</td>
<td>National standard</td>
</tr>
<tr>
<td>Recommendations</td>
<td>Industry (best) practice</td>
</tr>
<tr>
<td>Identify corrective action</td>
<td>Client specified</td>
</tr>
<tr>
<td></td>
<td>Formal</td>
</tr>
<tr>
<td></td>
<td>Informal</td>
</tr>
</tbody>
</table>

© 2013, National Fire Protection Association and DRI, International, All Rights Reserved

Version 4.0
Ratings

- Non-conforming to audit criteria
- Partially conforming to audit criteria
- Conforms to audit criteria

Example “Traffic Light” Report

Program Management: 80%
- Leadership and Commitment: 80%
- Program Coordinator: 80%
- Program Committee: 80%
- Program Administration: 80%
- Performance Objectives: 80%
- Records Management: 80%
- Planning: 80%
- Planning Process: 80%
- Common Plan Requirements: 80%
- Planning and Design: 80%
- Risk Assessment: 80%
- Business Impact Analysis: 80%
- Prevention: 80%
- Mitigation: 80%

Leadership and Commitment: 50%
- Program Coordinator: 50%
- Program Committee: 50%
- Program Administration: 50%
- Performance Objectives: 50%
- Records Management: 50%
- Planning: 50%
- Planning Process: 50%
- Common Plan Requirements: 50%
- Planning and Design: 50%
- Risk Assessment: 50%
- Business Impact Analysis: 50%
- Prevention: 50%
- Mitigation: 50%

Program Coordinator: 30%
- Program Coordinator: 30%
- Program Committee: 30%
- Program Administration: 30%
- Performance Objectives: 30%
- Records Management: 30%
- Planning: 30%
- Planning Process: 30%
- Common Plan Requirements: 30%
- Planning and Design: 30%
- Risk Assessment: 30%
- Business Impact Analysis: 30%
- Prevention: 30%
- Mitigation: 30%

Implementation: 80%
- Resource Management: 80%
- Mental Health: 80%
- Communications and Warning: 80%
- Operational Procedures: 80%
- Emergency Response: 80%
- Employee Assistance and Support: 80%
- Business Continuity and Recovery: 80%
- Crisis Communications and Public Information: 80%
- Incident Management: 80%
- Emergency Operations Centers (EOCs): 80%
- Training and Education: 80%
- Testing and Exercises: 80%
- Program Improvement: 80%
- Program Reviews: 80%
- Corrective Action: 80%

What is your opinion of this program?

Prioritization of Recommendations

- High
- Medium
- Low
- Custom
Quality of Communications

- Accurate
- Objective
- Clear
- Concise
- Complete
- Timely

Did I Answer Your Questions?

Congratulations