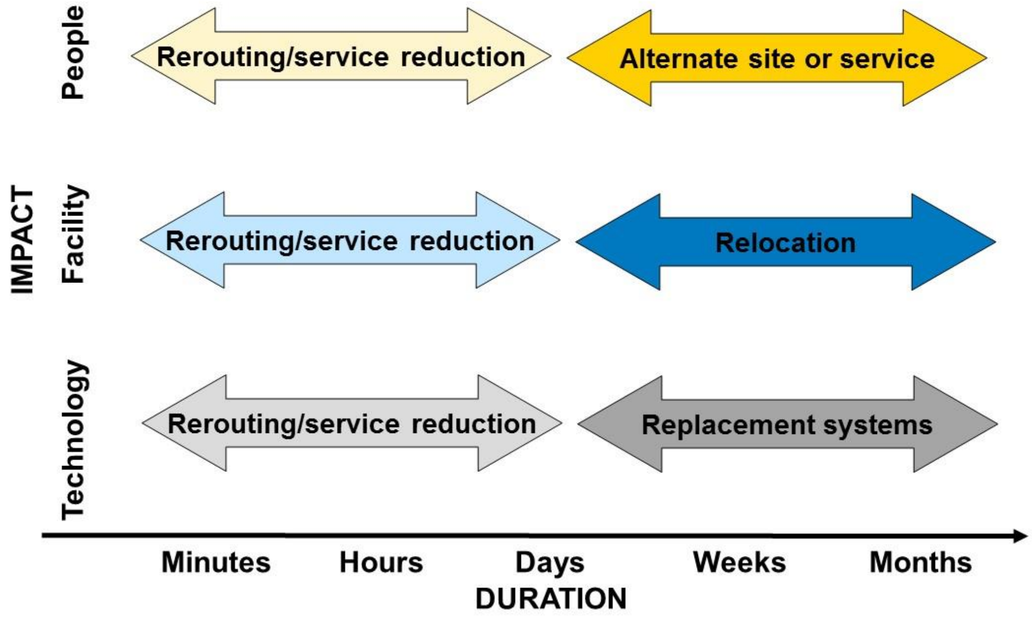
Business Continuity/Disaster Recovery Plan

Principles and Best Practices

A Business Continuity/Disaster Recovery (BC/DR) plan is critical to protect a contact center from a variety of events that can impact facilities (e.g., power outage, fire, storm, flood), people (e.g., virus, evacuation), and technology (e.g., network, systems, and/or power failure). The goals are:

- Minimize disruptions caused by (the most likely) events
- Continue operations when events occur
- Recover operations after catastrophic events

The graphic below provides a snapshot of the scope a plan should address.


People
Rerouting/service reduction
Alternate site or service
IMPACT
Facility
Rerouting/service reduction
Relocation
Technology
Rerouting/service reduction
Replacement systems
Minutes
Hours
Days
Weeks
Months
DURATION

Options to Enhance Continuity and Recovery

Contact centers have a number of options to enhance BC/DR, such as:

- Extra capacity
- Self-service – IVR, Web, mobile
- Multiple sites that back each other up
- Mirrored or partial duplication
- Network routing options
- Redundant technology
- Cloud solutions
- Remote/home-based agents and/or satellite sites
- Alternate temporary sites
- Third Party services
- Reciprocal agreements

Objectives of a BC/DR Plan

A BC/DR Plan should help a center achieve a number of important objectives:

- Identify and address business impacting events
- Define BC/DR team members (across IT and operations) and their roles
- Serve as a guide for the Business Continuity Team by providing procedures and identifying resources needed to assist in a timely response and recovery
- Identify employees and vendors that must be notified and engaged in the event of a disruption
- Complete and maintain an up-to-date Business Continuity Plan that addresses potential technology, facilities, or staffing issues
- Store and secure adequate backup materials off-site
- Guide comprehensive tests of the Plan and modify/update the Plan as a result of the tests
- Train assigned personnel (Business Continuity and Crisis Management Teams) on various aspects of the Business Continuity Plan, including adequate cross-training to reduce reliance on key personnel
- Enable everyone to respond effectively and consistently to an event or disruption

Keys to Success

Keys to success identified through lessons learned in writing, testing, and executing plans include:

- Strong sponsorship, leadership and vision
- A culture that values (and sees the value in) BC/DR Plans
  - Allocating resources
  - Investing in technology as appropriate
  - Testing
  - Updating
- A core team that makes decisions and can lead execution
  - A cross-functional team – IT and business – that works together to address technology, operations, and staff needs
- Consider all elements – people, technology, processes, facilities
- Consider external partners and dependencies as well
- Detailed, thorough documentation, routinely updated
- Effective communications across the organization
- Consider people first, and consider that they will consider their families first

Now is the Time!

There has never been a better time to develop or update your plan. Strategic Contact can help!

Our starter table of contents will help you think about what your plan needs to include. *Get started today*.

Sample BC/DR Plan Table of Contents

1. Document Version Control
2. Overview
    2.1. Business Overview
    2.2. Goals
    2.3. Scope
    2.4. Business Impact Matrix
    2.5. High-level Technology Architecture
    2.6. DR Options Matrix
    2.7. DR Overview
    2.8. Key Assumptions
        2.8.1. Recovery Facilities – alternate sites or services
        2.8.2. Replacement Equipment
        2.8.3. System and Data Back-ups
3. Team
    3.1. Crisis Management Team
        3.1.1. Names and Contact Information
        3.1.2. Command Center details
    3.2. Roles and Responsibilities
4. Declaration/Activation of DR Plan
    4.1. Responsibility for Activation/Deactivation
    4.2. Levels of Disaster
    4.3. Who, When (events)
    4.4. Disaster Scenario Timeline
5. Communications
    5.1. Critical Notifications of Office Closure
    5.2. Internal Checklist
    5.3. External Checklist
    5.4. Command Center
    5.5. Communications Channels, Messages, and Recipients
6. Execution Steps/Actions and Owners
    6.1. People Coordination
        6.1.1. Meeting/Gathering sites
        6.1.2. Transportation contacts between primary and backup sites
        6.1.3. Hotel/Motel reservations by backup site
        6.1.4. Expense procedures for backup sites
    6.2. Process
        6.2.1. Evacuation Checklist
        6.2.2. Employee Hotline
        6.2.3. Telephone Message Update Procedure
        6.2.4. IVR Update Procedure
        6.2.5. Web Site Update Procedure
        6.2.6. Mobile Update Procedure
        6.2.7. Social Media Update Procedure
        6.2.8. Post-Office Mail Forwarding to Recovery Site
    6.3. Technology
        6.3.1. Re-routing of Main/Toll Free Numbers
        6.3.2. Core Platform Failover Information by component
        6.3.3. Failover Procedures for Agents by Failed Component on Core Platform
        6.3.4. IVR System Recovery Procedures
        6.3.5. IVR Messaging Change Procedures
        6.3.6. Other Systems Change Procedures