AUGUST BROWN
BUSINESS CONTINUITY PLAN & TEST POLICY

Business Continuity Plan

Business Continuity Planning Process Diagram

When business is disrupted, it can cost money. Lost revenues plus extra expenses means reduced profits. Insurance does not cover all costs and cannot replace customers that defect to the competition. A business continuity plan to continue business is essential. Development of a business continuity plan includes four steps:

- Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.
- Identify, document, and implement to recover critical business functions and processes.
- Organize a business continuity team and compile a business continuity plan to manage a business disruption.
- Conduct training for the business continuity team and testing and exercises to evaluate recovery strategies and the plan.

Information technology (IT) includes many components such as networks, servers, desktop and laptop computers and wireless devices. The ability to run both office productivity and enterprise software is critical. Therefore, recovery strategies for information technology should be developed so technology can be restored in time to meet the needs of the business. Manual workarounds should be part of the IT plan so business can continue while computer systems are being restored.

Resources for Business Continuity Planning

- Standard on Disaster/Emergency Management and Business Continuity Programs - National Fire Protection Association (NFPA) 1600
- Professional Practices for Business Continuity Professionals - DRI International (non-profit business continuity education and certification body)
- Continuity Guidance Circular - Federal Emergency Management Agency
- Open for Business® Toolkit - Institute for Business & Home Safety

Business Continuity Impact Analysis

Business continuity impact analysis identifies the effects resulting from disruption of business functions and processes. It also uses information to make decisions about recovery priorities and strategies.

The Operational & Financial Impacts worksheet can be used to capture this information as discussed in Business Impact Analysis. The worksheet should be completed by business function and process managers with sufficient knowledge of the business. Once all worksheets are completed, the worksheets can be tabulated to summarize:

- the operational and financial impacts resulting from the loss of individual business functions and process
- the point in time when loss of a function or process would result in the identified business impacts

Those functions or processes with the highest potential operational and financial impacts become priorities for restoration. The point in time when a function or process must be recovered, before unacceptable consequences could occur, is often referred to as the "Recovery Time Objective."

Resource Required to Support Recovery Strategies

Recovery of a critical or time-sensitive process requires resources. The Business Continuity Resource Requirements worksheet should be completed by business function and process managers. Completed worksheets are used to determine the resource requirements for recovery strategies.

Following an incident that disrupts business operations, resources will be needed to carry out recovery strategies and to restore normal business operations. Resources can come from within the business or be provided by third parties. Resources include:

- Employees
- Office space, furniture and equipment
- Technology (computers, peripherals, communication equipment, software and data)
- Vital records (electronic and hard copy)
- Production facilities, machinery and equipment
- Inventory including raw materials, finished goods and goods in production.

- Utilities (power, natural gas, water, sewer, telephone, internet, wireless)
- Third party services

Since all resources cannot be replaced immediately following a loss, managers should estimate the resources that will be needed in the hours, days and weeks following an incident.

Conducting the Business Continuity Impact Analysis

The worksheets Operational and Financial Impacts and Business Continuity Resource Requirements should be distributed to business process managers along with instructions about the process and how the information will be used. After all managers have completed their worksheets, information should be reviewed. Gaps or inconsistencies should be identified. Meetings with individual managers should be held to clarify information and obtain missing information.

After all worksheets have been completed and validated, the priorities for restoration of business processes should be identified. Primary and dependent resource requirements should also be identified. This information will be used to develop recovery strategies.

Recovery Strategies

If a facility is damaged, production machinery breaks down, a supplier fails to deliver or information technology is disrupted, business is impacted and the financial losses can begin to grow. Recovery strategies are alternate means to restore business operations to a minimum acceptable level following a business disruption and are prioritized by the recovery time objectives (RTO) developed during the business impact analysis.

Recovery strategies require resources including people, facilities, equipment, materials and information technology. An analysis of the resources required to execute recovery strategies should be conducted to identify gaps. For example, if a machine fails but other machines are readily available to make up lost production, then there is no resource gap. However, if all machines are lost due to a flood, and insufficient undamaged inventory is available to meet customer demand until production is restored, production might be made up by machines at another facility—whether owned or contracted.

Strategies may involve contracting with third parties, entering into partnership or reciprocal agreements or displacing other activities within the company. Staff with in-depth knowledge of business functions and processes are in the best position to determine what will work. Possible alternatives should be explored and presented to management for approval and to decide how much to spend.

Depending upon the size of the company and resources available, there may be many recovery strategies that can be explored.

Utilization of other owned or controlled facilities performing similar work is one option. Operations may be relocated to an alternate site - assuming both are not impacted by the same incident. This

strategy also assumes that the surviving site has the resources and capacity to assume the work of the impacted site. Prioritization of production or service levels, providing additional staff and resources and other action would be needed if capacity at the second site is inadequate.

Telecommuting is a strategy employed when staff can work from home through remote connectivity. It can be used in combination with other strategies to reduce alternate site requirements. This strategy requires ensuring telecommuters have a suitable home work environment and are equipped with or have access to a computer with required applications and data, peripherals, and a secure broadband connection.

In an emergency, space at another facility can be put to use. Cafeterias, conference rooms and training rooms can be converted to office space or to other uses when needed. Equipping converted space with furnishings, equipment, power, connectivity and other resources would be required to meet the needs of workers.

Partnership or reciprocal agreements can be arranged with other businesses or organizations that can support each other in the event of a disaster. Assuming space is available, issues such as the capacity and connectivity of telecommunications and information technology, protection of privacy and intellectual property, the impacts to each other's operation and allocating expenses must be addressed. Agreements should be negotiated in writing and documented in the business continuity plan. Periodic review of the agreement is needed to determine if there is a change in the ability of each party to support the other.

There are many vendors that support business continuity and information technology recovery strategies. External suppliers can provide a full business environment including office space and live data centers ready to be occupied. Other options include provision of technology equipped office trailers, replacement machinery and other equipment. The availability and cost of these options can be affected when a regional disaster results in competition for these resources.

There are multiple strategies for recovery of manufacturing operations. Many of these strategies include use of existing owned or leased facilities. Manufacturing strategies include:

- Shifting production from one facility to another
- Increasing manufacturing output at operational facilities
- Retooling production from one item to another
- Prioritization of production—by profit margin or customer relationship
- Maintaining higher raw materials or finished goods inventory
- Reallocating existing inventory, repurchase or buyback of inventory
- Limiting orders (e.g., maximum order size or unit quantity)
- Contracting with third parties
- Purchasing business interruption insurance

There are many factors to consider in manufacturing recovery strategies:

- Will a facility be available when needed?

- How much time will it take to shift production from one product to another?
- How much will it cost to shift production from one product to another?
- How much revenue would be lost when displacing other production?
- How much extra time will it take to receive raw materials or ship finished goods to customers? Will the extra time impact customer relationships?
- Are there any regulations that would restrict shifting production?
- What quality issues could arise if production is shifted or outsourced?
- Are there any long-term consequences associated with a strategy?

Resources for Developing Recovery Strategies

- Professional Practices for Business Continuity Professionals - DRI International (non-profit business continuity education and certification body)
- The Telework Coalition (America's leading nonprofit telework education and advocacy organization)

Manual Workarounds

Telephones are ringing and customer service staff is busy talking with customers and keying orders into the computer system. The electronic order entry system checks available inventory, processes payments and routes orders to the distribution center for fulfillment. Suddenly the order entry system goes down. What should the customer service staff do now? If the staff is equipped with paper order forms, order processing can continue until the electronic system comes back up and no phone orders will be lost.

The order forms and procedures for using them are examples of "manual workarounds." These workarounds are recovery strategies for use when information technology resources are not available.

Developing Manual Workarounds

Identify the steps in the automated process - creating a diagram of the process can help. Consider the following aspects of information and workflow:

Internal Interfaces (department, person, activity and resource requirements)

- External Interfaces (company, contact person, activity and resource requirements)
- Tasks (in sequential order)
- Manual intervention points

Create data collection forms to capture information and define processes for manual handling of the information collected. Establish control logs to document transactions and track their progress through the manual system.

Manual workarounds require manual labor, so you may need to reassign staff or bring in temporary assistance.

Business Continuity Planning Suite

Business Impact Analysis

A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment. Operations may also be interrupted by the failure of a supplier of goods or services or delayed deliveries. There are many possible scenarios which should be considered.

The BIA identifies the operational and financial impacts resulting from the disruption of business functions and processes. Impacts to consider include:

- Lost sales and income
- Delayed sales or income
- Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
- Regulatory fines
- Contractual penalties or loss of contractual bonuses
- Customer dissatisfaction or defection
- Delay of new business plans

Timing and Duration of Disruption

The point in time when a business function or process is disrupted can have a significant bearing on the loss sustained. A store damaged in the weeks prior to the holiday shopping season may lose a substantial amount of its yearly sales. A power outage lasting a few minutes would be a minor inconvenience for most businesses but one lasting for hours could result in significant business losses. A short duration disruption of production may be overcome by shipping finished goods from a warehouse but disruption of a product in high demand could have a significant impact.

Conducting the BIA

Use a *BIA questionnaire* to survey managers and others within the business. Survey those with detailed knowledge of how the business manufactures its products or provides its services. Ask them to identify the potential impacts if the business function or process that they are responsible for is interrupted. The BIA also identifies the critical business processes and resources needed for the business to continue to function at different levels.

BIA Report

The BIA report documents the potential impacts resulting from disruption of business functions and processes. Scenarios resulting in significant business interruption should be assessed in terms of financial impact, if possible. These costs should be compared with the costs for possible recovery strategies.

The BIA report prioritizes the order of events for restoration of the business. Business processes with the greatest operational and financial impacts should be restored first.

Business Disruption Scenarios

- Physical damage to a building/building
- Damage to or breakdown of machinery, systems or equipment
- Restricted access to a site or building
- Interruption of the supply chain including failure of a supplier or disruption of transportation of goods from the supplier.
- Utility outage (e.g., electrical power outage)
- Damage to, loss or corruption of information technology including voice and data communications, servers, computers, operating systems, applications, and data
- Absenteeism of essential employees

Training

Training is essential to ensure that everyone knows what to do when there is an emergency, or disruption of business operations. Everyone needs training to become familiar with protective actions for life safety (e.g., evacuation, shelter, shelter-in-place and lockdown). Review protective actions for life safety and conduct evacuation drills ("fire drills") as required by local regulations. Sheltering and lockdown drills should also be conducted. Employees should receive training to become familiar with safety, building security, information security and other loss prevention programs.

Members of emergency response, business continuity and crisis communications teams should be trained so they are familiar with their role and responsibilities as defined within the plans. Team leaders should receive a higher level of training, including incident command system training, so they can lead their teams. Review applicable regulations to determine training requirements. Records documenting the scope of training, participants, instructor and duration should be maintained.

If emergency response team members administer first aid, CPR or use AEDs, they should receive training to obtain and maintain those certifications. If employees use portable fire extinguishers, fire hoses or other firefighting equipment, they should be trained in accordance with the applicable OSHA regulation. If employees respond to hazardous materials spills, they also require training.

Who needs training?	What training should be provided?

All employees	• Protective actions for life safety (evacuation, shelter, shelter-in-place, lockdown) • Safety, security, and loss prevention programs
Emergency Response Team (evacuation, shelter, shelter-in-place)	• Roles and responsibilities as defined in the plan • Training as required to comply with regulations or maintain certifications (if employees administer first aid, CPR or AED or use fire extinguishers or clean up spills of hazardous chemicals) • Additional training for leaders including incident management
Business Continuity Team	• Roles and responsibilities as defined in the plan • Additional training for leaders including incident management
Crisis Communications Team	• Roles and responsibilities as defined in the plan • Additional training for leaders including incident management • Training for spokespersons

Drills and exercises should also be conducted to validate emergency response, business continuity and crisis communications plans and to evaluate the ability of personnel to carry out their assigned roles and responsibilities.

Training Resources

- Training Requirements in OSHA Standards and Training Guidelines - U.S. Occupational Safety & Health Administration
- ICS (Incident Command System) Training Materials and Opportunities - Emergency Management Institute (EMI), Federal Emergency Management Agency (FEMA)
- Building An Information Technology Security Awareness and Training Program - National Institute of Standards and Technology, Special Publication 800-50
- Emergency Management Institute Higher Education Program - DHS, FEMA, EMI
- Business and Industry Crisis Management - DHS, FEMA, EMI
- Continuity of Operations Training – DHS, FEMA, EMI

IT Disaster Recovery Plan

Businesses use information technology to quickly and effectively process information. Employees use electronic mail and Voice Over Internet Protocol (VOIP) telephone systems to communicate. Electronic data interchange (EDI) is used to transmit data including orders and payments from one company to another. Servers process information and store large amounts of data. Desktop computers, laptops and wireless devices are used by employees to create, process, manage and communicate information. What do you when your information technology stops working?

An information technology disaster recovery plan (IT DRP) should be developed in conjunction with the business continuity plan. Priorities and recovery time objectives for information technology should be developed during the business impact analysis. Technology recovery strategies should be developed to restore hardware, applications and data in time to meet the needs of the business recovery.

Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential.

Resources for Information Technology Disaster Recovery Planning

- Computer Security Resource Center - National Institute of Standards and Technology (NIST), Computer Security Division Special Publications
- Contingency Planning Guide for Federal Information Systems - NIST Special Publication 800-34 Rev. 1
- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities – NIST Special Publication 800-84
- Building An Information Technology Security Awareness and Training Program - NIST Special Publication 800-50

IT Recovery Strategies

Recovery strategies should be developed for Information technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity. Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis. IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective for the business function or process that depends on the IT resource.

Information technology systems require hardware, software, data and connectivity. Without one component of the "system," the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- Data and restoration

Some business applications cannot tolerate any downtime. They utilize dual data centers capable of handling all data processing needs, which run in parallel with data mirrored or synchronized between the two centers. This is a very expensive solution that only larger companies can afford. However, there are other solutions available for small to medium sized businesses with critical business applications and data to protect.

Internal Recovery Strategies

Many businesses have access to more than one facility. Hardware at an alternate facility can be configured to run similar hardware and software applications when needed. Assuming data is backed up off-site or data is mirrored between the two sites, data can be restored at the alternate site and processing can continue.

Vendor Supported Recovery Strategies

There are vendors that can provide "hot sites" for IT disaster recovery. These sites are fully configured data centers with commonly used hardware and software products. Subscribers may provide unique equipment or software either at the time of disaster or store it at the hot site ready for use.

Data streams, data security services and applications can be hosted and managed by vendors. This information can be accessed at the primary business site or any alternate site using a web browser. If an outage is detected at the client site by the vendor, the vendor automatically holds data until the client's system is restored. These vendors can also provide data filtering and detection of malware threats, which enhance cyber security.

Developing an IT Disaster Recovery Plan

Businesses should develop an IT disaster recovery plan. It begins by compiling an inventory of hardware (e.g. servers, desktops, laptops and wireless devices), software applications and data. The plan should include a strategy to ensure that all critical information is backed up.

Identify critical software applications and data and the hardware required to run them. Using standardized hardware will help to replicate and reimage new hardware. Ensure that copies of program software are available to enable re-installation on replacement equipment. Prioritize hardware and software restoration.

Document the IT disaster recovery plan as part of the business continuity plan. Test the plan periodically to make sure that it works.

Data Backup

Businesses generate large amounts of data and data files are changing throughout the workday. Data can be lost, corrupted, compromised or stolen through hardware failure, human error, hacking and malware. Loss or corruption of data could result in significant business disruption.

Data backup and recovery should be an integral part of the business continuity plan and information technology disaster recovery plan. Developing a data backup strategy begins with identifying what data to backup, selecting and implementing hardware and software backup procedures, scheduling and conducting backups and periodically validating that data has been accurately backed up.

Developing the Data Backup Plan

Identify data on network servers, desktop computers, laptop computers and wireless devices that needs to be backed up along with other hard copy records and information. The plan should include regularly scheduled backups from wireless devices, laptop computers and desktop computers to a network server. Data on the server can then be backed up. Backing up hard copy vital records can be accomplished by scanning paper records into digital formats and allowing them to be backed up along with other digital data.

Options for Data Backup

Tapes, cartridges and large capacity USB drives with integrated data backup software are effective means for businesses to backup data. The frequency of backups, security of the backups and secure off-site storage should be addressed in the plan. Backups should be stored with the same level of security as the original data.

Many vendors offer online data backup services including storage in the “cloud”. This is a cost-effective solution for businesses with an internet connection. Software installed on the client server or computer is automatically backed up.

Data should be backed up as frequently as necessary to ensure that, if data is lost, it is not unacceptable to the business. The business impact analysis should evaluate the potential for lost data and define the “recovery point objective.” Data restoration times should be confirmed and compared with the IT and business function recovery time objectives.

Business

Preparedness Planning for Your Business

Businesses and their staff face a variety of hazards:

- Natural hazards like floods, hurricanes, tornadoes, and earthquakes.
- Health hazards such as widespread and serious illnesses like the flu.
- Human-caused hazards including accidents and acts of violence.
- Technology-related hazards like power outages and equipment failure.

There is much that a business leader can do to prepare his or her organization for the most likely hazards. The Ready Business program helps business leaders make a preparedness plan to get ready for these hazards.

Ready Business Toolkits

The Ready Business Toolkit series includes hazard-specific versions for earthquake, hurricane, inland flooding, power outage, and severe wind/tornado. Toolkits offer business leaders a step-by-step guide to build preparedness within an organization. Each toolkit contains the following sections:

- Identify Your Risk
- Develop A Plan
- Take Action
- Be Recognized and Inspire Others

Business Emergency Preparedness Social Media Toolkit

The Business Emergency Preparedness Social Media Toolkit has safety and preparedness messages you can share on your social media channels.

- Business Emergency Preparedness Social Media Toolkit

Earthquake "QuakeSmart" Toolkit

Unlike other natural disasters, earthquakes occur without warning and cannot be predicted. Most of the United States is at some risk for earthquakes, not just the West Coast, so it is important that you understand your risk, develop preparedness and mitigation plans, and take action.

- QuakeSmart Ready Business Toolkit
- Spanish Ready Business QuakeSmart Toolkit

Hurricane Toolkit

Many parts of the United States, including Atlantic and Gulf of Mexico coastal areas, Hawaii, parts of the Southwest, Puerto Rico, the Pacific Coast, and the U.S. Virgin Islands and territories in the Pacific may be directly affected by heavy rains, strong winds, wind-driven rain, coastal and inland floods, tornadoes, and coastal storm surges resulting from tropical storms and hurricanes. The Ready Business Hurricane Toolkit helps leaders take action to protect employees, protect customers, and help ensure business continuity as well.

- Hurricane Ready Business Toolkit
- Spanish Hurricane Ready Business Toolkit

Inland Flooding Toolkit

Most of the United States is at some risk for flooding, so it is important that organizations, businesses, and community groups understand the potential impacts.

- Inland Flooding Ready Business Toolkit
- Spanish Ready Business Inland Flooding Toolkit

Power Outage Toolkit

While a Power Outage may not seem as dangerous as a tornado or earthquake, they can still cause damage to homes, businesses and communities. Power Outages cost the U.S. economy $20 billion and $55 billion annually and continue to increase each year (CRS, 2012).

- Power Outage Ready Business Toolkit
- Spanish Ready Business Power Outages Toolkit

Severe Wind/Tornado Toolkit

It is not just in Tornado Alley. Most of the United States is at some risk for severe wind and tornadoes.

- Severe Wind Tornado Ready Business Toolkit
- Spanish Ready Business Severe Wind Tornado Toolkit

Ready Business Workshop "How-To" Guide

This "How-To" guide explains how to plan for and deliver effective Ready Business workshops.

- How-To Ready Business Toolkit

Ready Business Videos

- Ready Business Program Physical Surroundings Video

Last Updated: 09/28/2021

Leaders in Business Community Resilience

Developing resilient communities against all hazards requires leadership from government and business. Preparing the workforce, building safe facilities, investing in supplier relationships, and connecting to the community are all key pillars of true business community resilience—from the boardroom to the storefront.

The path to leadership involves connecting with the right people and resources and committing to action by helping the business community and whole community mitigate the hazards they face and bounce back quickly after an incident. Plus, it can decrease the overall costs of disruptions and disasters.

This page features the basics of this simple, scalable roadmap for businesses of all sizes.

The Leadership Path

The most successful leaders take action in a coordinated and collaborative way.

They integrate into a supportive environment that recognizes effective and actionable best practices and understand what makes a public-private partnerships successful. This in turn enables state and local partnership development and growth, as well as integration into planning, preparedness, and operational activities.

Connecting

The first step to becoming better prepared or becoming a leader is connecting within the community and industry. As the connections to people and resources grow across sectors, trust, aptitude for transparency, and efficiency in developing a preparedness program does too.

Integrating

Planning, Training, Exercises are fundamental to community preparedness. Identifying the challenges facing both government and private sector in these scenarios contributes to mutual understanding and community resilience.

Coordinating

Solving problems together in disruption, disasters, or crisis help the whole community work through adverse situations. Businesses have a unique opportunity in identifying capabilities that can help during emergencies. Government has responsibility to help businesses stay in business. As a result, customers and citizens benefit.

Collaborating

Influencing the community way ahead through mitigation, recovery, and strategies that enable resilience.

Committing

Growing your role as a leader in the community or industry - encouraging others to connect and take action.

This leadership path gives businesses of all sizes a roadmap to follow for building their own all-hazards preparedness and contributes to the resilience of their community or industry as well.

Information Sharing

Decisions need to be made before, during, and after disruption – regardless of magnitude. For businesses – either there is the normal and the not so normal, this is whether there is a local, state, or Federal declaration of emergency or disaster. Everyday nearly 30 million businesses of all sizes are constantly identifying problems, risks, and coping with crisis.

Sharing information helps translate ambiguity into clarity. Sharing is also based on a trusted relationship. Developing this trust within a community or state emergency operations center, state fusion center, business emergency operations center, and other information sharing centers can enable business and government leaders to improve decision-making.

Pillars of Business Preparedness

Whether a Fortune 500 company, a regional manufacturer, or a new online business, preparing employees, evaluating, and mitigating risks to systems, structures, and supply chains, and engaging in communities will make a business more resilient.

Staff
Preparing your employees for the threats and hazards likely to impact their community. By preparing your staff for the threats and hazards likely to impact your business, you can ensure that your people know how to stay safe in a disaster.

Structure & Systems
Taking deliberate actions to evaluate, mitigate, and reduce physical, cyber, and operational risks. A business's physical structures and technology systems are some of its largest investments and need protected.

Suppliers
Working with suppliers to share preparedness knowledge, expect business continuity practice, and build confidence in your supply chain. Securing your supply chain, both locally and globally, is an essential component to improving your business's likelihood to cope with disruptions and survive a disaster.

Service
Engaging with community leaders, emergency managers, planners, and elected officials to support pre-incident preparedness planning. In addition to preparing your organization, it is important to understand your local, tribal, state, and territorial community emergency plans and capabilities.

Focusing on these pillars builds capacity and can yield a competitive advantage benefiting businesses and the communities they serve.

Resources

Resource to build employee preparedness, an adaptive supply chain, resilient structures and internal systems, and community involvement and service are below.

Staff Preparedness

- American Red Cross Ready Rating
- FEMA Mobile App
- Ready Business
- Prepare My Business

Structures and Systems

- Critical Infrastructure Cyber Community C3 Voluntary Program
- Standard for the Design and Construction of Storm Shelters
- FCC Cyberplanner
- NIST Cybersecurity Framework

Strengthen Your Supply Chain

- Insurance Institute for Business and Home Safety EZ-Prep Guide
- National Preparedness Goal
- National Strategy for Global Supply Chain Security

Build a Service-Oriented Business

- State, Tribal and Territorial Emergency Management Agency listings
- St. Bernard Project (SBP) Business Resource Guide and Checklist

Last Updated: 06/24/2021

Program Administration

Program Coordinator

The program coordinator is accountable to management for achieving program objectives. Effective program administration is necessary to coordinate activities, review the program and initiate action to improve the program. The program coordinator is responsible for ensuring that the following are addressed in the program:

- Preparedness policy
- Goals and objectives

- Program scope
- Regulations
- Priorities
- Budget
- Schedule
- Resources
- Program evaluation
- Records management

Program Scope

The scope of the program is determined by multiple factors including type of business, complexity of business operations and information gathered from the risk assessment and business impact analysis. Regulations determine minimum requirements for the program. A business with complex business processes and significant exposure to possible injuries, loss of life, environmental pollution and business disruption would require much more planning than a business with one facility and one product line or service.

Budget

A program budget should be established to create the preparedness plan, provide funds to conduct exercises and tests and conduct periodic reviews and make improvements to the plan as necessary. Funding for preparedness planning improvements and maintenance should be part of the annual budget process.

Program Development Schedule

Make a program development schedule that includes major tasks, assignments and due dates. Organize the program into manageable phases prioritized to achieve goals and objectives. Identify milestones to mark completion of phases of the program. The program coordinator should use the schedule to track the completion of activities and tasks and to identify any slippage in the schedule.

Finance and Administrative Procedures

In addition to a budget, procedures should be established for procuring resources before, during and following an incident. A quick process to authorize funds to procure resources will reduce delays. Procedures that account for labor, materials and other costs associated with a hazard should be established before an incident. Risk management or insurance procedures for notification of insurance agents, brokers or underwriters should be included. Procedures for filing property damage, workers' compensation and liability claims should be referenced in the plan.

Program Reviews

As the program is developed, keep in mind the need for periodic reviews. Use the performance objectives to evaluate whether goals and objectives are being achieved. Identify personnel who can assist with reviews and develop checklists and procedures to conduct periodic reviews.

Records Management

Copies of all editions of plan documents should be kept in accordance with the organization's records management program. Records of committee meetings, training, exercises, evaluations and corrective action should be maintained. Research recordkeeping requirements within applicable regulations to identify additional records to be maintained. This may include records of inspections, testing and maintenance of fire protection, life safety, communications and other systems and equipment.

Last Updated: 06/02/2021

Planning

The planning process should take an "all hazards" approach. There are many different threats or hazards. The probability that a specific hazard will impact your business is hard to determine. That's why it's important to consider many different threats and hazards and the likelihood they will occur.

Strategies for prevention/deterrence and risk mitigation should be developed as part of the planning process. Threats or hazards that are classified as probable and those hazards that could cause injury, property damage, business disruption or environmental impact should be addressed.

In developing an all hazards preparedness plan, potential hazards should be identified, vulnerabilities assessed and potential impacts analyzed. The risk assessment identifies threats or hazards and opportunities for hazard prevention, deterrence, and risk mitigation. It should also identify scenarios to consider for emergency planning. The business impact analysis (BIA) identifies time sensitive or critical processes and the financial and operational impacts resulting from disruption of those business processes. The BIA also gathers information about resources requirements to support the time sensitive or critical business processes.

This information is useful in making informed decisions regarding investments to offset risks and avoid business disruptions.

Implementation

Implementation of the preparedness program includes identifying and assessing resources, writing plans, developing a system to manage incidents and training employees so they can execute plans.

- Resource Management: Resources needed for responding to emergencies, continuing business operations and communicating during and after an incident should be identified and assessed.
- Emergency Response Plan: Plans to protect people, property and the environment should be developed. Plans should include evacuation, sheltering in place and lockdown as well as plans for other types of threats identified during the risk assessment.
- Crisis Communications Plan: A plan should be established to communicate with employees, customers, the news media and stakeholders.
- Business Continuity Plan: A business continuity plan that includes recovery strategies to overcome the disruption of business should be developed.
- Information Technology Plan: A plan to recover computer hardware, connectivity and electronic data to support critical business processes should be developed.
- Employee Assistance & Support: The business preparedness plan should encourage employees and their families to develop family preparedness plans. Plans should also be developed to support the needs of employees following an incident.
- Incident Management: An incident management system is needed to define responsibilities and coordinate activities before, during and following an incident.
- Training: Persons with a defined role in the preparedness program should be trained to do their assigned tasks. All employees should be trained so they can take appropriate protective actions during an emergency.
-

Emergency Response Plan

The actions taken in the initial minutes of an emergency are critical. A prompt warning to employees to evacuate, shelter or lockdown can save lives. A call for help to public emergency services that provides full and accurate information will help the dispatcher send the right responders and equipment. An employee trained to administer first aid or perform CPR can be lifesaving. Action by employees with knowledge of building and process systems can help control a leak and minimize damage to the facility and the environment.

The first step when developing an emergency response plan is to conduct a risk assessment to identify potential emergency scenarios. An understanding of what can happen will enable you to determine resource requirements and to develop plans and procedures to prepare your business. The emergency plan should be consistent with your performance objectives.

At the very least, every facility should develop and implement an emergency plan for protecting employees, visitors, contractors and anyone else in the facility. This part of the emergency plan is called “protective actions for life safety” and includes building evacuation (“fire drills”), sheltering from severe weather such as tornadoes, “shelter-in-place” from an exterior airborne hazard such as a chemical release and lockdown. Lockdown is protective action when faced with an act of violence.

When an emergency occurs, the first priority is always life safety. The second priority is the stabilization of the incident. There are many actions that can be taken to stabilize an incident and minimize potential damage. First aid and CPR by trained employees can save lives. Use of fire extinguishers by trained employees can extinguish a small fire. Containment of a small chemical spill

and supervision of building utilities and systems can minimize damage to a building and help prevent environmental damage.

Some severe weather events can be forecast hours before they arrive, providing valuable time to protect a facility. A plan should be established, and resources should be on hand, or quickly, available to prepare a facility. The plan should also include a process for damage assessment, salvage, protection of undamaged property and cleanup following an incident. These actions to minimize further damage and business disruption are examples of property conservation.

Guidance for the development of an emergency response plan can be found in this step.

Protective Actions for Life Safety

When there is a hazard within a building such as a fire or chemical spill, occupants within the building should be evacuated or relocated to safety. Other incidents such as a bomb threat or receipt of a suspicious package may also require evacuation. If a tornado warning is broadcast, everyone should be moved to the strongest part of the building and away from exterior glass. If a transportation accident on a nearby highway results in the release of a chemical cloud, the fire department may warn to "shelter-in-place." To protect employees from an act of violence, "lockdown" should be broadcast and everyone should hide or barricade themselves from the perpetrator.

Protective actions for life safety include:

- Evacuation
- Sheltering
- Shelter-In-Place
- Lockdown

Your emergency plan should include these protective actions. If you are a tenant in multi-tenanted building, coordinate planning with the building manager.

Evacuation

Prompt evacuation of employees requires a warning system that can be heard throughout the building. Test your fire alarm system to determine if it can be heard by all employees. If there is no fire alarm system, use a public address system, air horns or other means to warn everyone to evacuate. Sound the evacuation signal during planned drills so employees are familiar with the sound.

Make sure that there are sufficient exits available at all times.

- Check to see that there are at least two exits from hazardous areas on every floor of every building. Building or fire codes may require more exits for larger buildings.

- Walk around the building and verify that exits are marked with exit signs and there is sufficient lighting so people can safely travel to an exit. If you find anything that blocks an exit, have it removed.
- Enter every stairwell, walk down the stairs, and open the exit door to the outside. Continue walking until you reach a safe place away from the building. Consider using this safe area as an assembly area for evacuees.

Appoint an evacuation team leader and assign employees to direct evacuation of the building. Assign at least one person to each floor to act as a "floor warden" to direct employees to the nearest safe exit. Assign a backup in case the floor warden is not available or if the size of the floor is very large. Ask employees if they would need any special assistance evacuating or moving to shelter. Assign a "buddy" or aide to assist persons with disabilities during an emergency. Contact the fire department to develop a plan to evacuate persons with disabilities.

Have a list of employees and maintain a visitor log at the front desk, reception area or main office area. Assign someone to take the lists to the assembly area when the building is evacuated. Use the lists to account for everyone and inform the fire department whether everyone has been accounted for. When employees are evacuated from a building, OSHA regulations require an accounting to ensure that everyone has gotten out safely. A fire, chemical spill or other hazard may block an exit, so make sure the evacuation team can direct employees to an alternate safe exit.

Sheltering

If a tornado warning is broadcast, a distinct warning signal should be sounded and everyone should move to shelter in the strongest part of the building. Shelters may include basements or interior rooms with reinforced masonry construction. Evaluate potential shelters and conduct a drill to see whether shelter space can hold all employees. Since there may be little time to shelter when a tornado is approaching, early warning is important. If there is a severe thunderstorm, monitor news sources in case a tornado warning is broadcast. Consider purchasing an Emergency Alert System radio - available at many electronic stores. Tune in to weather warnings broadcast by local radio and television stations. Subscribe to free text and email warnings, which are available from multiple news and weather resources on the Internet.

Shelter-In-Place

A tanker truck crashes on a nearby highway releasing a chemical cloud. A large column of black smoke billows into the air from a fire in a nearby manufacturing plant. If, as part of this event, an explosion, or act of terrorism has occurred, public emergency officials may order people in the vicinity to "shelter-in-place." You should develop a shelter-in-place plan. The plan should include a means to warn everyone to move away from windows and move to the core of the building. Warn anyone working outside to enter the building immediately. Move everyone to the second and higher floors in a multistory building. Avoid occupying the basement. Close exterior doors and windows and shut down the building's air handling system. Have everyone remain sheltered until public officials broadcast that it is safe to evacuate the building.

Lockdown

An act of violence in the workplace could occur without warning. If loud "pops" are heard and gunfire is suspected, every employee should know to hide and remain silent. They should seek refuge in a room, close and lock the door, and barricade the door if it can be done quickly. They should be trained to hide under a desk, in the corner of a room and away from the door or windows. Multiple people should be trained to broadcast a lockdown warning from a safe location.

Resources for Protective Actions for Life Safety

In addition to the following resources available on the Internet, seek guidance from your local fire department, police department, and emergency management agency.

- Exit Routes and Emergency Planning – U.S. Occupational Safety & Health Administration (OSHA) 29 CFR 1910 Subpart E
- NFPA 101: Life Safety Code® – National Fire Protection Association
- Employee Alarm Systems – OSHA 29 CFR 1910.165
- Evacuation Planning Matrix – OSHA
- Evacuation Plans and Procedures eTool - OSHA
- Design Guidance for Shelters and Safe Rooms – Federal Emergency Management Agency (FEMA 453)

Incident Stabilization

Stabilizing an emergency may involve many different actions including: firefighting, administering medical treatment, rescue, containing a spill of hazardous chemicals or handling a threat or act of violence. When you dial 9-1-1 you expect professionals to respond to your facility. Depending upon the response time and capabilities of public emergency services and the hazards and resources within your facility, you may choose to do more to prepare for these incidents. Regulations may require you to take action before emergency services arrive.

If you choose to do nothing more than call for help and evacuate, you should still prepare an emergency plan that includes prompt notification of emergency services, protective actions for life safety and accounting of all employees.

Developing the Emergency Plan

Developing an emergency plan begins with an understanding of what can happen. Review your risk assessment. Consider the performance objectives that you established for your program and decide how much you want to invest in planning beyond what is required by regulations.

Assess what resources are available for incident stabilization. Consider internal resources and external resources including public emergency services and contractors. Public emergency services include fire departments that may also provide rescue, hazardous materials and emergency medical

services. If not provided by your local fire department, these services may be provided by another department, agency or even a private contractor. Reach out to local law enforcement to coordinate planning for security related threats.

Document available resources. Determine whether external resources have the information they would need to handle an emergency. If not, determine what information is required and be sure to document that information in your plan.

Prepare emergency procedures for foreseeable hazards and threats. Review the list of hazards presented at the bottom of the page. Develop hazard and threat specific procedures using guidance from the resource links at the bottom of this page.

Warning, Notifications, and Communications

Plans should define the most appropriate protective action for each hazard to ensure the safety of employees and others within the building. Determine how you will warn building occupants to take protective action. Develop protocols and procedures to alert first responders including public emergency services, trained employees and management. Identify how you will communicate with management and employees during and following an emergency.

Roles and Responsibilities for Building Owners and Facility Managers

Assign personnel the responsibility of controlling access to the emergency scene and for keeping people away from unsafe areas. Others should be familiar with the locations and functions of controls for building utility, life safety and protection systems. These systems include ventilation, electrical, water and sanitary systems; emergency power supplies; detection, alarm, communication and warning systems; fire suppression systems; pollution control and containment systems; and security and surveillance systems. Personnel should be assigned to operate or supervise these systems as directed by public emergency services if they are on-site.

Site and Facility Plans and Information

Public emergency services have limited knowledge about your facility and its hazards. Therefore, it is important to document information about your facility. That information is vital to ensure emergency responders can safely stabilize an incident that may occur. Documentation of building systems may also prove valuable when a utility system fails—such as when a water pipe breaks, and no one knows how to shut off the water.

Compile a site-plan and plans for each floor of each building. Plans should show the layout of access roads, parking areas, buildings on the property, building entrances, the locations of emergency equipment and the locations of controls for building utility and protection systems. Instructions for operating all systems and equipment should be accessible to emergency responders.

Provide a copy of the plan to the public emergency services that would respond to your facility and others with responsibility for building management and security. Store the plan with other emergency

planning information such as chemical Material Safety Data Sheets (MSDS), which are required by Hazard Communication or "right to know" regulations.

Training and Exercises

Train personnel so they are familiar with detection, alarm, communications, warning and protection systems. Review plans with staff to ensure they are familiar with their role and can carry out assigned responsibilities. Conduct evacuation, sheltering, sheltering-in-place and lockdown drills so employees will recognize the sound used to warn them and they will know what to do.
Facilitate exercises to practice the plan, familiarize personnel with the plan and identify any gaps or deficiencies in the plan.

10 Steps for Developing the Emergency Response Plan

1. Review performance objectives for the program.
2. Review hazard or threat scenarios identified during the risk assessment.
3. Assess the availability and capabilities of resources for incident stabilization including people, systems and equipment available within your business and from external sources.
4. Talk with public emergency services (e.g., fire, police and emergency medical services) to determine their response time to your facility, knowledge of your facility and its hazards and their capabilities to stabilize an emergency at your facility.
5. Determine if there are any regulations pertaining to emergency planning at your facility; address applicable regulations in the plan.
6. Develop protective actions for life safety (evacuation, shelter, shelter-in-place, lockdown).
7. Develop hazard and threat-specific emergency procedures using the Emergency Response Plan for Businesses.
8. Coordinate emergency planning with public emergency services to stabilize incidents involving the hazards at your facility.
9. Train personnel so they can fulfill their roles and responsibilities.
10. Facilitate exercises to practice your plan.

Links to Emergency Planning Information

Pre-Incident Planning (Site and Building Information for First Responders)

- Fire Service Features of Buildings and Fire Protection Systems - U.S. Occupational Safety & Health Administration (OSHA) Publication 3256-07N
- Standard on Pre-Incident Planning - National Fire Protection Association (NFPA) 1620

Protective Actions for Life Safety

- Evacuation Planning Matrix – OSHA
- Evacuation Plans and Procedures eTool - OSHA
- Design Guidance for Shelters and Safe Rooms

Medical

- CPR and ECC Guidelines - American Heart Association
- Automated External Defibrillators (AEDs) – OSHA
- Bloodborne pathogens – OSHA 29 CFR 1910.1030
- Model Plans and Programs for the OSHA Bloodborne Pathogens and Hazard Communications Standards – OSHA Publication 3186

Firefighting

- Fire Protection – OSHA 29 CFR 1910 Subpart L
- Fire Brigades - OSHA 29 CFR 1910.156
- Standard on Industrial Fire Brigades - NFPA 600

Hazardous materials

- Hazardous Materials Emergency Planning Guide (NRT-1) - U.S. National Response Team

Natural hazards

- National Hurricane Center, Publications, Tropical Cyclone Advisory Mailing Lists, Hurricane Preparedness, The Saffir-Simpson Hurricane Wind Scale (Experimental) - National Weather Service (NWS)
- Thunderstorms, Tornadoes, Lightning, Nature's Most Violent Storms: A Preparedness Guide, Including Tornado Safety Information for Schools - NOAA, National Weather Service
- Tornado Protection: Selecting Refuge Area in Buildings - FEMA 431

Rescue

- Permit-Required Confined Spaces - OSHA 29 CFR 1910.146
- Standard for Rescue Technician Professional Qualifications - NFPA 1006
- Standard on Operations and Training for Technical Search and Rescue Incidents - NFPA 1670

Workplace Violence

- Dealing with Workplace Violence: A Guide for Agency Planners - United States Office of Personnel Management
- Workplace Violence—Issues in Response - Federal Bureau of Investigation

Terrorism, Bomb Threats, and Suspicious Packages

- Ensuring Building Security – DHS
- Safe Rooms and Shelters - Protecting People Against Terrorist Attacks - FEMA 453
- Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks - National Institute for Occupational Safety and Health, Publication No. 2002-139, 2002

Hazards to Consider When Developing the Emergency Plan

Natural hazards

Geological hazards

- Earthquake
- Tsunami
- Volcano
- Landslide, mudslide, subsidence

Meteorological Hazards

- Flood, flash flood, tidal surge
- Water control structure/dam/levee failure
- Drought
- Snow, ice, hail, sleet, arctic freeze
- Windstorm, tropical cyclone, hurricane, tornado, dust storm
- Extreme temperatures (heat, cold)
- Lightning strikes (wildland fire following)

Biological hazards

- Foodborne illnesses
- Pandemic/Infectious/communicable disease (Avian flu, H1N1, etc.)

Human-caused events

Accidental

- Hazardous material spill or release

- Nuclear power plant incident (if located in proximity to a nuclear power plant)
- Explosion/Fire
- Transportation accident
- Building/structure collapse
- Entrapment and or rescue (machinery, confined space, high angle, water)
- Transportation Incidents (motor vehicle, railroad, watercraft, aircraft, pipeline)

Intentional

- Robbery
- Lost person, child abduction, kidnap, extortion, hostage incident, workplace violence
- Demonstrations, civil disturbance
- Bomb threat, suspicious package
- Terrorism

Technology caused events

- Utility interruption or failure (telecommunications, electrical power, water, gas, steam, HVAC, pollution control system, sewerage system, other critical infrastructure)

Cyber security (data corruption/theft, loss of electronic data interchange or ecommerce, loss of domain name server, spyware/malware, vulnerability exploitation/botnets/hacking, denial of service)

Property Conservation

Taking action before a forecast event, such as a severe storm, can prevent damage. Prompt damage assessment and cleanup activities following the storm can minimize further damage and business disruption. These actions are considered “property conservation”—an important part of the emergency response plan. Much of the following guidance is directed to building owners and facility managers. However, tenants should also develop a plan in coordination with building owners and managers as well as public authorities.

Preparing a Facility for a Forecast Event

Body copy: Actions to prepare a facility for a forecast event depend upon the potential impacts from the hazards associated with the event. Conduct a risk assessment to identify severe weather hazards including winter storms, arctic freeze, tropical storm, hurricane, flooding, storm surge, severe thunderstorm, tornado and high winds. Also consider non-traditional hazards, such as a planned event involving a large crowd.

Property conservation actions should focus on protection of the building and valuable machinery, equipment and materials inside. Potential damage may be prevented or mitigated by inspecting the following building features, systems and equipment:

- Windows and doors
- Roof flashing, covering and drainage
- Exterior signs
- Mechanical equipment, antennas and satellite dishes on rooftops
- Outside storage, tanks and equipment
- Air intakes
- High value machinery
- Sensitive electronic equipment including information technology and process controllers

The review of building components may also identify opportunities for longer-term mitigation strategies.

Property conservation activities for specific forecast events include the following:

- **Winter storm** - Keep building entrances and emergency exits clear; ensure there is adequate fuel for heating and emergency power supplies; monitor building heat, doors and windows to prevent localized freezing; monitor snow loading and clear roof drains.
- **Tropical storms and hurricanes** - Stockpile and pre-cut plywood to board up windows and doors (or install hurricane shutters); ensure there is sufficient labor, tools and fasteners available; inspect roof coverings and flashing; clear roof and storm drains; check sump and portable pumps; backup electronic data and vital records off-site; relocate valuable inventory to a protected location away from the path of the storm.
- **Flooding** - Identify the potential for flooding and plan to relocate goods, materials and equipment to a higher floor or higher ground. Clear storm drains and check sump and portable pumps. Raise stock and machinery off the floor. Prepare a plan to use sandbags to prevent water entry from doors and secure floor drains.

Salvage and Actions to Prevent Further Damage Following an Incident

Separating undamaged goods from water-soaked goods is an example of salvage. Covering holes in a roof or cleaning up water and ventilating a building are also part of property conservation. The property conservation plan should identify the resources needed to salvage undamaged good and materials; make temporary repairs to a building; clean up water, smoke and humidity; and prepare critical equipment for restart.

Resources for property conservation include the following:

- water vacuums and tools to remove water
- fans to remove smoke and humidity
- tarpaulins or plywood to cover damaged roofs or broken windows
- plastic sheeting to cover sensitive equipment

Compile an inventory of available equipment, tools and supplies and include it with the emergency response plan. Identify precautions for equipment exposed to water or high humidity and procedures for restarting machinery and equipment.

Identify contractors that may be called to assist with clean up and property conservation efforts. Keep in mind that competition for contractors, labor, materials and supplies prior to a forecast storm or following a regional disaster may be intense. Plan ahead and secure contractors and other resources in advance.

Resources for Property Conservation

- Protect Your Property from High Winds - Federal Emergency Management Agency
- Natural Disasters - U.S. Environmental Protection Agency
- Emergency Drying Procedures for Water Damaged Collections - Library of Congress
-

Resource Management

There are many resources required for the preparedness program including:

- People
- Facilities
- Communications and warning technologies
- Fire protection and life safety systems
- Pollution control systems
- Equipment
- Materials and supplies
- Funding
- Special expertise
- Information about the threats or hazards

Consider the following examples:

If there is a fire inside a building, the fire alarm system warns employees to evacuate. An evacuation team guides employees to safe exits and outside to assembly areas. The fire alarm system, evacuation team and exits are resources.

When a primary facility cannot be occupied, a suitable alternate facility (if available) may be used. The alternate facility is a resource for the business continuity plan.

Needs Assessment

A needs assessment should be conducted to determine resources needed. Resources may come from within the business including trained employees, protection and safety systems, communications equipment and other facilities owned or leased by the business. Other resources from external sources include public emergency services, business partners, vendors and contractors.

The availability and capability of resources must be determined - some are required immediately. For example, trained people (employees or public emergency services) capable of administering first aid or cardiopulmonary resuscitation (CPR) must be available to respond at a moment's notice. Other resources such as plywood to board up windows in anticipation of a hurricane may be stockpiled in advance or purchased when a storm is forecast. Even if plywood is stockpiled in advance, temporary labor may be needed to install the plywood over windows and doors.

The availability of resources often depends on logistics. Logistics is the management of resources to get them to where they are needed when they are needed.

Assessing resources for the preparedness program begins with reviewing program goals and performance objectives. High-level goals of the program include:

- Protect the safety of employees, visitors, contractors and others who may be at risk from hazards at the facility
- Maintain customer service by minimizing disruptions of business operations
- Protect facilities, physical assets and electronic information
- Prevent environmental pollution
- Protect the organization's brand, image, and reputation

Examples of performance objectives include:

- The first aid team (that is trained to administer first aid and perform CPR) will be able to reach any employee within two minutes.
- The evacuation team will be able to direct all employees to safe exits and account for them outside the building within four minutes.
- Customer service staff will begin contacting customers within 8 hours of a service disruption using office space and telephone service provided by a business partner.
- The primary network server will be restored within 24 hours with replacement equipment from your primary vendor and data restored from backup media retrieved from the secure storage site.
- Production of product A will resume within 1 week by displacing production of product B at Plant B.

For each objective, an assessment of resources needed to accomplish the objective should be conducted. Simple objectives may require limited resources. Aggressive objectives will require many resources with significant capabilities available on short notice. Remember, without sufficient resources, or if resources lack required capabilities, objectives may not be attainable.

Conducting the Needs Assessment

Besides identifying specific resources for the preparedness program, the needs assessment should answer other questions:

- What quantity of a resource is required?

- When will the resource be needed?
- What capability does the resource need to have? Are there any limitations?
- What is the cost for procuring or having the resource available? Are there any liabilities associated with use of the resource?

Resources

There are many resources needed to support the preparedness program. These resources can be organized into different categories:

- People
- Facilities
- Systems
- Equipment
- Materials
- Supplies
- Funding
- Information

Resources are needed for all phases of the program including prevention/deterrence, mitigation, emergency response, business continuity, crisis communications and disaster recovery.

Human Resources

Employees are needed to staff emergency response, business continuity and crisis communications teams. The emergency response team may be limited to employees trained to direct evacuation or sheltering. Some businesses may choose to organize emergency response teams to administer first aid, perform CPR and use automated external defibrillators (AEDs). Still others may train staff to use portable fire extinguishers. Regulations define minimum requirements that include training and organizing employees. Staff is needed to develop and manage the business continuity and crisis communication plans. The teams will likely be made up of employees working in their respective departments. Some staff may be assigned to work at alternate worksites if a primary worksite cannot be occupied.

Facilities

Facilities for emergency response include defined shelter space for protection from a tornado or interior space when "shelter-in-place" from an exterior airborne hazard is required. Facilities should also include a room that can be equipped to serve as an emergency operations center for supporting response to an incident. Other facilities needed include office space or a meeting room with communications equipment to serve as a communications hub.

Facilities for business continuity may include alternate workspace equipped for continuation of business operations. Alternate facilities may be owned or contracted including office space, data center, manufacturing and distribution.

Systems

Systems for emergency response may include detection, alarm, warning, communications, suppression and pollution control systems. Protection of critical equipment within a data center may include sensors monitoring heat, humidity and attempts to penetrate computer firewalls.

Every building has exit routes so people can evacuate if there is a hazard within the building. These exit routes should be designed and maintained in accordance with applicable regulations.

Business continuity resources may include spare or redundant systems that serve as a backup in case primary systems fail. Systems for crisis communications may include existing voice and data technology for communicating with customers, employees and others.

Equipment

Equipment includes the means for teams to communicate. Radios, smartphones, wired telephone and pagers may be required to alert team members to respond, to notify public agencies or contractors and to communicate with other team members to manage an incident.

Other equipment depends on the functions of the team. Automated External Defibrillators may be required for a first aid/CPR team. Fire extinguishers would be required for a fire brigade. Spill containment and absorbent equipment would be required for a hazardous materials response team or trained employees working in their assigned workspace. Personal protective equipment including hearing, eye, face and foot protection may be required for employees as part of a safety program.

Many tools may be required to prepare a facility for a forecast event such as a hurricane, flooding or severe winter storm.

Materials and Supplies

Materials and supplies are needed to support members of emergency response, business continuity and crisis communications teams. Food and water are basic provisions.

Systems and equipment needed to support the preparedness program require fuel. Emergency generators and diesel engine driven fire pumps should have a fuel supply that meets national standards or local regulatory requirements. That means not allowing the fuel supply to run low because replenishment may not be possible during an emergency. Spare batteries for portable radios and chargers for smartphones and other communications devices should be available.

Funding

Money invested in the preparedness program can pay big dividends if an incident occurs. Consider the benefits of a fire being controlled quickly; immediate medical assistance that saves an injured employee; or a recovery strategy that enables continued customer service. Spending funds prudently

on preparedness can pay back multiple times when measured against the potential for damage to equipment, facilities, loss of staff, lost customers and lost revenue.

Worksheets

Two worksheets are provided to assist with the needs assessment. Think about your program needs, identify additional resources and assess what is needed for your business.

Emergency response resource requirements.

Business continuity resource requirements.

Internal Resources

There are many resources within your business that are needed for your preparedness program. These internal resources include staff for emergency response, business continuity and crisis communications teams. Other resources include facilities, systems, equipment, materials and supplies to support response, continuity and recovery operations. Identify needed resources and determine what resources are available internally. Resources that are not available must be obtained from external resources. Consider the following internal resources for your preparedness program.

People

Employees can be assigned the following tasks.

- Monitor weather forecasts and Emergency Alert System messages, broadcast warnings if severe weather is approaching or other warnings are broadcast, and alert the emergency response team
- Direct evacuation and shelter actions (See Protective Actions for Life Safety)
- Administer first aid, CPR and use automated external defibrillators (AEDs)
- Provide facility security and take the lead on threats including bomb threats and suspicious packages
- Operate building detection, alarm, communications, warning, protection and utility systems
- Stabilize an incident using fire extinguishers; or cleaning up /containing small spills of hazardous chemicals
- Prepare a facility for a forecast event such as severe weather
- Clean up damage following an incident
- Lead the business continuity team; provide support for the team
- Execute recovery strategies for critical or time sensitive business processes;
- Serve as a spokesperson as part of the crisis communications team; communicate with employees, stakeholders and the news media; answer requests for information

Employees should be trained so they understand the importance of their assignments and follow established procedures. Some employees may be given the opportunity to learn new skills.

Facilities

Office space and meeting rooms can be used as an emergency operations center (EOC), which is a facility for incident management. The EOC is a place to bring together personnel, gather information, facilitate communications, procure resources and support preparedness, response, continuity and recovery efforts.

Rooms or areas within the interior of a building that are structurally strong can shelter people from a tornado. Unobstructed exits that are marked with signs and equipped with emergency lighting are essential to quickly evacuating people if there is a fire or hazard inside.

Owned buildings at another site may be used as alternate workspace if a building cannot be occupied. This depends upon the location of the building and whether the building would be affected by the same hazard that prevented use of the primary building. The alternate facility may be a viable business recovery strategy if the building can be configured with the required equipment or existing equipment can be configured to need business requirements.

Systems and Equipment

Many systems and equipment are needed to detect potential hazards and threats, protect life safety and property and continue business operations. These resources include:

- Detection systems (fire detection, burglar alarm or intrusion detection, computer network security, Emergency Alert System receivers and television, radio, for news and weather)
- Alarm systems (fire alarm, intrusion alarm and process system alarms)
- Warning systems (occupant warning systems include fire alarm, public address and tornado warning)
- Communications systems (landline telephones, cellphones, smartphones, email and data, radios and pagers)
- Pollution containment systems (primary and secondary building containment and devices to stop the flow of materials from tanks and piping)
- Fire protection and suppression systems (fire sprinklers, fire extinguishers, fire pumps and water supplies, special extinguishers for computer rooms and special hazards)
- Emergency power supplies (uninterruptible power supplies and generators).
- Building utility systems (electrical, plumbing, heating, ventilation, air conditioning and sanitary)

Evaluate these systems to determine whether they meet the needs of the program. Identify and plan to overcome emergency communication system limitations such as weak radio or cellular service or areas where a warning system cannot be heard. Upgrading this critically important system may be required. Verify that these systems are in reliable working condition. If fuel, battery backup power or batteries are required, make sure the system can run for the required time and chargers are available. Document how to operate these systems and mark the locations of controls. Make sure the information is available during an emergency. Many of these systems also require periodic

inspection, testing and maintenance in accordance with national codes and standards. Train staff so a knowledgeable person is able to operate systems and equipment.

Materials and Supplies

There are lots of basic materials and supplies needed for the preparedness program. These "consumable" resources include clipboards, paper forms, pens and pencils. Sufficient copies of paper forms are especially important to do automated tasks manually. Flashlights with spare batteries are needed if the power goes out. Provision of food and water for personnel engaged in preparedness, response, continuity and recovery activities should also be addressed in the plan.

Be sure to compile a list of available resources using the Emergency Response Resource Requirements and Business Continuity Resource Requirements worksheets as a guide.

External Resources

Preparing for an emergency, responding to an emergency, executing business recovery strategies and other activities require resources that come from outside the business. If there were a fire in the building, you would call the fire department. Contractors and vendors may be needed to prepare a facility for a forecast storm or to help repair and restore a building, systems or equipment following an incident.

An understanding of the availability and capabilities of external resources is needed to make decisions about the preparedness program. How long would it take the fire department to arrive? How do you reach a contractor late at night and how long will it take them to arrive? Determination of the response time and capabilities of external resources will help you identify gaps between what you need and what is available. Strategies should be developed to fill these gaps.

The following external resources should be identified within plan documents. Include contact information to reach them during an emergency and any additional instructions within the preparedness plan.

Public Emergency Services

(Note: one agency or department may provide multiple services)

- Fire
- Emergency medical services
- Hospital or emergency health care provider
- Rescue
- Hazardous materials
- Law enforcement (local, county, state police)
- Public health
- Public works

Contractors and Vendors

- Emergency services (hazardous materials cleanup, facility repair and restoration)
- Systems and equipment (procurement, inspection, testing and maintenance)
- Information technology (equipment procurement, data backup, recovery solutions)
- Business continuity (generators, temporary equipment, leased space, office trailers)

Partnerships

(*Reciprocal or mutual aid agreements)

- Business partners (suppliers, contractors, vendors and professional services firms that could lend assistance with services, temporary workspace and other resources)
- Businesses or civic organizations in the community

* Reciprocal or other agreements should be documented in writing if possible.

Logistics

Logistics considerations are an important part of the preparedness program to ensure that resources will be available when and where they are needed.

Compile an inventory of internal and external resources to identify their location, the operating procedures and the persons who can operate these systems. Also, note the estimated delivery or response time of external resources.

A person should be assigned responsibility for logistics and to manage resources to support the preparedness program. They should work with the emergency response and business continuity teams who can identify resource needs.

Logistics procedures should define procurement requirements including the names of employees who have the authority to issue purchase orders and contract for services. Procedures should also be established to expedite obtaining resources during an emergency. Open purchase orders with potential contractors and vendors will expedite the procurement process.

Last Updated: 05/26/2021

Crisis Communications Plan

When an emergency occurs, the need to communicate is immediate. If business operations are disrupted, customers will want to know how they will be impacted. Regulators may need to be notified and local government officials will want to know what is going on in their community. Employees and their families will be concerned and want information. Neighbors living near the

facility may need information—especially if they are threatened by the incident. All of these "audiences" will want information before the business has a chance to begin communicating.

An important component of the preparedness program is the crisis communications plan. A business must be able to respond promptly, accurately and confidently during an emergency in the hours and days that follow. Many different audiences must be reached with information specific to their interests and needs. The image of the business can be positively or negatively impacted by public perceptions of the handling of the incident.

This step of Ready Business provides direction for developing a crisis communications plan. Understanding potential audiences is key, as each audience wants to know: "How does it affect me?" Guidance for scripting messages that are specific to the interests of the audience is another element of the plan. The Contact & Information Center tab explains how to use existing resources to gather and disseminate information during and following an incident.

Audiences

Understanding the audiences that a business needs to reach during an emergency is one of the first steps in the development of a crisis communications plan. There are many potential audiences that will want information during and following an incident and each has its own needs for information. The challenge is to identify potential audiences, determine their need for information and then identify who within the business is best able to communicate with that audience.

The following is a list of potential audiences.

- Customers
- Survivors impacted by the incident and their families
- Employees and their families
- News media
- Community—especially neighbors living near the facility
- Company management, directors and investors
- Government elected officials, regulators and other authorities
- Suppliers

Contact Information

Contact information for each audience should be compiled and immediately accessible during an incident. Existing information such as customer, supplier and employee contact information may be exportable from existing databases. Include as much information for each contact as possible (e.g., organization name, contact name, business telephone number, cell number, fax number and email address). Lists should be updated regularly, secured to protect confidential information and available to authorized users at the emergency operations center or an alternate location for use by members of

the crisis communications team. Electronic lists can also be hosted on a secure server for remote access with a web browser. Hard copies of lists should also be available at the alternate location.

Customers

Customers are the life of a business, so contact with customers is a top priority. Customers may become aware of a problem as soon as their phone calls are not answered or their electronic orders are not processed. The business continuity plan should include action to redirect incoming telephone calls to a second call center (if available) or to a voice message indicating that the business is experiencing a temporary problem. The business continuity plan should also include procedures to ensure that customers are properly informed about the status of orders in process at the time of the incident.

Customer service or sales staff normally assigned to work with customers should be assigned to communicate with customers if there is an incident. If there are a lot of customers, then the list should be prioritized to reach the most important customers first.

Suppliers

The crisis communication or business continuity plan should include documented procedures for notification of suppliers. The procedures should identify when and how they should be notified.

Management

Protocols for when to notify management should be clearly understood and documented. Consider events that occur on a holiday weekend or in the middle of the night. It should be clear to staff what situations require immediate notification of management regardless of the time of day. Similar protocols and procedures should be established for notification of directors, investors and other important stakeholders. Management does not want to learn about a problem from the news media.

Government Officials & Regulators

Communications with government officials depends upon the nature and severity of the incident and regulatory requirements. Businesses that fail to notify a regulator within the prescribed time risk incurring a fine. OSHA regulations require notification to OSHA when there are three or more hospitalizations from an accident or if there is a fatality. Environmental regulations require notification if there is chemical spill or release that exceeds threshold quantities. Other regulators may need to be notified if there is an incident involving product tampering, contamination or quality. Notification requirements specified in regulations should be documented in the crisis communications plan.

A major incident in the community will capture the attention of elected officials. A senior manager should be assigned to communicate with elected officials and public safety officials.

Employees, Victims and Their Families

Human Resources (HR) is responsible for the day-to-day communications with employees regarding employment issues and benefits administration. HR management should assume a similar role on the crisis communications team. HR should coordinate communications with management, supervisors, employees and families. HR should also coordinate communications with those involved with the care of employees and the provision of benefits to employees and their families. Close coordination between management, company spokesperson, public agencies and HR is needed when managing the sensitive nature of communications related to an incident involving death or serious injury.

The Community

If there are hazards at a facility that could impact the surrounding community, then the community becomes an important audience. If so, community outreach should be part of the crisis communications plan. The plan should include coordination with public safety officials to develop protocols and procedures for advising the public of any hazards and the most appropriate protective action that should be taken if warned.

News Media

If the incident is serious, then the news media will be on scene or calling to obtain details. There may be numerous requests for information from local, regional or national media. The challenge of managing large numbers of requests for information, interviews and public statements can be overwhelming. Prioritization of requests for information and development of press releases and talking points can assist with the need to communicate quickly and effectively.

Develop a company policy that only authorized spokespersons are permitted to speak to the news media. Communicate the policy to all employees explaining that it is best to speak with one informed voice.

Determine in advance who will speak to the news media and prepare that spokesperson with talking points, so they can speak clearly and effectively in terms that can be easily understood.

Messages

During and following an incident, each audience will seek information that is specific to them. “How does the incident affect my order, job, safety, community…?” These questions need to be answered when communicating with each audience.

After identifying the audiences and the spokesperson assigned to communicate with each audience, the next step is to script messages. Writing messages during an incident can be challenging due to the

pressure caused by “too much to do” and “too little time.” Therefore, it is best to script message templates in advance if possible.

Pre-scripted messages should be prepared using information developed during the risk assessment. The risk assessment process should identify scenarios that would require communications with stakeholders. There may be many different scenarios but the need for communications will relate more to the impacts or potential impacts of an incident:

- accidents that injure employees or others
- property damage to company facilities
- liability associated injury to or damage sustained by others
- production or service interruptions
- chemical spills or releases with potential off-site consequences, including environmental
- product quality issues

Messages should be scripted to address the specific needs of each audience, which may include:

Customer - “When will I receive my order?” “What will you give me to compensate for the delay?”

Employee - “When should I report to work?” “Will I have a job?” “Will I get paid during the shutdown or can I collect unemployment?” “What happened to my co-worker?” “What are you going to do to address my safety?” “Is it safe to go back to work?”

Government Regulator - “When did it happen?” “What happened (details about the incident)?” “What are the impacts (injuries, deaths, environmental contamination, safety of consumers, etc.)?”

Elected Official - “What is the impact on the community (hazards and economy)?” “How many employees will be affected?” “When will you be back up and running?”

Suppliers - “When should we resume deliveries and where should we ship to?”

Management - “What happened?” “When did it happen?” “Was anyone injured?” “How bad is the property damage?” “How long do you think production will be down?”

Neighbors in the Community - “How can I be sure it’s safe to go outside?” “What are you going to do to prevent this from happening again?” “How do I get paid for the loss I incurred?”

News Media - “What happened?” “Who was injured?” “What is the estimated loss?” “What caused the incident?” “What are you going to do to prevent it from happening again?” “Who is responsible?”

Messages can be pre-scripted as templates with blanks to be filled in when needed. Pre-scripted messages can be developed, approved by the management team and stored on a remotely accessible server for quick editing and release when needed.

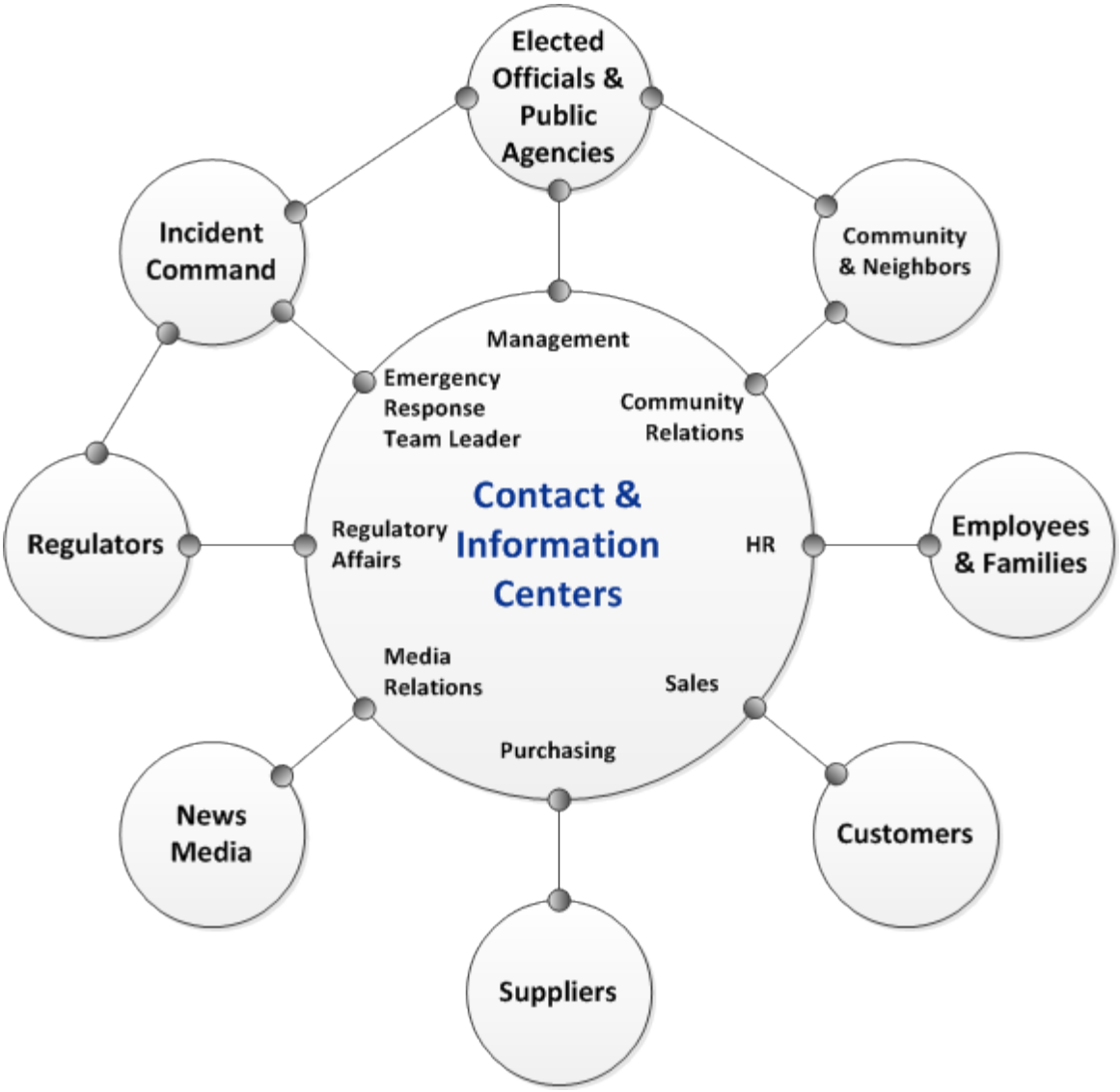
Another important element of the crisis communications plan is the need to coordinate the release of information. When there is an emergency or a major impact on the business, there may be limited information about the incident or its potential impacts. The "story" may change many times as new information becomes available.

One of the aims of the crisis communication plan is to ensure consistency of message. If you tell one audience one story and another audience a different story, it will raise questions of competency and credibility. Protocols need to be established to ensure that the core of each message is consistent while addressing the specific questions from each audience.

Another important goal of the crisis communications plan is to move from reacting to the incident, to managing a strategy, to overcome the incident. Management needs to develop the strategy and the crisis communications team needs to implement that strategy by allaying the concerns of each audience and positioning the organization to emerge from the incident with its reputation intact.

Contact & Information Centers

Communications before, during and following an emergency is bi-directional. Stakeholders or audiences will ask questions and request information. The business will answer questions and provide information. This flow of information should be managed through a communications hub.



Crisis Communications Hub & Spoke Diagram - Text Version

Contact and Information Centers form the "hub" of the crisis communications plan. The centers receive requests for information from each audience and disseminate information to each audience. Employees from multiple departments may be assigned to communicate with a specific audience.

The "contact center" fields inquiries from customers, suppliers, the news media and others. The contact center should be properly equipped and staffed by personnel to answer requests for information. The staff working within the contact center should be provided with scripts and a "frequently asked questions" (FAQ) document to answer questions consistently and accurately.

The "information center" consists of existing staff and technologies (e.g., website, call center, bulletin boards, etc.) that field requests for information from customers, employees and others during

normal business hours. The information center and its technologies can be used to push information out to audiences and post information for online reading.

The crisis communications team, consisting of members of the management team, should operate in an office environment to support the contact and information centers. The offices may be clustered near the emergency operations center or at an alternate site if the primary site cannot be occupied. The goal of the crisis communications team is to gather information about the incident. This should include monitoring the types of questions posed to call center operators or staff in the office; emails received by customer service; social media chatter or stories broadcast by the news media. Using this input, the crisis communications team can inform management about the issues that are being raised by stakeholders. In turn, management should provide input into the messages generated by the crisis communications team. The team can then create appropriate messages and disseminate information approved for release.

Resources for Crisis Communications

Resources should be available within the primary business site and provisions should be made to set up similar capabilities within an alternate site in case the primary site cannot be occupied.

- Telephones with dedicated or addressable lines for incoming calls and separate lines for outgoing calls
- Access to any electronic notification system used to inform employees
- Electronic mail (with access to "info@" inbox and ability to send messages)
- Fax machine (one for receiving and one for sending)
- Webmaster access to company website to post updates
- Access to social media accounts
- Access to local area network, secure remote server, message template library and printers
- Hard copies of emergency response, business continuity and crisis communications plan
- Site and building diagrams, information related to business processes and loss prevention programs (e.g., safety and health, property loss prevention, physical and information/cyber security, fleet safety, environmental management and product quality)
- Copiers
- Forms for documenting events as they unfold
- Message boards (flipcharts, white boards, etc.)
- Pens, pencils, paper, clipboards and other stationery supplies

IT Disaster Recovery Plan

Businesses use information technology to quickly and effectively process information. Employees use electronic mail and Voice Over Internet Protocol (VOIP) telephone systems to communicate. Electronic data interchange (EDI) is used to transmit data including orders and payments from one company to another. Servers process information and store large amounts of data. Desktop

computers, laptops and wireless devices are used by employees to create, process, manage and communicate information. What do you when your information technology stops working?

An information technology disaster recovery plan (IT DRP) should be developed in conjunction with the business continuity plan. Priorities and recovery time objectives for information technology should be developed during the business impact analysis. Technology recovery strategies should be developed to restore hardware, applications and data in time to meet the needs of the business recovery.

Businesses large and small create and manage large volumes of electronic information or data. Much of that data is important. Some data is vital to the survival and continued operation of the business. The impact of data loss or corruption from hardware failure, human error, hacking or malware could be significant. A plan for data backup and restoration of electronic information is essential.

Resources for Information Technology Disaster Recovery Planning

- Computer Security Resource Center - National Institute of Standards and Technology (NIST), Computer Security Division Special Publications
- Contingency Planning Guide for Federal Information Systems - NIST Special Publication 800-34 Rev. 1
- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities – NIST Special Publication 800-84
- Building An Information Technology Security Awareness and Training Program - NIST Special Publication 800-50

IT Recovery Strategies

Recovery strategies should be developed for Information technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity. Priorities for IT recovery should be consistent with the priorities for recovery of business functions and processes that were developed during the business impact analysis. IT resources required to support time-sensitive business functions and processes should also be identified. The recovery time for an IT resource should match the recovery time objective for the business function or process that depends on the IT resource.

Information technology systems require hardware, software, data and connectivity. Without one component of the "system," the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

- Computer room environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals)
- Connectivity to a service provider (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)

- Data and restoration

Some business applications cannot tolerate any downtime. They utilize dual data centers capable of handling all data processing needs, which run in parallel with data mirrored or synchronized between the two centers. This is a very expensive solution that only larger companies can afford. However, there are other solutions available for small to medium sized businesses with critical business applications and data to protect.

Internal Recovery Strategies

Many businesses have access to more than one facility. Hardware at an alternate facility can be configured to run similar hardware and software applications when needed. Assuming data is backed up off-site or data is mirrored between the two sites, data can be restored at the alternate site and processing can continue.

Vendor Supported Recovery Strategies

There are vendors that can provide "hot sites" for IT disaster recovery. These sites are fully configured data centers with commonly used hardware and software products. Subscribers may provide unique equipment or software either at the time of disaster or store it at the hot site ready for use.

Data streams, data security services and applications can be hosted and managed by vendors. This information can be accessed at the primary business site or any alternate site using a web browser. If an outage is detected at the client site by the vendor, the vendor automatically holds data until the client's system is restored. These vendors can also provide data filtering and detection of malware threats, which enhance cyber security.

Developing an IT Disaster Recovery Plan

Businesses should develop an IT disaster recovery plan. It begins by compiling an inventory of hardware (e.g. servers, desktops, laptops and wireless devices), software applications and data. The plan should include a strategy to ensure that all critical information is backed up.

Identify critical software applications and data and the hardware required to run them. Using standardized hardware will help to replicate and reimage new hardware. Ensure that copies of program software are available to enable re-installation on replacement equipment. Prioritize hardware and software restoration.

Document the IT disaster recovery plan as part of the business continuity plan. Test the plan periodically to make sure that it works.

Data Backup

Businesses generate large amounts of data and data files are changing throughout the workday. Data can be lost, corrupted, compromised or stolen through hardware failure, human error, hacking and malware. Loss or corruption of data could result in significant business disruption.

Data backup and recovery should be an integral part of the business continuity plan and information technology disaster recovery plan. Developing a data backup strategy begins with identifying what data to backup, selecting and implementing hardware and software backup procedures, scheduling and conducting backups and periodically validating that data has been accurately backed up.

Developing the Data Backup Plan

Identify data on network servers, desktop computers, laptop computers and wireless devices that needs to be backed up along with other hard copy records and information. The plan should include regularly scheduled backups from wireless devices, laptop computers and desktop computers to a network server. Data on the server can then be backed up. Backing up hard copy vital records can be accomplished by scanning paper records into digital formats and allowing them to be backed up along with other digital data.

Options for Data Backup

Tapes, cartridges and large capacity USB drives with integrated data backup software are effective means for businesses to backup data. The frequency of backups, security of the backups and secure off-site storage should be addressed in the plan. Backups should be stored with the same level of security as the original data.

Many vendors offer online data backup services including storage in the “cloud”. This is a cost-effective solution for businesses with an internet connection. Software installed on the client server or computer is automatically backed up.

Data should be backed up as frequently as necessary to ensure that, if data is lost, it is not unacceptable to the business. The business impact analysis should evaluate the potential for lost data and define the “recovery point objective.” Data restoration times should be confirmed and compared with the IT and business function recovery time objectives.

Employee Assistance & Support

When disaster strikes a business, the impacts include more than just the property damage and business disruption. Employees may be injured or temporarily out of a job. A disaster that affects a community may also damage employees’ homes or force them to stay with family or friends. The human impact could be significant.

Providing assistance and support for employees should be part of a business' preparedness program. It should include communicating with employees and their families and providing support as appropriate.

Communicating with Employees

Following a disaster in the community, it is in the best interest of the business to communicate with all employees. Employee information, typically compiled in a human resource information system, includes home addresses and telephone numbers. Consider asking for additional information including home email addresses and cellular telephone numbers (for text messaging/SMS). Also, request the name and contact information of a family member or friend who can be reached in an emergency. The confidentiality of this information should be protected and only be available to authorized users who are operating from their office, emergency operations center or alternate business facility.

If the business uses an electronic notification system, the additional contact information should also be added to that database. Use call lists or the electronic notification system to contact employees and identify those who need assistance or are awaiting instructions from their employer. If your business has a call center, inform employees to contact the call center following a disaster to obtain official information. The crisis communications plan should include procedures to provide official information to call center operators.

Incident Management

When an emergency occurs or there is a disruption to the business, organized teams will respond in accordance with established plans. Public emergency services may be called to assist. Contractors may be engaged and other resources may be needed. Inquiries from the news media, the community, employees and their families and local officials may overwhelm telephone lines. How should a business manage all of these activities and resources? Businesses should have an incident management system (IMS). An IMS is "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" [NFPA 1600].

The National Incident Management System (NIMS) was established by FEMA and includes the Incident Command System (ICS). NIMS is used as the standard for emergency management by all public agencies in the United States for both planned and emergency events. Businesses with organized emergency response teams that interface with public emergency services can benefit from using the ICS. ICS is also well suited for managing disruptions of business operations. Public information and crisis communications are an integral part of the ICS structure.

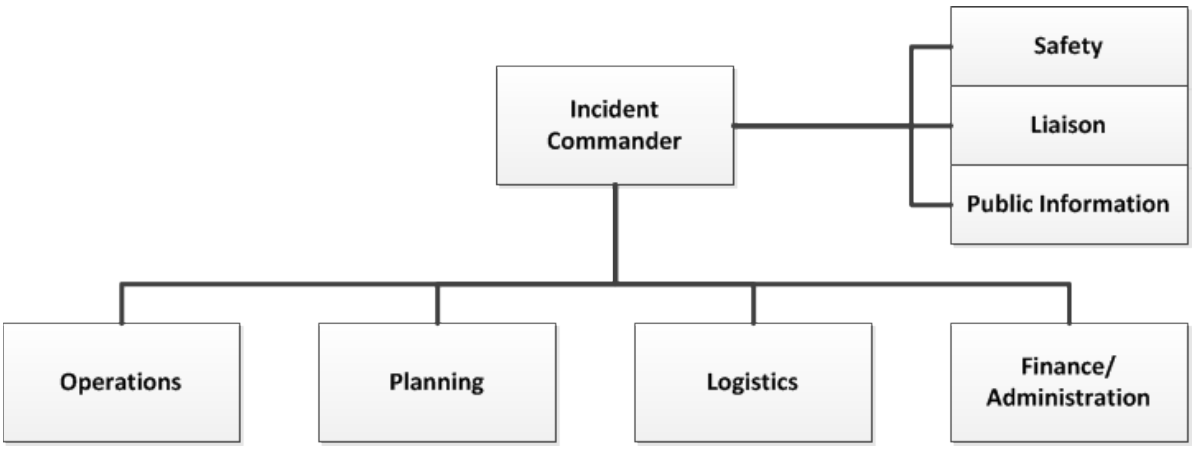
When an incident occurs, incident stabilization activities (e.g. firefighting, damage assessment, property conservation) may be underway at the scene of the incident. Others assigned to support incident stabilization, business continuity or crisis communications activities will report to an emergency operations center (EOC). The emergency operations center is a physical or virtual location from which coordination and support of incident management activities is directed.

The Incident Command System and the use of an Emergency Operations Center supports incident management.

Resources for Emergency Operations Centers

- National Incident Management System and NIMS Resource Center - U. S. Department of Homeland Security, Federal Emergency Management Agency
- ICS Resource Center - Incident Command System, Emergency Management Institute, Federal Emergency Management Agency
- Standard on Emergency Services Incident Management System - NFPA 1561

Incident Command System



Incident Command System Diagram - Text Version

The Incident Command System (ICS) is used by public agencies to manage emergencies. ICS can be used by businesses to work together with public agencies during emergencies. Private sector businesses should be familiar with the fundamental concepts of incident command and should

coordinate planning with local public emergencies services. The use of ICS within a business depends upon the size and complexity of the business. Functions and roles may be assigned to multiple individuals or a few persons may be assigned multiple responsibilities.

Not all of the ICS positions need to be active in each incident. The ICS structure is meant to expand and contract as the scope of the incident requires. For small-scale incidents, only the incident commander may be assigned. Command of an incident would likely transfer to the senior on-scene officer of the responding public agency when emergency services arrive on the scene. Command transfers back to the business when the public agency departs.

An abbreviated summary of the roles and responsibilities of each ICS position are presented below.

Incident Commander

- 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
- Assess the situation
- 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 others to incident command positions as needed
- Brief 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, crisis communications and 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

Safety

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

Liaison

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

Public Information

- 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 useful information to the media

Operations

- Manage all tactical operations during the incident
- Assist in the development of the operations portion of the Incident Action Plan
- Ensure safe tactical operations 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

- 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

- Provides resources to stabilize the incident and support personnel, 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:

- 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 materials 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

Emergency Operations Center

An emergency operations center (EOC) is a physical (e.g., a conference room) or virtual (e.g., telephone conference call) location designed to support emergency response, business continuity and crisis communications activities. Staff meets at the EOC to manage preparations for an impending event or manage the response to an ongoing incident. By gathering the decision makers together and supplying them with the most current information, better decisions can be made. A primary EOC should be established at the main business facility and a secondary EOC should be available at another company facility, a temporary facility (such as a hotel) or through a teleconference bridge established to bring staff together virtually. The EOC supports the following incident management functions.

Activation -Bring knowledge and expertise together to deal with events that threaten the business

Situation Analysis -Gather information to determine what is happening and to identify potential impacts

Incident Briefing - Efficiently share information among team members

Incident Action Plan - Provide a single point for decision-making and decide on a course of action for the current situation

Resource Management - Provide a single point of contact to identify, procure and allocate resources

Incident Management -Monitor actions, capture event data and adjust strategies as needed

An EOC is not an on-scene incident command post (ICP) - where the focus is on tactics to deal with the immediate situation. An EOC is used to support on-scene activities through the prioritization of activities and the allocation of available resources. A major function within the EOC is communications between the emergency response team, business continuity team, crisis communications team and company management.

Emergency Operations Center

A large conference room can be used as an emergency operations center and primary team meeting location. It must be outfitted with furniture, telephone and internet access and be in close proximity to photocopiers, network printers, fax machines and other office equipment. The conference room or other space to be used as the EOC should be equipped with the following equipment and supplies:

- Communications equipment including sufficient telephones (cell and landline with at least one speakerphone) to handle incoming and outgoing calls; incoming and outgoing fax machines; and access to any radio systems used by the business
- Computers and printers with access to network resources (including electronic copies of emergency response, business continuity and crisis communications plans that can be printed on demand), electronic mail and the internet
- Information gathering and display tools including access to broadcast radio and television (preferably with recording capability) or internet news sources; white boards, TV monitors, projection units or flipcharts with easel and markers to compile and display information
- Hard copies of emergency response, business continuity and crisis communications plans, contact/telephone lists, resource inventory and diagrams of facilities and systems
- Stationery, business and incident management forms, pens, pencils, markers and supplies
- Food, water and dining supplies for EOC staff

The emergency operations center should be activated whenever there is a major incident that causes significant property damage, potential or actual business disruption or has the potential to cause a significant impact on the business.

Training

If there is a fire in the building would employees know what to do? Are they familiar with the system that would alert them to evacuate, shelter or lockdown? Do they know who is in charge during an emergency? Do they know who is authorized to speak with the news media? Are employees familiar with their responsibilities for building and information security? Can they carry out their assigned responsibilities during an emergency or business disruption?

Training is essential to ensure that everyone knows what to do when there is an emergency, or disruption of business operations. Everyone needs training to become familiar with protective actions for life safety (e.g., evacuation, shelter, shelter-in-place and lockdown). Review protective actions for life safety and conduct evacuation drills (“fire drills”) as required by local regulations. Sheltering and lockdown drills should also be conducted. Employees should receive training to become familiar with safety, building security, information security and other loss prevention programs.

Members of emergency response, business continuity and crisis communications teams should be trained so they are familiar with their role and responsibilities as defined within the plans. Team leaders should receive a higher level of training, including incident command system training, so they can lead their teams. Review applicable regulations to determine training requirements. Records documenting the scope of training, participants, instructor and duration should be maintained.

If emergency response team members administer first aid, CPR or use AEDs, they should receive training to obtain and maintain those certifications. If employees use portable fire extinguishers, fire hoses or other firefighting equipment, they should be trained in accordance with the applicable OSHA regulation. If employees respond to hazardous materials spills, they also require training.

Who needs training?	What training should be provided?
All employees	• Protective actions for life safety (evacuation, shelter, shelter-in-place, lockdown) • Safety, security, and loss prevention programs
Emergency Response Team (evacuation, shelter, shelter-in-place)	• Roles and responsibilities as defined in the plan • Training as required to comply with regulations or maintain certifications (if employees administer first aid, CPR or AED or use fire extinguishers or clean up spills of hazardous chemicals) • Additional training for leaders including incident management
Business Continuity Team	• Roles and responsibilities as defined in the plan • Additional training for leaders including incident management
Crisis Communications Team	• Roles and responsibilities as defined in the plan • Additional training for leaders including incident management • Training for spokespersons

Drills and exercises should also be conducted to validate emergency response, business continuity and crisis communications plans and to evaluate the ability of personnel to carry out their assigned roles and responsibilities.

Training Resources

- Training Requirements in OSHA Standards and Training Guidelines - U.S. Occupational Safety & Health Administration
- ICS (Incident Command System) Training Materials and Opportunities - Emergency Management Institute (EMI), Federal Emergency Management Agency (FEMA)
- Building An Information Technology Security Awareness and Training Program - National Institute of Standards and Technology, Special Publication 800-50
- Emergency Management Institute Higher Education Program - DHS, FEMA, EMI
- Business and Industry Crisis Management - DHS, FEMA, EMI
- Continuity of Operations Training – DHS, FEMA, EMI

Testing & Exercises

You should conduct testing and exercises to evaluate the effectiveness of your preparedness program, make sure employees know what to do and find any missing parts. There are many benefits to 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 regulations
- Gain recognition for the emergency management and business continuity program

Testing the Plan

When you hear the word "testing," you probably think about a pass/fail evaluation. You may find that there are parts of your preparedness program that will not work in practice. Consider a recovery strategy that requires relocating to another facility and configuring equipment at that facility. Can equipment at the alternate facility be configured in time to meet the planned recovery time objective? Can alarm systems be heard and understood throughout the building to warn all employees to take protective action? Can members of emergency response or business continuity teams be alerted to respond in the middle of the night? Testing is necessary to determine whether or not the various parts of the preparedness program will work.

Exercises

When you think about exercises, physical fitness to improve strength, flexibility and overall health comes to mind. Exercising the preparedness program helps to improve the overall strength of the preparedness program and the ability of team members to perform their roles and to carry out their responsibilities. There are several different types of exercises that can help you to evaluate your program and its capability to protect your employees, facilities, business operations, and the environment

Testing

Tests should be conducted to validate that business continuity recovery strategies will work. Tests should also be conducted to verify that systems and equipment perform as designed. Tests can take several forms, including the following:

Component - Individual hardware or software components or groups of related components that are part of protective systems or critical to the operation of the organization are tested.

System - A complete system test is conducted to evaluate the system's compliance with specified requirements. A system test should also include an examination of all processes or procedures related to the system being tested.

Comprehensive - All systems and components that support the plan are tested. An example of a comprehensive test is confirming that IT operations can be restored at a backup site in the event of an extended power failure at the primary site.

Tests of information technology systems and recovery strategies should be conducted in a manner that resembles the everyday work environment. If feasible, an actual test of the components or systems used should be employed. Since tests can potentially be disruptive, tests may be performed on systems that mimic the actual operational conditions.

Inspection, testing and maintenance of building protection systems including fire detection, alarm, warning, communication, employee notification, emergency power supplies, life safety, fire suppression, pollution containment and others should be conducted in accordance with manufacturers' instructions and regulatory requirements. If a critical warning system or protection system fails, the consequences could be significant.

A test schedule should be developed in accordance with applicable regulations, standards and best practices and designed to meet performance objectives. Records should be maintained.

Guidance on evaluating the need for testing; creating a test plan; and designing, developing, conducting and evaluating tests is provided in the Resources for Testing.

Resources for Testing

- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities - Recommendations of the National Institute of Standards and Technology, Special Publication 800-84
- Fire Code - National Fire Protection Association (NFPA) 1
- Recommended Practice on Commissioning and Integrated Testing of Fire Protection and Life Safety Systems -NFPA 3
- Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems - NFPA 25
- National Fire Alarm and Signaling Code - NFPA 72
- Standard for Emergency and Standby Power Systems - NFPA 110
- Standard on Stored Electrical Energy Emergency and Standby Power Systems - NFPA 111

Exercises

Post-incident critiques often confirm that experience gained during exercises was the best way to prepare teams to respond effectively to an emergency. Exercises should be designed to engage team members and get them working together to manage the response to a hypothetical incident. Exercises enhance knowledge of plans, allow members to improve their own performance and identify opportunities to improve capabilities to respond to real events.

Exercises are a great method to:

- Evaluate the preparedness program
- Identify planning and procedural deficiencies
- Test or validate recently changed procedures or plans
- Clarify roles and responsibilities
- Obtain participant feedback and recommendations for program improvement
- Measure improvement compared to performance objectives
- Improve coordination between internal and external teams, organizations and entities
- Validate training and education
- Increase awareness and understanding of hazards and the potential impacts of hazards.
- Assess the capabilities of existing resources and identify needed resources

Types of Exercises

There are different types of exercises that can be used to evaluate program plans, procedures and capabilities.

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

Walkthroughs, workshops and orientation seminars are basic training for team members. They are designed to familiarize team members with emergency response, business continuity and crisis communications plans and their roles and responsibilities as defined in the plans.

Tabletop exercises are discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator guides participants through a discussion of one or more scenarios. The duration of a tabletop exercise depends on the audience, the topic being exercised and the exercise objectives. Many tabletop exercises can be conducted in a few hours, so they are cost-effective tools to validate plans and capabilities.

Functional exercises allow personnel to validate plans and readiness by performing their duties in a simulated operational environment. Activities for a functional exercise are scenario-driven, such as the failure of a critical business function or a specific hazard scenario. Functional exercises are

designed to exercise specific team members, procedures and resources (e.g. communications, warning, notifications and equipment set-up).

A full-scale exercise is as close to the real thing as possible. It is a lengthy exercise which takes place on location using, as much as possible, the equipment and personnel that would be called upon in a real event. Full-scale exercises are conducted by public agencies. They often include participation from local businesses.

Developing an Exercise Program

Develop an exercise program beginning with an assessment of needs and current capabilities. Review the risk assessment and program performance objectives. Conduct a walkthrough or orientation session to familiarize team members with the preparedness plans. Review roles and responsibilities and ensure everyone is familiar with incident management. Identify probable scenarios for emergencies and business disruption. Use these scenarios as the basis for tabletop exercises. As the program matures, consider holding a functional exercise. Contact local emergency management officials to determine if there is an opportunity to participate in a full-scale exercise within your community.

Exercises should be evaluated to determine whether exercise objectives were met and to identify opportunities for program improvement. A facilitated "hot wash" discussion held at the end of an exercise is a great way to solicit feedback and identify suggestions for improvement. Evaluation forms are another way for participants to provide comments and suggestions. An after-action report that documents suggestions for improvement should be compiled following the exercise and copies should be distributed to management and others. Suggestions for improvement should be addressed through the organization's corrective action program.

Resources for Exercises

- Emergency Planning Exercises for Your Organization - Federal Emergency Management Agency
- Homeland Security Exercise, and Evaluation Program - U.S. Department of Homeland Security
- IS-139 Exercise Design - Emergency Management Institute Independent Study Program
- A Guide for the Conduct of Emergency Management Tabletop Activities - Oak Ridge Institute for Science and Education
- Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities - Recommendations of the National Institute of Standards and Technology, Special Publication 800-84

Program Improvement

There are opportunities for program improvement following an actual incident. A critique should be conducted to assess the response to the incident. Lessons learned from incidents that occur within the community, within the business' industry or nationally can identify needs for preparedness program changes. Best practices and instructional guidance published by trade associations, professional societies, newsletters and government website can be resources to evaluate and improve your preparedness program.

Gaps and deficiencies identified during reviews should be recorded and addressed through a corrective action program. Reviews, evaluations and improvements should be documented and maintained on file.

Program Reviews

Businesses should improve the effectiveness of their preparedness programs through review of policies, performance objectives, program implementation and changes resulting from preventive and corrective actions.

Triggers for Program Reviews

Reviews of the preparedness program should be conducted periodically and whenever the effectiveness of the program is questioned. The goal of program reviews is to provide assurance that the program meets the needs of the business and complies with regulations. Changes that should trigger a review of the program include the following:

- 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

If any of these changes or triggers occurs, the program coordinator should initiate the appropriate program review.

Scope of Program Reviews

Program reviews should assess compliance with policies; determine whether performance objectives are being met; assess the adequacy of program implementation; and determine whether preventive and corrective actions have been taken on previously identified deficiencies.

The following should also be reviewed:

- Plans and procedures have been reviewed and are up-to-date
- Team rosters have been updated to ensure membership is current
- Contact information for team members, public agency contacts, contractors, vendors and suppliers
- Resources (e.g., systems, equipment, and supplies) are in place and properly maintained

Resources for Program Reviews

- Lessons Learned Information Sharing - U. S. Department of Homeland Security
- U. S. Chemical Safety and Hazard Investigation Board - The CSB is an independent federal agency charged with investigating industrial chemical accidents. The CSB website provides reports on current and completed investigations as well as videos.
- Fatality Assessment and Control Evaluation (FACE) Program - National Institute for Occupational Safety and Health, Division of Safety Research

Corrective Actions

Gaps and deficiencies identified during program reviews should be recorded and addressed through a corrective action program. Gaps or deficiencies in the program may be identified during training, drills, exercises, post-incident critiques, regulatory compliance audits, insurance surveys and from lessons learned.

Corrective Action Program

The corrective action program should document information on deficiencies. A table similar to the one below can be used. Include a full description of the deficiency; the action that should be taken; the resources required to address the deficiency; and justification for the need to correct the deficiency. Action on deficiencies should be assigned to the person or department best able to address the issue. A due date should be assigned and the corrective action database reviewed regularly to track progress. The status column should be updated until the deficiency has been addressed.

Description Action or Resources Required Justification Priority Assigned To Due Date Status

All program gaps or deficiencies are not equally important. Prioritization of corrective actions is helpful because funding and time are usually limited. Prioritization can also identify significant deficiencies that should be reported to management and corrected as quickly as possible. Criteria or categories for corrective action may include the following:

- Hazards to health and safety
- Regulatory compliance
- Hazards to property, operations, the environment or the entity (e.g., image or reputation)
- Conformity to national standards
- Following industry best practices

Management Reporting

Significant deficiencies should be reported to management along with appropriate information to explain the problem, how to correct it and the reasons it needs to be addressed in order to gain management support for action. Management should also be periodically informed of the status of corrective actions until deficiencies have been resolved.