Business Continuity Planning

Business continuity is an organization's ability to maintain critical business functions during and after a disaster has occurred. Business continuity planning establishes risk management processes and procedures that aim to prevent interruptions to critical services and reestablish full day-to-day function to the organization as quickly and smoothly as possible. This checklist can serve as a framework to build your plan. The back page is a continuity planning example but every plan will be different to reflect the specific company.

Risk/Threat Analysis

- □ *Identify risks that can leave employees, customers, vendors, property and operations vulnerable.*
- □ *Which are mostly likely to occur? Weigh the probability of the event against the potential impact to your business and your readiness to respond.*

Business Impact Analysis

- □ *What people, places, equipment, processes and providers are critical to the survival of your business?*
- □ *What functions and resources, if interrupted or lost, could impact your ability to provide goods and services or meet regulatory requirements?*

Restoration Needs

- □ *Who and what are absolutely necessary to restore critical operations?*
- □ *Prioritize the need to restore each item after the event.*
- □ *Plan to use limited resources wisely.*

Prevention and Mitigation Controls

- □ *Plan and create processes to help prevent an event (e.g., fire from unsafe conditions, driver error)*
- □ *Plan and create procedures to reduce the impact or severity of an event (e.g., backing up files, software systems to the cloud if equipment goes down)*
- □ *As you build your plans, consider emergency response, public relations, resource management, and employee communications.*

Test, Exercise and Improve Your Plan

- □ *Review and update your plan regularly—at least yearly or any time critical functions, facilities, suppliers or personnel change.*
- □ *Train employees to understand their role in executing the plan.*
- □ *Test with live drills, simulations, or hypothetical walk-throughs to ensure the processes you've created work as intended.*

Most Common Threats to Business Continuity

- *Natural disasters (e.g., floods, tornadoes, lightning strikes)*
- *Manmade events (e.g., fires, explosions, chemical spills, utility outages)*
- *Malicious attacks (e.g., bomb threats, vandalism, civil unrest, robbery, armed intruders)*
- *Cyber attacks (e.g., computer viruses, cyberterrorism, ransom hacks)*
- *Loss of workforce (e.g., long-term disability or illness, epidemic, fatalities)*
- *Supply chain disruptions (e.g., equipment/materials availability, transportation delays)*
- *Human error (e.g., poor training, carelessness, misconduct, fatigue, substance abuse)*

Continuity Planning Example

THREAT TO BUSINESS	RISKS	IMPACT	PREVENTION/ MITIGATION
Cyber Security	• Technology fails or is compromised • Stolen information • Ransom attack	• PR if client info stolen • Locked out of digital content/systems	• Multi authentication log-in Insurance • Data backup and recovery • Test/train your staff • Cloud-based security
Disaster	• Fire office/shop • Flood • Weather (i.e. tornado)	• Total or partial loss • Interruption to operations • Lost clients due to service failure • Loss of insurance	• GPS tracking • Insurance • Equipment and keys stored separate from office
Death/Team Absence	• Potential change in ownership • Loss of institutional knowledge	• Impact on internal and external relationships • Lost clients due to service failure • Team morale if no succession plan is in place (confusion of roles, who's in charge now, etc.)	• ID key positions • Cross train roles • Establish org chart • Document processes/key tasks for each role • Life Insurance for biz partner or 2nd in command • Buy-sell agreement
Death/ Injury from Operations	• Fatality or major injury to the public or operator (i.e. vehicle accident)	• Impact on employee, other team members • Bad PR • Equipment being seized for investigation	• Insurance • Safe driver training • Mental health/crisis counselors • Public relations contact
Theft and Vandalism	• Exposure to loss from theft, overt mechanical damage and sabotage • Theft of financial, client or proprietary information	• Loss of production capacity • Insurance premium increases or loss of coverage • Compromised banking accounts	• Insurance • GPS tracking • Security protocols and policies • Backup equipment • Financial checks and balances
Active Shooter	• Current/former employee or unknown individual bent on destruction	• Disruption to operations • Potential injury or death to one or more employees	• Site security (i.e. locks/ access, cameras, firearms training) • Thorough background checks • HR training/management