

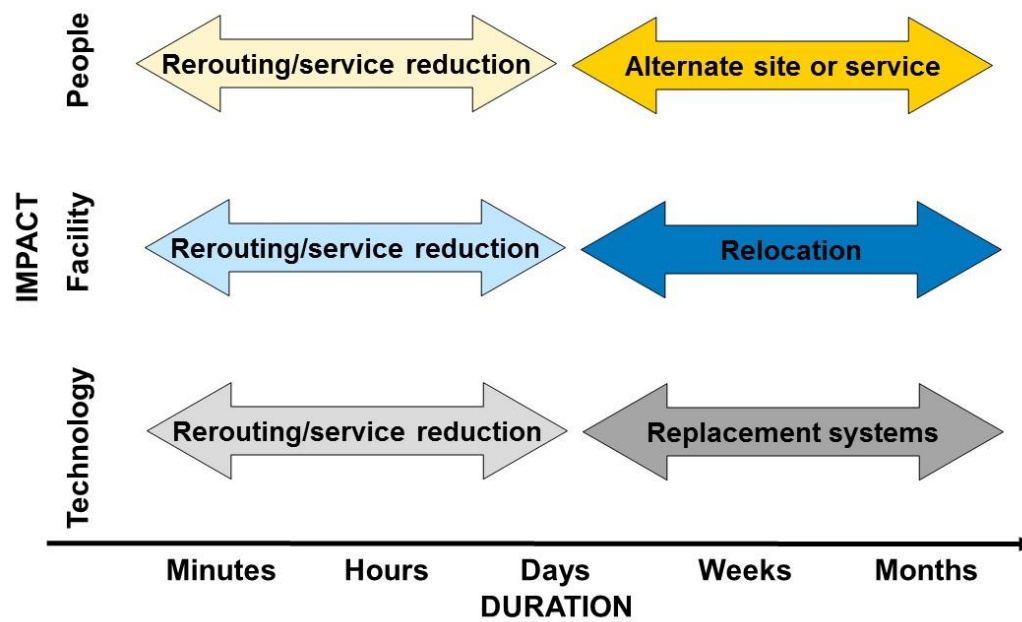
Business Continuity/Disaster Recovery Plan

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.



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



- 7. Full Recovery
 - 7.1. Facilities
 - 7.1.1. Checklist for Facilities Safety/Inspection Prior to Reoccupation
 - 7.2. People
 - 7.2.1. Transportation process to return staff to primary site
 - 7.3. Process
 - 7.3.1. Telephone Message Update Procedure
 - 7.3.2. IVR Update Procedure
 - 7.3.3. Web Site Update Procedure
 - 7.3.4. Mobile Update Procedure
 - 7.3.5. Social Media Update Procedure
 - 7.3.6. Post-Office Mail Forwarding to Recovery Site
 - 7.4. Technology
 - 7.4.1. How to Move Main/Toll Free Numbers Back to Primary Facility
 - 7.4.2. How to Ensure Core Platform Recovery
 - 7.4.3. Other Systems Recovery
- 8. Disaster Review
 - 8.1. Post Mortem Review
 - 8.2. Lessons Learned
 - 8.3. Update Documentation
- 9. Testing
 - 9.1. Top Scenarios
 - 9.1.1. Rerouting Contacts
 - 9.1.2. Building Evacuation/Relocation (and Remote Agents)
 - 9.1.3. Systems Down
 - 9.1.4. Return to Normal Operations
 - 9.2. Frequency and Responsibilities
 - 9.2.1. Bi-annual Testing Schedule
 - 9.2.2. Testing Roles and Responsibilities
- 10. BC/DR Plan Maintenance
 - 10.1. Events to Trigger a New Version or Update
 - 10.2. Responsibility
 - 10.3. Maintenance Tasks
 - 10.3.1. Informational Changes
 - 10.3.2. Process Changes
 - 10.4. Documentation Updates
 - 10.5. Version Control and Copy Access and Management
- 11. Appendix A – Employee Availability
- 12. Appendix B – Critical Business Functions Information
- 13. Appendix C – Other Contacts and Resources
 - 13.1. Internal
 - 13.2. Vendors
 - 13.2.1. Network
 - 13.2.2. Core Contact Center Technology Platform
 - 13.2.3. IVR
 - 13.2.4. Performance Tools
 - 13.2.5. CRM, KM, etc.
 - 13.3. Key Contacts
 - 13.3.1. Bank
 - 13.3.2. Utilities
 - 13.3.3. Emergency Management Agency
 - 13.3.4. Hospital
 - 13.3.5. Insurance Agent
 - 13.3.6. Post Office, FedEx, Other Shipping