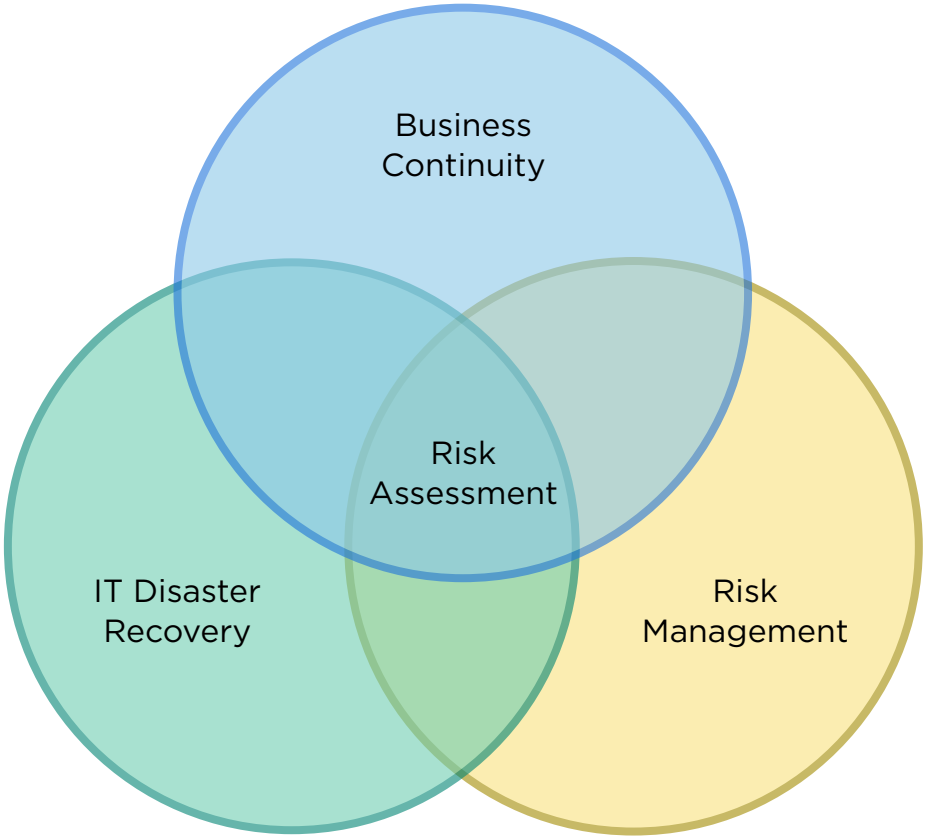
Business Continuity Management Program

Businesses fail in planning by not being able to identify potential threats and underestimating the severity of known potential threats.

Objectives of Business Continuity Management (BCM) include:

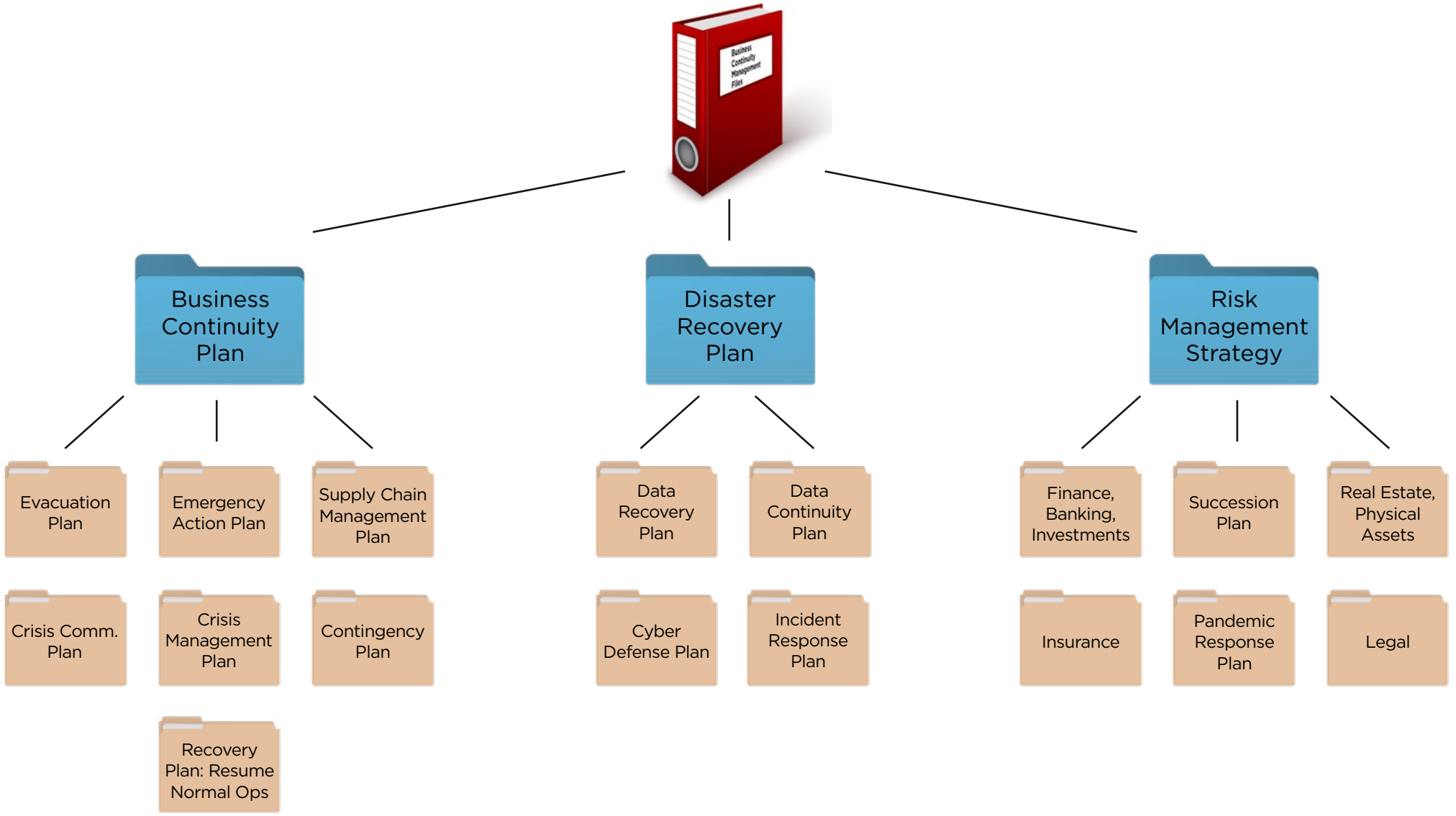
1. Health and safety of all personnel
2. Protect the reputation of the business
3. Protect sales and revenue
4. Retain existing customers
5. Improve the business
6. Avoid lawsuits and legal liability

Business owners should ensure necessary steps are taken to identify the different types of potential losses and their impacts, who is involved in the plan and how the plans are to be executed.



Link: [Introduction to Business Continuity Planning]

Overview: Sample Business Continuity Management Flowchart



Overview

Whether starting from scratch or enhancing a Business Continuity Plan, there are some steps to keep in mind when getting started. Those steps include:

1. **Prepare to Plan:** Identify what you already know about your business/operation
2. **Define Your Plan Objective:** Define your company's core mission
3. **Identify and Prioritize Your Potential Risks and Impacts:** Identify what threats/hazards your organization is exposed to and calculate the possibility and impact those threats present to your organization
4. **Develop Your Business Continuity Strategy:** Start putting plans together to address those threats or hazards that can have an impact on your organization
5. **Identify the Teams and Define Their Tasks:** When creating the Business Continuity Plan, also identify teams within the organization. The teams and team members should have designated roles/responsibilities.
6. **Train Staff and Test Your Plan:** Train all key personnel on the organization Business Continuity Plan. Periodically test the plan to verify that it meets the organization's needs and key personnel understand and know their roles and responsibilities.

Nationwide®

Step 1: Prepare to Plan

What is already known about the organization? There is information that can be pulled together for future discussions and help with the development of a Business Continuity Management Program.

Good practice in preparing is gathering information on your organization. The information can help understand what gaps are present. To help understand what type of information to gather, a list of examples is below.

- Organizational charts
- Company confidentiality requirements
- Information about teams and team members
- Business insurance
- Vital records
- Raw materials and supply lists
- Customers (customer lists)
- Processes and procedures (SOPs and interdependencies like power and water, phone, internet, fuel, email, and critical software)
- Contact information
- Account numbers
- Points of contact (primary and secondary)
- Suppliers, vendors, and customers
- Fire, police, ambulance, hospital, and poison control
- Utilities and communications (service providers)
- Manufacturing systems providers
- Equipment providers
- Software providers
- Alternate on/off site storage locations

Step 2: Define Your Objective

Determine your company's core mission. This is the organization's reason for existence. An organization's mission statement supports the vision and serves to communicate the purpose and direction.

The overall health and safety of all personnel is priority, as are minimizing business interruptions, minimizing financial loss and resuming operations within a specified time frame.

Link: Core Mission Statement Worksheet

Step 3: Identify and Prioritize Risks and Impacts

There are several types of disasters and threats that organizations are exposed to, whether they are natural, willful, accidental, or technological. Some organizations are exposed more than others.

Organizations can see how vulnerable they are by conducting a vulnerability/risk assessment on the different types of threats. To help identify the impact a threat has on your organization, a Business Impact Analysis should be conducted. If you're unsure about resources currently available or required, analyze what is needed and how much time it will take to be back up in operation.

Natural Disasters/Threats

Willful Disasters/Threats

Accidental Disasters/Threats

Technological Disasters/Threats

Examples of Technological Disasters/Threats include:

- Computer Virus
- Hacking
- Software Failure
- Hardware Failure
- Ransomware

Step 4: Develop Your Business Continuity Strategy

A Business Continuity Management Program is broken down into three different areas with specific topics under each area.

Business Continuity Plan

- Crisis Management and Response Worksheet
- Crisis Management and Communication
- Emergency Action Plans
- Supply Chain Management Plan
  - Sample Supply Chain Input Form
- Evacuation Plan
- Contingency Plan
- Recovery Plan

Disaster Preparedness Recovery Plan

- Cyber Defense Plan: FCC Cyberplanner
- Incident Response Plan
- Data Continuity Plan
- Data Recovery Plan: Ready.gov IT Disaster Recovery Plan

Risk Management Strategy

- Pandemic Response Plan
- Legal Considerations
- Real Estate Asset Management
- Finance, Banking, Investment Consideration:
  - Ready.gov: Financial Preparedness
  - CFPB: Disasters and Emergencies
- Insurance Consideration, Business Interruption, etc.:
  - Ready.gov - Document and Insure Your Property
  - Insurance Information Institute: Do I Need Business Interruption Insurance?

Step 5: Identify Your Teams and Define Their Tasks

When creating the Business Continuity Plan, identify teams within the organization. The teams and team members should have designated roles and responsibilities. That way when an event occurs, the organization's team(s) know what to do. The teams must meet regularly and review their roles and responsibilities.

Examples of different teams include, but are not limited to:

- Emergency response team (i.e., fire, spill, severe weather)
- Recovery team
- Supply management team

Link: Critical Teams Worksheet

Step 6: Train Staff and Test the Continuity Plan

Key to any successful Business Continuity Plan is to train key personnel and test the plan through mock drills and/or tabletop exercises.

Drills/tabletop exercises should be documented to identify what went right or what gaps/exposures does the organization still have, so measures can be taken to narrow the exposures/gaps.

Anytime changes are made to a Business Continuity Plan, key personnel must be retrained. Situations consistently change within an organization, regardless of whether they are external or internal. An organization must adapt and adjust their plans accordingly.

Link: Introduction to BCM Tabletop Exercises

Context and Definitions

There are many **Business Continuity Management (BCM)** models because there are numerous organizations that provide standards to regions around the world. In the United States, we have relied on standards such as National Fire Protection Association (NFPA) and are beginning to adopt the International Standards Organization (ISO).

Consider BCM as the umbrella or master file under which all other plans are subsets, including **Business Continuity Planning (BCP)** and **Disaster Recovery (DR)**. While BCP developed because of DR through the 1970's and 1980's, the difference between business continuity and disaster recovery is quite specific (see definitions below). Balancing the two planning strategies is a matter of priorities.

The terms Business Continuity and Disaster Recovery are not interchangeable though many seem to think otherwise (Google either term and search results will include a mish-mash of improperly used words and definitions). DR and BCP are two entirely different strategies, each of which plays a significant aspect in safeguarding business operations and each of which can be executed in tandem or separately.

The third factor under the BCM umbrella is the overall organization **Risk Management Strategy**. This is where considerations are made for less tactical and sometimes less tangible operational concerns such as insurance and short and long-term financing.

One thing all elements of BCM have in common is that they cannot be effective if they are not written, including the business impact analysis for each factor. In addition, organizations that plan, train, communicate, and assess their plans are likely to have the best outcomes in terms of mitigating damage to people property, and finances. Many businesses write the plan, but neglect to update it, at least annually.

When a natural disaster or event caused by human action disrupts normal business operations the BCP, DRP, and Risk Management Strategy and subsequent elements of each can be executed concurrently or individually, depending on the nature of the event. In all cases, the **Emergency Action Plan (EAP)** is immediately activated to ensure employees and guests on premise are safe. Crisis response and communication occurs according to plan once EAP has been initiated. Specific event contingencies are then executed. Once business operations are stabilized and personnel are accounted for, the long-term business recovery plan is executed.

The following is not a comprehensive list of definitions (nor are the definitions themselves comprehensive) but used with the accompanying chart provides context and one suggestion for logical organization of the master BCM file.

Context and Definitions Table of Contents

- Business Continuity Management / Resiliency Planning
- Business Continuity Plan
- Contingency Plan
- Crisis Communication Plan (CCP)
    - Public Relations
- Crisis Management Plan (CMP)
    - Command Center
    - Contact List
    - Crisis Management Team (CMT)
    - Evaluation and Corrections
    - Logistics
    - Organizational Responsibilities of the Team
    - Sub-Teams
- Cyber Defense Plan
- Data Continuity Plan
- Data Recovery Plan
- Disaster Recovery Plan
- Emergency Action Plan (EAP)
- Evacuation Plan
- Finance, Banking, Investments
- Incident Response Plan
- Insurance
- Legal Contracts, Compliance
- Pandemic Response Plan
- Real Estate, Physical Assets
- Risk Management Strategy
- Supply Chain Management Plan (SCM)
- Business Impact Analysis
- Crisis
- Disruption
- Emergency
- Execution or Invocation
- Incident
- Maximum Acceptable Outage
- Process or Activity
- Stakeholder or Interested Party

Context and Definitions

Business Continuity Management/Resiliency Planning: The BCM can be considered the umbrella or master file for subsequent plans. BCM provides a cyclical framework to monitor and continuously improve the ensuing resiliency plans:

1. Plans and Procedures – Threat assessment and Plan development
2. Test, Training and Exercise
3. Evaluations, After Action Reports, Lessons Learned
4. Develop Corrective Action Plans

Business Continuity Plan: While a subset of BCM, BCP can be considered a master file for subsequent strategies or plans of action for critical processes and procedures executed to ensure business operations continue during a disaster. Proper execution of the BCP can mean the difference between survival and total shutdown. It is based on relentless analysis of critical business processes and operations.

Contingency Plan: After the incident, this plan will be executed to ensure contingent plans occur to keep the business operating. This can include other contingencies such as secondary office location being set up until use of primary office location can be reestablished. The plan should consider the most likely disruption events and layout expected actions and responsibilities for each. Think tornado, earthquake, fire, hurricane, civil unrest, etc. These considerations may also require adjustment to other related plans based on the type of event.

Crisis Communication Plan (CCP): The Federal Emergency Management Agency (FEMA) recommends a crisis communication plan CCP. The plan describes how the organization will communicate with employees, local authorities, customers, and others during and after a disaster. Employees need information about reporting to work. Emergency responders, the general public, and neighboring businesses should be provided with a briefing on the nature of the emergency.

- **Public Relations:** In a time of crisis the last thing an organization needs is 'bad press'. A CMT member should be specifically assigned to this task. Interaction with media regarding the crisis and action being taken to contain it should be consistent regardless of communication platform (radio, television, internet, print, etc.)

Context and Definitions, Continued

Crisis Management Plan (CMP): The CMP is a component of the overall Business Continuity Plan and could contain overlapping communication and decisionmaking components of the BCP. A well thought of and documented Crisis Management Plan will facilitate communication between all stakeholders with safety considerations being paramount.

- The elements of a CMP include:
  1. Defining the crisis – exactly what happened
  2. Determining if disaster should be declared
  3. Detailed steps for impact assessment
  4. Activating the Crisis Management Plan
- **Command Center:** A Crisis Management/Emergency Operations Command Center should be designated as the focal point for handling the crisis.
- **Contact List:** A regularly updated contact list should be compiled to keep internal and external stakeholders in the loop.
- **Crisis Management Team (CMT):** Includes senior managers who have the expertise and experience needed to manage a crisis. Anyone else with specialized knowledge useful in combating the crisis.
- **Logistics:** The logistical support for notification, mobilization and manning of crisis centers should be clearly laid out.
- **Organizational responsibilities of the team:** Each member should be assigned a specific task by defining their functions, duties and responsibilities during a crisis.
- **Sub-teams:** Function under the overall direction a CMT member. A sub-team will have people with different types of expertise, who can handle the tasks associated with the crisis
- **Evaluation and Corrections:** After the conclusion of the crisis, assigned members should evaluate the response and take corrective action toovercome deficiencies.

Context and Definitions, Continued

Cyber Defense Plan: Defense can be divided into three areas: Physical, Technical, and Administrative. It focuses on building capabilities for effective cybersecurity defend networks, systems, and information; defend the organization against cyberattacks of significant consequence; and support operational and contingency plans.

In addition to regular updates and training, the Cyber Defense Plan should include:

- Acceptable Use Policy
- Password Policy
- Backup Policy
- Network Access Policy
- Incident Response Policy
- Remote Access Policy
- Email Policy
- Guest Access Policy
- Wireless Policy
- Third Party Connection Policy
- Network Security Policy
- Encryption Policy
- Confidential Data Policy
- Data Classification Policy
- Mobile Device Policy
- Retention Policy
- Outsourcing Policy
- Physical Security Policy
- Virtual Private Network (VPN) Policy

Context and Definitions, Continued

Data Continuity Plan: A subset of the DRP, the data continuity plan focuses on ensuring that alternate processes are in place to carry out key operational functions. In case of outage, the IT team should be able to recover and restart systems locally or in the cloud to continue providing services to internal and external clients until the business can safely fail back.

- Identify personnel responsible for executing the backup plan (data confidentiality best interests – laws govern personally identifiable information).
- Identify all systems and data lakes that require backup.
- Construct a schedule that routinely checks systems and backup data.
- Depending on backup and recovery solution provider, the cost of service and backup may increase.
- Develop and detail specific recovery procedures to restore data from backup repositories.

Data Recovery Plan: A subset of the DRP, the data recovery plan focuses on methodically restoring each critical application in the IT structure. Considerations include maximum downtime to restore to restore the system through cloud-based technology and/or backups (restore-point tolerance). A restore point is a time between the last cloud backup and when the system went down.

Disaster Recovery Plan (DRP): DRPs involve restoring vital communications, hardware, and IT asset support systems. Disaster recovery aims to minimize business downtime by focusing on getting technical operations back to normal in the shortest time possible. IT disasters can range from small hardware failures to large scale security breaches.

Context and Definitions, Continued

Emergency Action Plan (EAP): An EAP ensures the safety of employees and guests on site at the time of the emergency. It is a written document required byOSHA's emergency action plan standard (29 CFR 1910.38). In addition to immediate safety, the EAP should facilitate and organize employer and employee actions during a workplace emergency. Train, Communicate, Practice.

The plan should be written, communicated to and accessible by all employees, but it can be communicated orally in an organization with 10 or fewer employees. A well-developed plan that is understood by employees can result in fewer and less severe injuries and less damage to the facilities and equipment.

Employee training should be offered after developing the initial plan and to all new hires and individuals whose role or responsibility within the organization has changed. Employees should be retrained when duties or responsibilities under the plan change, or if a new facility layout, equipment, or hazards are introduced. Educate employees about the types of emergencies that could occur. Be sure they understand the elements the EAP and any specific site hazards. In addition, training should address:

- Who will be in charge, overall and within each facility
- Notification procedures
- How CMT members in an emergency
- Evacuation and sheltering procedures
- Location and use of emergency equipment
- Shutdown procedures

Context and Definitions, Continued

Evacuation Plan: Building evacuation procedures employees and site visitors to:

1. Safely stop work and shut down equipment that could become unstable or present a hazard.
2. Leave the building through the nearest door with an EXIT sign. Do not use elevators.
3. Report to designated assembly area.
4. Wait for instructions from emergency responders.

Plan what to take. Will employees need to grab their laptop, hard copy of the BCM, key contact lists, password lists for cloud data retrieval, etc. Conduct drills.

If the plan includes leaving the facility and property completely, choose several destinations in different directions to leave options in an emergency. Leave early enough to avoid being trapped by severe weather. Follow recommended evacuation routes. Do not take shortcuts; they may be blocked. Be alert for road hazards such as washed-out roads or bridges and downed power lines.

Finance, Banking, Investments: A financial recovery plan is a pathway to gaining stability after an unexpected, disastrous expense depletes reserves. Plan steps to build savings and capital back up and ensure the ability to recover and prepare for the next significant event. Basic financial recovery plans should include:

1. Evaluate the damage
2. Set short-term financial goals
3. Redo the short-term budget. Follow and update the budget regularly.
4. Plan now for future losses. Build a reserve through savings and investments.

Making a full financial recovery plan will help get operations back up but the process can be long and arduous, depending on the gravity the situation and the extent of organizational responsibilities.

Context and Definitions, Continued

Incident Response Plan: The purpose of an Incident Response Plan (IR) is to establish and test clear measures that an organization should take to reduce the impact of a breach from external and internal threats. While not every attack can be prevented, an organization's IR should emphasize anticipation, agility, and adaptation. With a successful program, damage can be mitigated or avoided altogether. Enterprise architecture and systems engineering assume that systems or components have either been compromised or contain undiscovered vulnerabilities that could lead to undetected compromises. Additionally, missions and business critical functions must continue to operate in the presence of compromise.

Insurance: First rule; don't rely exclusively on insurance to help the organization recover from the unexpected – cash reserves, investments, redundant physical assets (key equipment) etc. are some good companions to insurance under the overall risk management strategy.

A business insurance policy may only cover loss or damage to your inventory and equipment. There are a lot of other things that may not be considered or covered in your insurance policies. Insurers can ad exclusions or endorsements to a standard package policy such as flood, earthquake, hurricane, pandemic, civil unrest, etc. Make sure you have discussed with your insurance agent the most likely events that can disrupt your organization; then make sure the agent has discussed coverage options with your insurance company.

Legal Contracts, Compliance:

1. Maintain a list of names and contact information for legal experts within or retained by the organization. Don't overlook specialty counsel for brand and image, environmental impact, human impact as a result of the organization's operations.
2. Maintain a schedule of contracts where the organization is leagally bound to delivery products, goods, or services. Include a list of organizations, vendors, etc., who are legally bound to deliver to your organization.
3. Review contracts to ensure wording is favorable to your organization and will not leave undue burden following an interruption or disaster.
4. Maintain necessary proof of compliance for DOT, OSHA, EPA, and other government agencies.

Context and Definitions, Continued

Pandemic Response Plan: According to Merriam-Webster Dictionary, a pandemic is "Outbreak of a disease that occurs over a wide geographic area and affects an exceptionally high proportion of the population: a pandemic outbreak of a disease".

Pandemics happen when a new virus emerges to infect people and can spread between people sustainably. Because there is little to no pre-existing immunity against the new virus, it can spread quickly. Causes can be naturally occurring or the result of human action such as bioterrorism. Considerations for the response plan should include communications, international travel, screening of travelers, and incident management structures, shelter in place, and work from home scenarios.

Real Estate, Physical Assets:

1. Maintain up to date lists including current valuations for all buildings and properties owned by the organization.
2. Maintain asset and inventory lists of critical and/or expensive equipment (i.e. data servers, data processing equipment, lab equipment, communications equipment, etc.).
3. Maintain names and contact information for realtors, contractors, suppliers, vendors, etc. who could assist with replacing or rebuilding. Prequalify these individuals by requesting proof of insurance – keep this documentation current.

Risk Management Strategy: Even if your organization survives a disaster, without effective planning it could experience the following losses:

- Financial: Lost profits, a lower market share, government fines because of data breaches. HIPAA fines, for example, have amounted to multi-millions.
- Damage to reputation and brand through negative publicity.
- Sanctions: Loss of business license or legal liability. Lost time and money even if a lawsuit is won.
- Breach of contract: Inability to meet obligations to clients. Includes a ripple effect up and down the supply chain. Could even drive some suppliers and customers out of business.
- Dead in the water: Stalled or frozen business objectives and plans, missed market opportunities.

Context and Definitions, Continued

Supply Chain Management Plan (SCM): SCM is often overlooked because organizations think they don't need to worry about it because they may not be involved in manufacturing. Think about cloud data storage vendors – your organization is the consumer and they are the vendor. Think about medical supplies or drinking water for employees or business guests who are temporarily unable to leave the premises. Consider third parties that provide digital tools or content upon which the organization relies.

SCM can also be considered the processes that control the flow of goods and services within an organization. It includes all processes that turn raw materials into final products but also involves the design, planning, procurement, execution, control, and monitoring of supply and demand, materials, and resource capacity.

Additional components of supply chain management could include: Planning, Information, Source, Inventory, Production, Location, Transportation, and Return of goods.

Related Definitions

Business Impact Analysis: Process of analyzing activities and the effect that a business disruption might have upon them.

Crisis: An unstable condition involving an impending abrupt or decisive change; a turning point. A disruptive event which affects a business's facilities, IT systems, data, personnel etc. The halt in production could have a cascading effect on revenues, profitability, production schedules, business reputation, customer goodwill, etc. A crisis could be internal or external in nature and could be major or minor.

Disruption: An event, whether anticipated or unanticipated, causing an unplanned negative deviation from the expected delivery of products or services according to the organization's objectives

Emergency: A serious situation or occurrence that happens unexpectedly and demands immediate action

Execution or Invocation: An act of declaring that an organization's business continuity arrangements need to be put into effect in order to continue delivery of key products or services. Following through on the plans that are already in place.

Context and Definitions, Continued

Incident: A situation or event that might or could lead to a disruption, loss, emergency or crisis.

Maximum Acceptable Outage (MAO): The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable (aka aximum Tolerable Period of Disruption)

Process or Activity: Process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products and services. Prioritized Activities are those to which priority must be given following an incident in order to best mitigate impacts.

Stakeholder or Interested Party: A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Definitions adapted from IRMI, ISO, and DRJ and reputable internet sources.

Link Index

Nationwide Resources

- Vulnerability and Risk Assessment
- Resource Requirement Worksheet
- Business Impact Analysis Worksheet
- Emergency Action Plan Decision Matrix
- Business Impact Analysis and Resource Requirement
- Pre-Incident Planning
- Emergency Action Plans
- Crisis Management and Response Worksheet
- Crisis Management and Communication
- Supply Chain Management Plan
- Cyber-Incident Response Plan
- Sample Supply Chain Assessment Form
- An Easy-to Use Guide to Business Continuity Planning

External Resources

- Ready.gov: Financial Preparedness
- FEMA: Document and Insure Your Property
- Consumer Financial Protection Bureau: Disasters and Emergencies
- FEMA: Floodsmart.gov
- Insurance Information Institute: Do I Need Business Interruption Insurance?
- Ready.gov: Insurance Coverage Discussion Form
- Insurance Institute for Business & Home Safety (IBHS)