

# DISASTER RECOVERY PLANNING

for Digital and IT Technology  
of a US based business



**In today's digital age** businesses are heavily reliant on digital and IT technology for their operations. However, disasters such as natural calamities, cyber-attacks, or system failures can cause significant disruption to these technologies, leading to loss of critical data, downtime, and potential loss of revenue. Therefore, it is essential for businesses to have a comprehensive disaster recovery plan in place to ensure the continuity of their digital and IT operations

**Unforeseen events can happen at any moment** and it's therefore important to have a disaster recovery plan in place before an unforeseen event occurs. Because so much can change so quickly, it is recommended to review and update the plan regularly to ensure it is up-to-date and relevant to the current business operations and environment.

## 7 Steps of creating and testing a disaster recovery plan:

### Step 1: Risk Assessment -

The team and the consultant identify potential risks and threats that could affect the digital and IT technology of the business. This could include natural disasters, cyber-attacks, power outages, hardware failures, etc.

### Step 2: Business Impact Analysis -

The team can now determine the impact of the identified risks on the business operations and prioritize them based on their severity.

### Step 3: Define Recovery Objectives -

The team and the consultant can now set specific goals and objectives for recovering IT systems, data, and operations after a disaster. This could include recovery time objectives (RTO) and recovery point objectives (RPO). Once determined, various providers can be engaged so as to determine which ones can offer the solutions that suit the organization best.

### Step 4: Define Recovery Strategies -

The team, the consultant and the provider or providers can now develop strategies to minimize the impact of disasters, such as data backup and restoration, cloud-based solutions, redundancy, and failover systems.

### Step 5: Document the Plan -

The team with support of the consultant can now create a detailed document outlining the disaster recovery plan, including roles and responsibilities, contact information, and step-by-step procedures to follow during a disaster.

It's helpful if the plan includes:

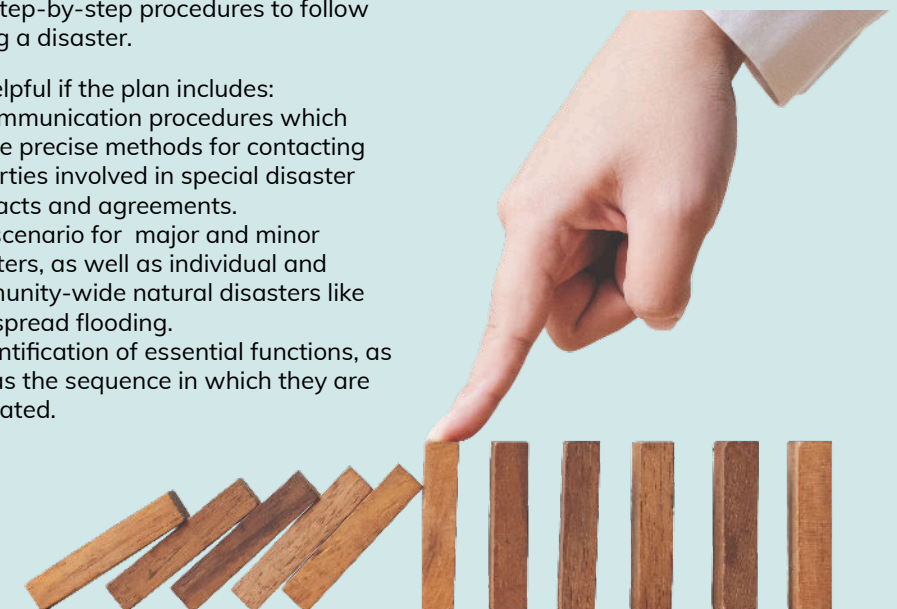
- Communication procedures which outline precise methods for contacting all parties involved in special disaster contracts and agreements.
- A scenario for major and minor disasters, as well as individual and community-wide natural disasters like widespread flooding.
- Identification of essential functions, as well as the sequence in which they are reinstated.

### Step 6: Test and Train -

The team can now regularly test the disaster recovery plan to identify any weaknesses and make necessary improvements. Additionally, the organization can now ensure that all employees are trained to follow the plan in case of a disaster.

### Step 7: Update and Maintain -

As the organization evolves, so should the disaster recovery plan. The team with support of the consultant can regularly review and update the plan to ensure it remains effective and relevant.



20 West 20th Street Suite 604  
New York NY 10011

<https://fcxnyc.com>  
Contact us at [inquiry@fcxnyc.com](mailto:inquiry@fcxnyc.com)