Investwell Business Continuity Planning (BCP) /Disaster Recovery (DR)

Introduction

Interruptions to business functions can result from major natural disasters such as earthquakes, floods, and fires, or from man-made disasters such as terrorist attacks, riots or war. The most frequent disruptions are less sensational—equipment failures, theft or sabotage.

Business Continuity Planning (BCP Plan), also known as Contingency Planning, defines the process of identification of the applications, customers (internal & external) and locations that a business plans to keep functioning in the occurrence of such disruptive events, as well the failover processes & the length of time for such support. This encompasses hardware, software, facilities, personnel, communication links and applications.

BCP plan is intended to enable a quick and smooth restoration of operations after a disruptive event. It includes business impact analysis, where each critical business function has been reviewed to determine the maximum allowable downtime before causing significant degradation to Excel Net Solutions Private Limited (Investwell) business operations. BCP plan development includes testing, awareness, training, and maintenance.

The BCP plan also defines actions to be taken before, during, and after a disaster.

Purpose

The plan has been developed to allow for Continuity of Business operations at a minimum level within Investwell facilities in Gurugram in the event of an emergency.

BCP Objective

- Protect personnel, assets and information resources from further injury and/ or damage
- Minimize economic losses resulting from disruptions to business functions Provide a plan of action to facilitate an orderly recovery of critical business functions
- Identify key individuals who will manage the process of recovering and restoring the business after a disruption
- Identify the teams that will complete the specific activities necessary to continue critical business functions
- Specify the critical business activities that must continue after a disruption
- Recover critical business functions and support entities

- Minimize damage and loss
- Resume critical functions at an alternate location
- Return to normal operations when possible

BCP Committee members and Contact details

Name	Designation	Phone	Email id
Sunil Jain	Director	9810154212	jains@investwellonline.com
Rohan Jain	Director	8368267066	rohan@investwellonline.com
Anuj Jain	Director	9971888720	anuj@investwellonline.com
Peeyush Srivastava	Chief Technical Officer	8882734913	peeyush@investwellonline.com
Arpit Wadhawan	Database Admin	8950308850	arpita.wadhawan@investwellonline.com

Recovery Management Co-ordinator (RMC)

Praveen Singh	Chief Security Officer	9910484322	praveen@investwellonline.com

The BCP Procedure is also sent to their mail ID. In case of emergency committee members can retrieve the data from their mail for acting toward the disaster.

Procedure - Business Continuity Plan

This is a disaster recovery plan for Investwell Data. The information present in this plan guides Investwell operation & data management and technical staff in the recovery of computing and network facilities and client data in the event that a disaster destroys all or part of the facilities. The primary focus of this BCP is to provide a plan to respond to a disaster that destroys or severely cripples Investwell operation & data computer systems.

The intent is to restore operations as quickly as possible with the latest and most up-to-date data available.

Disaster recovery plans are developed to span the recovery of data, systems, links and also include worst case scenarios such as:

1. Loss of access to facility
2. Loss of access to information resources

3. Loss of key personnel who are responsible for performing critical functions

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any storage media are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site

Designate Recovery Site / Alternate site / Backup site

The Three offices spread across 2 cities in India act as backup sites to each other. Each site is equipped to provide similar working environments as other centers. The offices are interconnected with redundant leased lines and LAN network.

Purchase New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The Investwell operation will rely upon emergency procurement procedures for equipment, supplies, software, and any other needs.

Begin Reassembly at Recovery Site

Salvaged and new components are reassembled at the recovery site. If vendors cannot provide a certain piece of equipment on a timely basis, then recovery personnel can make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Executive Management Team (EMT)

This group consists of members of BCP Committee, the Recovery Management Coordinator. The Executive Management Group decides to mobilize Investwell's recovery organization. This decision is based upon their best judgment in determining the extent and impact of the outage.

Recovery Management Co-ordinator (RMC)

The Recovery Management Coordinator (RMC) is the individual who manages the recovery operation. Throughout the recovery process, all recovery teams function under the supervision of the RMC.

IT Recovery Group

The IT Recovery Group manages the computer processing, internal/ external network connectivity and computer support requirements of the recovery effort.

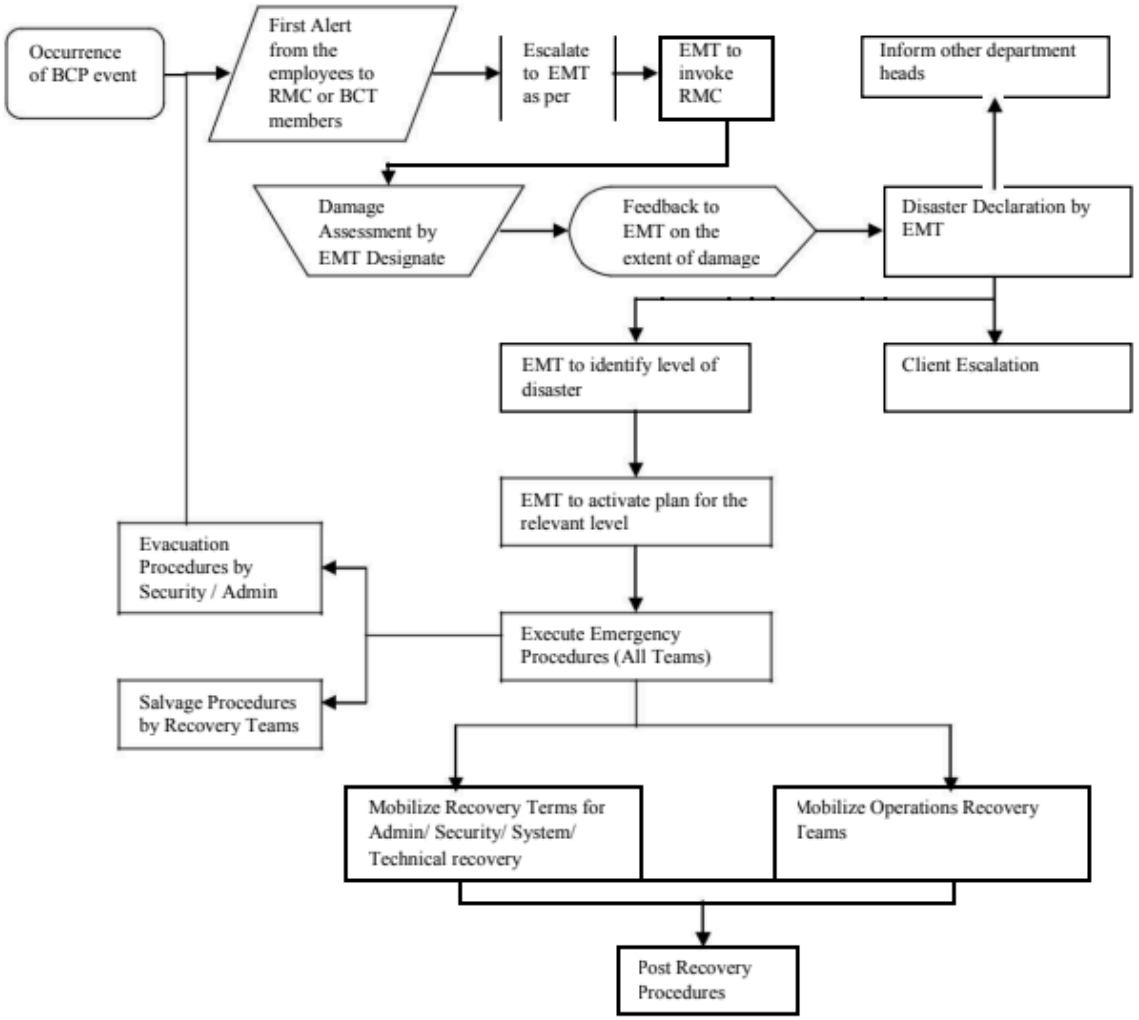
Logistics Recovery Group

The Logistic Recovery Group manages the administrative and logistical requirements of the recovery effort, and the performance of those duties and activities not directly related to the recovery of business functions.

Corporate Communication Group

Corporate Communication Group is responsible for communication with all Investwell employees and clients during recovery operations.

Investwell's Business Continuity Process



Restore Data from Backups

Data can be restored from other locations in case of any disaster. Multiple backup copies are stored on Amazon Web Service (AWS) servers, in different locations.

Potential Causes of service interruptions

1. Server Hardware Failure
2. Loss of data/software
3. Failure in communication link components
4. Loss of power supply
5. Loss / inaccessibility of other location

Geared for eventuality

Server Hardware Failure	Company user Net Magic servers for hosting its applications. A disaster at company's site will not affect server availability in any manner. Net Magic users highest standards of BCP-DR plans.
Loss of Data/Software	Adequate backup maintained to recover loss of data Every 24-hour backup of database taken in AWS Backup media to be tested at least once in two months Copies of backup maintained in secure multiple locations.
Failure in Communication link components	Failure of communication link components at Investwell's end will not affect availability of its hosted services platform access in any way. Only support services will be interrupted. For all communication problems at Investwell's end: Equipments (router, connections hub) are checked and rectified for problems detected Fully configured backup routers Alternate backup link facility in case of failure in dedicated link in one location
Loss of Power supply	Loss of power at Investwell's site will not affect availability of its hosted services platform access in any way. All office sites are equipped with fuel based generators for continuous power supply. UPS system for 2 hrs. to avoid interruption in working.
Loss/inaccessibility of other location	Square up of position or important client orders can be managed form alternate locations.

Prevention

As important as having a disaster recovery plan is, taking measures to prevent a disaster or to mitigate its effects beforehand is even more important. This portion of the plan reviews the various threats that can lead to a disaster, our vulnerabilities, and the steps we should take to minimize our risk. The threats covered here are both natural and human-created:

- Fire
- Flood
- Cyclones and High Winds
- Earthquake
- Computer Crime
- Terrorist Actions

Sabotage Fire

The threat of fire in office premises is typically real. The Building is equipped with a fire alarm system. Hand-held fire extinguishers are placed in visible locations throughout the building. All Staff are trained in the use of fire extinguishers.

Flood

None of the offices are on ground floor, thus risk due to flood is very much limited.

Cyclones and High Winds

Offices are based in Delhi NCR. Probability of cyclones is close to zero, and very sever cyclone, if any can only have marginal impact on the operations. Due care and preventive measure appropriate are carried out.

Earthquake

The threat of an earthquake in Delhi NCR area is medium to low but should not be ignored. An earthquake has the potential for being the most disruptive for this disaster recovery plan. Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do large scale building
Repairs.
Since all hosted services are hosted on AWS on multiple remote sites, earthquake may result in disruption of support services only. In case ofearthquake at one office location, staff in other city can continue to provide services, and critical staff from one city can be moved to another city location within a period of 12 hours.

Computer Crime

Investwell has best in industry measures to safeguard from Computer Crime. Detailed policies
Are available at: https://joinsuperset.com/security.html
All data and servers are hosted on AWS. More on AWS security at:
https://aws.amazon.com/security/

Terrorist Actions and Sabotage

Terroristic action and sabotage are potential risk under the circumstances in all the offices in big cities. To prevent such occurrences Investwell has a system in place whereby each office will permit entry on verification of fingerprint and due care is taken to provide adequate security.

Training

Training seminars addressing business continuity in are conducted on a regular basis. Also awareness programme is conducted to educate management and senior individuals who will be required to participate in the project.

The objectives of Business Continuity Planning training are:

- Train employees and management who are required to help maintain the Business Continuity Plan
- Train employees and management who are required to execute various plan segments in the event of a disaster

Testing and Evaluation

The response to each threat situation is tested periodically to assess the preparedness of the organization to execute the recovery plans. Some of the threats that occur frequently are tested in due course of business and, hence are not tested specifically. Others, however, require testing and for them, a disaster scenario is assumed and the team representatives "walk through" the recovery actions checking for errors or omissions. Persons involved in the test include the Recovery Management Coordinator and members of various recovery teams.

An ongoing testing programme is established. However, special testing is considered whenever there is a major revision to Investwell operation or when significant changes in hardware or communications environments occur. The Recovery Management Coordinator is responsible for analyzing change, updating impacts on the plan and for making recommendations for plan testing.

The Team Leaders and the Recovery Management Coordinator review the test results, discuss weaknesses, resolve problems and suggest appropriate changes to the plan.

Author: Anuj Jain (Director)
Last revised: 19th March, 2023
Version 1.0