

# DISASTER RECOVERY CHECKLIST

This document provides suggestions for executives to evaluate their current disaster avoidance plans or, should a plan not exist, provide directional measures to protect their information and communications systems. It is broken down into 3 functional areas: General Planning, Data Center Preparation and Communications System Continuance. This checklist does not cover human resources, insurance protection or crisis management communications.

## General Planning

### DR Team, Communication and Organizational Plan:

- Establish a Disaster Recovery (DR) functional team made up of mission-critical employees of major departments. Have a back-up person for each individual on the team
- Elect one spokesperson from the group for communication
- In the event of a multi-location organization each location should have a core team or representative that works with the corporate entity
- Risk Assessment - Identify key organizational risks in the following areas:
  - Information** - What information and information systems are most vital to continue to run the business at an acceptable level?
  - Communication Infrastructure** - What communications (email, toll free lines, call centers, VPNs, Terminal Services) are most vital to continue to run the business at an acceptable level?
  - Access and Authorization** - Who needs to access the above systems and in what secure manner (VPN, SSL, DR Site) in the event of a disaster?
  - Physical Work Environment** - What is necessary to conduct business in an emergency should the affected location not be available?
  - Internal and External Communication** - Who do we need to contact in the event of an emergency and with what information?
- Categorize the key risks by geographic location and the impact of each scenario to critical business systems, business continuance, employees, and accessibility

## Recovery Time Process Analysis

Stack rank all business applications, systems and if necessary, physical locations by Recovery Time Objective (RTO) and Recovery Point Objective (RPO). The Recovery Time Objective (RTO) is the maximum duration of time allowable for complete restoral after a disaster (or disruption) to maintain an acceptable level of business continuity. Recovery Point Objective is defined as the maximum tolerable period in which data can be lost (from its last update or refresh state) from an IT service due to a major incident. The most critical systems to maintaining normal operations during a crisis event will have a LOWER RTO/RPO and a higher stack ranking in priority. For example, the CRM and Order Entry System may have an RTO of 4 hours with the maximum sustainable data loss of 2 hours RPO making this a Priority 1 application whereas system drives and folders for documents may have a lower RTO/RPO of 8 hours and 24 hours.

Use the above Risk Assessment and Recovery Time Process Analysis to use as a guideline in creating your Disaster Recovery Plan objectives. These objectives can then aid in the completion of the remainder of this checklist and ultimately be used to establish guidelines to communicate to the organization.

## Data Center Checklist

### Cloud-based Data Centers and Applications:

- Produce a written recovery plan that is hosted remotely in a secure and redundant data center. Schedule and test your plan at least once per year or in accordance with regulatory/compliance requirements
- Ensure your deployment can properly meet the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) outlined by the committee in your planning process
- Validate your supplier's SLA quarterly. The goal should be 99.999% on core applications
- Ensure employees can access the hosted environment (both from within the business confines and remotely) during fail-over mode from the designated location/s

### Premise-based Data Centers:

- Produce a written recovery plan that is stored remotely
- Identify water entry areas (including roof exposure) throughout the building and have sandbags available
- Employ a non-water based fire-suppression system
- Install VESDA smoke detection and thermal detectors
- Ensure there are no windows in the data room
- Have a fail-safe alarm system
- Place high-temperature sensors on fire sprinkler heads if non-water based fire-suppression is unavailable
- Provide adequate cooling and ventilation
- Keep your data center above street level and place critical servers as high as possible in the rack. If you are in a single-floor building, raise your racks from the floor
- Employ multiple internet service/data providers and test for failover regularly
- Purchase uninterrupted power supplies and provide for generator access where necessary
- Determine how much fuel is required for a pro-longed outage
- If you don't own the property evaluate your landlord's systems and priorities for refueling
- Determine alternate ways to fuel the system should fuel trucks be unable to get to your area for several days:
  - Have back-up fuel contracts
  - Evaluate Natural Gas supply in your area
  - Contract for back-up emergency generators (roll-ups)
  - Parallel power (A+B) for rack hardware, preferably from two different sources
  - Multiple battery line ups with continuous power

## Data Back-up

- If you employ physical tape back-up take the 'human factor' out of your recovery. Tape back-ups should be removed daily (pending RTO/RPO objectives) and stored in a secure, easily accessed public building with at least 2-3 individuals having keys to the location
- Back-up data to a geographically distant location, either electronically, or ensure physical media is in a diverse location and can be transmitted in a time conducive with your RTO/RPO

## Communications Systems: Telephony

### Hosted Telephony Systems:

- Employ multiple internet providers and test for failover regularly
- Verify that critical phone numbers have the ability to Call Forward in an Unreachable condition
- Pre-deploy additional handsets to remote locations (other offices or home offices) to allow a distribution of calls in the event of an office shutdown

### Premise-based PBX:

- See all component of Premise Based Data Center
- Prepare a checklist of key telephony vendors to quickly (if possible) re-route calls to enable alternative ring-to locations and numbers
- Designated emergency personnel to take company and triage calls

## Communications Systems: Call Center

### General Items:

- Identify key business applications required and how call center staff will access these applications from alternative locations
- Identify any client, contractual, HR, legal or compliance requirements that must be met for staff working from an alternative location
- Identify critical call types that must be answered and determine mechanism to segregate those calls
- Determine minimum staffing requirements for critical call types
- Identify alternative location(s) to house the staff with the appropriate systems, phones, and work environment
- Ensure call center staff has the ability to reach/access the alternative location(s)
- Ensure administrative staff has the ability to remotely change call routing, messaging, and related call center functionality
- Ensure call center leadership has access to call center monitoring, reporting, and recording
- Determine situational specific routing and announcements that should be activated for critical call types

- Determine appropriate messaging for non-critical call types, how these calls will be routed, and who needs to be notified
- Identify the decision-maker(s) that will enact the disaster recovery plan and how that will be communicated to staff during business hours and outside business hours
- Identify reports that will be distributed, frequency, and recipients during the DR event
- Identify criteria for changing call routing, messaging, or moving call types between critical and non-critical classification

## About Evolve IP

Evolve IP is The Cloud Services Company™. Designed from the beginning to provide organizations with a unified option for cloud services, Evolve IP enables decision-makers to migrate all or select IT technologies to its award-winning cloud platform. Evolve IP's combination of security, stability, scalability and lower total cost of ownership is fundamentally superior to outdated legacy systems and other cloud offerings. Today, over 130,000 users across the globe depend daily on Evolve IP for cloud services like virtual servers, desktop services, disaster recovery, unified communications, contact centers and more.