CIRCUMSPEX™

Why We Plan

Today, businesses face a myriad of challenges in growing and sustaining themselves. These challenges include factors that are within the organization's control and many that are not. In this document we explore a planning process that harnesses the power of what you can control and the collective knowledge of your business or organization. Through this process, you will empower yourself to minimize the risks of disastrous events and crisis that are beyond your control.

The need for this planning is obviously to protect people, equipment, systems, and facilities from the dire impacts of disasters. In an age of information deluge there has never been a time when the need for disaster planning has been so apparent. Yet, despite our awareness of the impacts that tragedies like 9/11, Hurricane Katrina, and the western wildfires have had, disaster planning remains overlooked in many homes and businesses across the country.

The Association of Records Managers and Administrators reports that 60 percent of businesses impacted by a major disaster close within two years of the event. Similarly, the Strategic Research Institute states "companies that aren't able to resume operation within 10 days of a disaster are not likely to survive."

Time magazine reports that the Hazards and Vulnerability Research Institute at the University of South Carolina finds that "91 percent of Americans live in places with a moderate to high risk of earthquakes, volcanoes, tornadoes, wildfires, hurricanes, flooding, high wind damage, or terrorism." So, with all the media images, television reports, magazine articles, and research studies, why aren't we better prepared?

Most Americans continue to be in denial of the risks. In the same *Time* article, Eric Holdeman, Director of Emergency Management for King County, Seattle, sums it up best: "There are four stages of denial. One: It won't happen. Two: If it does happen, it won't happen to me. Three: If it does happen to me, it won't be that bad. And four: If it happens to me and it's that bad, there's nothing I can do to stop it anyway."

Obviously, if you are reading this, you manifest an interest in overcoming denial and inertia to engage the planning process. As we set about this process, we have endeavored to keep it realistic, pragmatic, and resilient. The importance lies here in the process. The collaborative efforts within the process provide a unique opportunity to discover the true integration of business process within an organization. It is in exploring the causes and effects, the internal and external forces, impact points, and areas of overlap that we identify needs to bridge gaps in survival and recovery plans.

This resilience approach to business survival contains two principal sections: The business continuity plan, which focuses on maintaining critical business systems, and the emergency response plan, which protects people and facilities with proactive responses to disasters.

Business Continuity Plan

The goal of a business continuity plan is to assist businesses in organizing the tools and resources they will need to minimize the impacts of disruptive events by reducing business interruption losses, downtime, and associated financial impacts, while maintaining critical business processes and operations.

Business Continuity Management Process

- Sets continuity planning as a critical project
- Establishes business continuity planning policy
- Identifies committee members
- Sets requirements for awareness and training
- Assures regulatory compliance
- Establishes guidelines for the protection of people, equipment, and property
- Provides the framework for disaster response
- Approves final plan documents
- Maintains and implements the plan

The business continuity plan focuses on people, critical business processes, services, suppliers, and vendors. These critical factors are considered across a spectrum of essential business processes including IT/voice/data,

records, manufacturing and production, physical spaces, and support elements. Here we identify alternatives to normal operations, whether the disruption is loss of a facility or a critical component in a manufacturing process. Viable, tested alternatives will, when needed, ensure business survival.

Fundamental Goals

- Protection of people and assets
- Prevention of potential disasters
- Development, testing, and maintenance of the plan
- Elevation of disaster awareness

Six Stages

- Risk Identification and Assessment
- Business Impact Analysis
- Strategy Development
- Plan Creation
- Testing
- Plan Maintenance

Risk Identification and Assessment

This phase focuses on potential threats to an organization and extrapolates the financial impacts of each. Considerations in the phase include:

Threat Sources

Natural, man-made, or technical

Events by Type

Flood, hurricane, power loss, etc. A site survey conducted by a professional can help expose risks that are not readily identifiable. Surrounding properties and businesses can add risk; consider hazardous materials stored upstream or the attack of government offices housed in your building.

Outcomes

Consequences of an event for a critical business asset. Interruption in production, or inability to fulfill customer orders, for example.

Single Loss Exposure

Also called Potential Single Loss Cost, it's the value of an asset as exposed to a particular risk, i.e. the cost of a disruption that happens only one time.

Likelihood of Events

Annualized rate of threat occurrence. This is a mathematical formula that identifies the number of times a specific threat might occur in one year. Unlikely and highly unlikely probabilities can be rated with a fraction, or even zero.

Identify Risk Values

Multiply the Annualized Loss Exposure by the Annual Rate of Threat Occurrence. The result of this equation helps you rank threats in order of priority, based on the most likely and the most costly to your business. Understanding the threats, their likelihood, and their financial impact will help you determine how to best control the risk.

Risk Control Operations

Options for handling risk

- Risk Acceptance – Do nothing
- Risk Avoidance – Avoid the risk completely. For example, remove hazardous materials from the site and thereby eliminate the associated risk.
- Risk Reduction – Reduce the risk to acceptable level. In a flood zone, for example, locating valuables above the first floor could be a solution.
- Risk Transfer – Transfer the risk to another entity (i.e. insurance company)

Business Impact Analysis

Analyzing risk and related exposures identifies the financial and operational (non-financial) impacts of disasters or disruptive events.

Key components

- Identification of business critical processes
- Financial and operational costs
- Requirements for recovering critical business processes following a disruption

The information for this process is derived from interviews, surveys, and workshops involving the business staff. This process generates several fundamental business continuity planning concepts:

Maximum Tolerable Downtime

How long can downtime be tolerated without dire impact?

Recovery Time Objective

The length of time between a disruptive event and the recovery of systems and resources, such as computer systems, voice and data, manufacturing equipment, facility and associated building systems.

Strategy Development

This phase develops recovery options to be utilized when experiencing a disaster or disruptive business event. Generally, these options relate to physical workspace, IT systems, manufacturing and production, customer service, data, and critical business records. The output of this phase is a document that specifies costs for potential recovery options. This provides benchmark information for the organization's management team to choose the best combination of options and pricing to accommodate their accepted level of risk.

Plan Creation

Building on the prior phases, the plan document contains information required by the organization to recover critical business processes and hasten return to normal operation.

As the plan takes shape, guidelines will be developed for:

- Disaster declaration, including the individual(s) who have authority to make the declaration
- Procedures for assessing the event
- Initial response and notification of interested parties
- Contact information for all interested parties, including staff, vendors, and other resources identified in the plan
- Specific business functions to be handled outside of normal operations (i.e. customer service department) and the number of seats available for staff
- Recovery processes and procedures
- Normalization of work processes
- Routine updates and changes to the plan

Testing

Consistent testing and evaluation is essential to effective execution of a business continuity plan. Testing will help confirm the practicality and adequacy of the strategy as outlined. It will also highlight gaps, help train staff, and provide a benchmark for further improvements to the plan.

The methodology for testing generally falls into one of the following categories:

Checklist Test

The most frequently used and routine of all plan tests, the checklist test is performed by a designated individual or team to ensure all plan documents are in place and current.

Tabletop Test

A review of the plan with other team members, often in the form of a presentation describing specific scenarios to be discussed. Generally this type of test addresses one specific part of the plan at a time.

Simulation Test

Test the plan against specific disaster scenarios. Simulation may include testing of an alternate facility and may require certain business units to cease operations during the test.

Parallel Test

Carried out at alternate site, while normal operations continue at the main facility. Recovery is based on data retrieved from backup sources and manually recorded information from real transactions at the main site.

Full/Interruption Test

Assumes that all critical business processes have been disrupted. This testing may involve shut down of all, or some, critical business functions. In all cases, management should consider the cost and benefits of announced versus unannounced tests to the business and its clients or customers.

Plan Maintenance

Maintenance of the plan is a continual process that assures there is a constant state of readiness. Routine maintenance of the plan should be scheduled to minimize gap failure due to changes in personnel, equipment, IT systems, or regulatory requirements. Monthly or quarterly maintenance is appropriate depending on the size of the company. Triggers for updating the plan should also include major changes in personnel or equipment, and any actual event or test that provides new information.

Maintenance of the plan should be assigned to a specific person or team. Be sure to include instructions for distributing changes to the plan and for requiring those involved the keep their copy up to date. A check-list test can be a useful tool for making sure your plan is current and properly distributed.

Emergency Response Plan

An emergency response plan lays out procedures to deal with the immediate physical effects of a disaster. It is developed as a methodology for initial response, and is a complement to the business continuity plan.

Purpose

- Provide a managed, coordinated, and effective response to the immediate physical effects of an emergency
- Safeguard people, facilities, and other assets
- Reduce the likelihood that the business continuity plan will need to be invoked

Primary Objectives

- Preventing injury
- Providing shelter
- Evacuating the premises

Secondary Objectives

- Mitigate the threat of emergency situations
- Control or terminate the emergency as quickly as possible
- Prevent a minor incident from escalating to major disaster
- Familiarize employees and staff members with procedures to follow in the event of an emergency
- Protect environment
- Protect company assets
- Determine unsafe or hazardous conditions
- Minimize impact to the business

Emergency Response Plan Policy

A company policy regarding the emergency response plan reflects the company's commitment to safety and the interests of its staff, shareholders, clients, customers, and vendors. The business establishes a comprehensive organization-wide business continuity program to protect staff, and safeguard corporate assets and environment. It also ensures continuous availability of its products and services. The organization recognizes the need for emergency response capability as part of an effective overall business continuity program policy.

Scope

The emergency response plan policy should apply to all business facilities and locations. The individual plans are customized to the particular issues and conditions at each location. Teams at each site will define, approve, and implement an emergency response plan, which includes essential activities, procedures, and tasks necessary to ensure an effective response.

The broad scope of the plan is reflected in particular event responses such as fires, floods, hurricanes, earthquakes, chemical spills, and terrorist attacks. For these events, the plan will clearly spell out actions to take in regard to evacuation, coordination with public safety officials, utility shut-down, establishing alternate work sites, first aid, shelter in place, mitigation, and engaging the disaster restoration contractor and other key service providers.

Conclusion

There is an absolute need to plan for surviving and recovering from disasters. The responsibility to employees, shareholders, clients, and other parties with vested interests is clear. To minimize potential harm to people and minimize downtime are paramount objectives. A collaborative business environment employing processes and procedures from business continuity planning and emergency response planning will provide a company with its best opportunity to meet these objectives.

CIRCUMSPEX™

1555 Mittel Blvd, Suite S
Wood Dale, IL 60191
877-315-PLAN [7526]
www.circumspex.com