Business Continuity & Disaster Recovery Planning

Business Recovery is about being able to continue business after a disaster and after a business disruption. A Disaster Recovery plan (DRP) features key action steps and contact information. Business Continuity Disaster Recovery Plans (BDDRP) are comprehensive in detailing actions from beginning to end. The following outlines basic steps for both and references in-depth sources for Main Street communities to use in planning.

This Tech Sheet is designed with the Main Street organization in mind:

Disaster Recovery: reactive and has steps to follow after a disaster—response time from seconds to days—zeros in on technology during recovery.

Resiliency: being able to resist and withstand issues; being impervious to potential disruption situation. Consider the analogy of a rubber band: if the business is resilient it will be stretched, but not broken—but if it does snap that's where Business Continuity kicks in to address the breakage.

Business Continuity: proactive and done prior to a disaster.
♦ Employee contact list
♦ Business contact list
♦ Vendor contact list
♦ Business Continuity also considers risk management and other planning an organization needs to stay afloat during this time

Business Impact Analysis (BIA) identifies the mission critical functions an organization must maintain or restore following an incident and the resources needed to support those functions.

A BIA should consider the following:
♦ Determine internal and external risks important to the Business Continuity Disaster Recovery (BCDR): both financial analysis and external risks important to BCDR.
♦ The organization should gain management support when putting together a BIA given the intensity of the process
♦ The organization uses risk analysis and BIA data to determine business continuity and disaster recovery strategies and the appropriate responses. Each strategy is turned into a series of actions that will help achieve operational recovery such as data replication, failing over to a cloud-based service activating alternate network routes and working remotely.

Basics on: How to build a Business Continuity (BC) and Disaster Recovery (DR) Plan
♦ Break plan into BC and DR components
♦ A BC Plan (BCP) contains contact information; change management procedures; guidelines on how and when to activate the plan and
♦ Step-by-Step procedures; and a schedule for reviewing, testing and updating
♦ A Disaster Recovery Plan (DRP) features a summary of key action steps and contact information and should consider the following:
  ♦ The defined responsibilities of the DR team
  ♦ Guidelines for when to use the plan
  ♦ DR policy statement & Plan goals
  ♦ Incident response and recovery steps
  ♦ Authentication tools
  ♦ Geographical risks and plan history
  ♦ Take into account staffing, ensuring that personnel able to execute the various steps of the DRP are always available to enact critical recovery tasks.
♦ BCDR plans are clear about the varying levels of risks to the organization

Business Continuity & Disaster Recovery Planning

- BCDR plans provide well-defined and actionable steps for resilience and recovery *NC Main Street can provide a sample Business/Organizational Continuity Plan: Vital Information Inventory in Excel at* https://www.ncmainstreetconference.com/organization
  - Protect the organization's employees, facilities and brand;
  - Include a communication plan;
  - And be comprehensive in detailing actions from beginning to end

First steps to building a BCDR Plan: Please see the Sample Continuity and Recovery Plan Template that is included with this Tech Sheet for a more comprehensive guide on establishing a plan.

- **Set a BCDR policy as a first step.** The policy aspect is often overlooked, but it's an important business continuity auditing item.
  - Policy sets the foundation for the process and typically covers the scope of the business continuity management system such as:
    - Which employees are responsible for it and which activities are performed such as plan development and Business Impact Analysis (BIA)
    - A policy might also establish a common set of metrics, such as key performance indicators and key risk indicators.
- **Gather a team and perform a risk analysis and a BIA**
  - Organization identifies the most critical aspects of the business, and how quickly and to what extent they must be running after an incident occurs.
  - After the organization writes the step-by-step procedures, the documents should be consistently tested, reviewed and updated.
  - Educate your board and others that are critical to your program on the plan. They must understand the plan.

- **Remember third parties and the services they provide** and keep them in the loop in order for them to understand how the plan is going to work. Examples of third parties to a downtown organization:
  - Banks
  - Insurance
  - City/State govt. (if organization is a non-profit and not a part of city/state govt.)
  - Key Vendors
  - Critical funders:
    - It is important to let key funders know that you have a plan and that you are still in business
    - Goal to convey to funder is confidence and their continued support still matters even if you may be shifting funding priorities during this time

Resources for this Tech Sheet:

Enterprise Community Partners, https://www.enterprisecommunity.org/blog/maintaining-business-continuity-during-covid-19-pandemic

International City/County Manager Association, https://icma.org/blog-posts/how-local-governments-are-working-keep-small-business-alive

TechTarget, https://searchdisasterrecovery.techtarget.com/Using-a-pandemic-recovery-plan-template-A-free-download-and-guide

Non-Profit Committee of New York, August 2018, https://www.nonprofitnewyork.org/