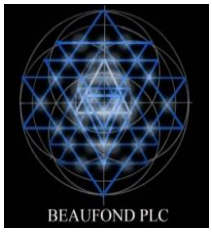


Business Continuity Plan

Beaufond Plc

Preface:

The concept of Business Continuity Planning (BCP) has over the past few years, become a major business management requirement. It is the responsibility of the board to support business sustainability under normal as well as under adverse operating conditions. The internationally recognized Standard ISO 17799 and the BS7799 requires that a managed process be implemented for developing and maintaining business continuity throughout an organization. The subject has been well researched and a great deal of documentation and advice is available.

Disaster Recovery Planning is also known as BCP (Business Continuity Planning) or BRP (Business Resumption Planning). It has become generally acknowledged that the planning process should go beyond catering for major disasters such as earthquakes, fire and flood, to include the less threatening emergencies like power outages, server downtime and limited access to the workplace, which start out as minor emergencies, but can quickly escalate to full blown disasters. The BCP is intended to be used in addition to the Emergency Preparedness and Response Plan.

Beaufond Plc formulated an excellent plan by creating systems of prevention and recovery to deal with potential threats to the company. In addition to prevention, the goal is to permit ongoing operation, before and during execution of disaster recovery. This plan identifies key resources and needs to ensure that business may continue, perhaps in a limited capacity, or how the business will fully recover should the disaster be catastrophic.

This plan includes information such as:

- Critical assets
- Critical operations
- Key suppliers, Customers and contractors
- Alternate business Process / location

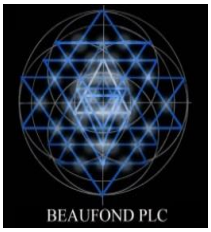
This plan identifies and prioritizes the key hazards that may affect business operations, and outlines preparedness and mitigation activities. This plan also includes operational procedures to respond effectively and efficiently to an incident. This goal of this procedure is to ensure life and safeties are secure in response to a disaster.

The board strongly believes that a business continuity plan to be successful, all employees—even those who aren't on the continuity team—must be aware of the plan. Hence it is important that all the employees, stake holders and customers etc., should understand the company's BCP and have the capacity to recover back immediately with less damage from the disaster if any.

24.04.2019 DIRECTOR & CEO

BEAUFOND PLC

Contents:



I. Definition:

Business continuity planning (BCP) is the process involved in creating a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected, and are able to function quickly in the event of a disaster. The BCP is generally conceived in advance and involves input from key stakeholders and personnel.

BCP involves defining any and all risks that can affect the company's operations, making it an important part of the organization's risk management strategy. Risks may include natural disasters—fire, flood, or weather-related events—and cyber-attacks.

Once the risks are identified, the plan should also include:

- Determining how those risks will affect operations.
- Implementing safeguards and procedures to mitigate the risks.
- Testing procedures to ensure they work.
- Reviewing the process to make sure that it is up to date.

BCPs are an important part of any business. Threats and disruptions mean a loss of revenue and higher costs, which leads to a drop in profitability. And businesses can't rely on insurance alone because it doesn't cover all the costs and the customers who move to the competition.

II. Business Continuity Plan:

Beaufond Plc's BCP is a well-developed preparatory and planning method which allows the company to continue its operations in the event of any natural disaster or event which can lead to the loss of facilities and utilities, unavailability of personnel, or accessibility to other resources necessary to the company's operations.

Beaufond Plc develops several steps for solid BCP which are given below:

They include:

1. **The Business Impact Analysis:** Here, the business identifies functions and related resources that are time-sensitive.

2. **Recovery:** In this portion, the business implements steps to recover critical business functions.

3. **Organization:** The Company created a continuity team headed by the Chef of the Risk Management of the Company which devises the plan to manage the disruption.

4. **Training:** The continuity team is trained regular interval of time and tested. Members of the team have complete exercises that go over the plan and strategies.

Beaufond Plc has a checklist that includes key details such as emergency contact information, a list of resources the continuity team members, backup data and other required information is stored on line for ready reference.

Along with testing the continuity team, the company also tests the BCP itself for several times to ensure it can be applied to many different risk scenarios. This helps to identify any weaknesses in the plan which is then be identified and corrected.

III. Business Continuity Impact Analysis

An important part of developing a BCP is a business continuity impact analysis. It identifies the effects of disruption of business functions and processes. It also uses information to make decisions about recovery priorities and strategies.

Beaufond Plc annexed a sample of the Threat / Vulnerability Worksheet to help run a business continuity analysis. The worksheet is fully completed by business function and process managers who are well acquainted with the business.
This worksheet summarizes:

- The impacts—both financial and operational—that stem from the loss of individual business functions and process.
- Identifying when loss of a function or process would result in the identified business impacts.

This analysis helps the company to identify and prioritize the processes that have the most impact on the business' financial and operational functions.

IV. Emergency Preparedness and Response Plan:

This plan includes information such as:

- Preparedness
- Hazard identification and assessment
- Employee education and training
- Drills and exercises timelines and plans for your business
- First aid kits
- Disaster supply kits

Response

- Evacuation procedures
- Fire procedures
- Shelter-in-place procedures o

Staff notification

- Information gathering procedures
- Incident management

Potential Hazard:

This information includes the company's Emergency Preparedness and Response Plan, however reiterating key potential hazards in the Business Continuity and Recovery Plan helps to focus on the types of incidents from which the company needs to recover, taking in to account to look inside and outside the business as well as the surrounding community - staff, suppliers, and customers and the depth of interruption.

V. GOALS AND OBJECTIVES

The goal of the plan is to prevent loss of life, reduce property damage and minimise impact on the overall business i.e.:

- Minimise and support the number of decisions that must be made during a crisis;
- Minimise the dependence on any specific person during the crisis;
- Minimise the need to perform crisis actions by trial-and-error when a crisis occurs; and
- Minimise the need to develop new procedures, programs or systems during a crisis so that all components necessary to assist the site during a crisis are documented and stored off-site, ready for use.

The overall objective of the plan is to provide the information and procedures necessary to: -

- Rapidly respond to a disaster or emergency situation;
- Notify necessary trained personnel;
- Assemble business recovery teams;
- Rapidly recover services to clients; and
- Rapidly resume normal business functions.

VI. CORPORATE RESPONSIBILITIES:

(a) CRISIS CONTROL UNIT

CONCEPT

The concept of a Crisis Control Unit /team/ department requires careful explanation. It is not exist as a day-to-day ongoing business entity, but the members come together as a team, to orchestrate all matters relating to an actual or potential disaster and the ongoing task of Disaster Recovery Planning, including the implementation of disaster prevention activities. The Team members include some of the most senior members in the organisation and are ultimately responsible for all aspects of disaster prevention and disaster recovery, relating to Beaufond Plc.

Any team, even at this level, requires an internal orchestrator to ensure that the team operates effectively despite ongoing day-to-day responsibilities that are not disaster related. With this in mind a senior management role has been created in the group viz. Chief Risk management Officer (CRM) as Crisis Control Officer (CCO). The CCO is a senior person with a good understanding of the business and business practices together with a detailed knowledge of the Information Technology on which the business has become so dependant. The CCO together with his/her deputy, is responsible for the development, ongoing maintenance and testing of an effective Disaster Recovery Plan and disaster prevention measures. The CCO must ensure that all members of the Crisis Control Unit understand all aspects of the Business Continuity Plan and are fully aware of their respective responsibilities in their area.

Whilst the Crisis Control team carries ultimate responsibility for all facets of disaster recovery, specific responsibility lays in the "across all business units in various countries" disaster related activities. The Crisis Control team, through the Crisis Control Officer will also be responsible for ensuring that each Strategic Business team has developed a business specific Business Continuity Plan which clearly states and covers the key business processes of the department and is in line with the corporate Business Continuity Plan, as determined by the Crisis Control team.

(b) RISKS AND BALANCES

The plan assumes that the required quorum of the Crisis Control team remains functional, in a post disaster situation, even in a major disaster if any Crisis Control team is not functioning or lost. Hence the company has small groups of well-trained CC teams in various areas instead of having a wide / large team in one area.

(c) CRISIS CONTROL UNIT MEMBERS

Title	**Major DR Function**
Chief Executive Officer	Leadership and group PR
Chief Risk Management Officer	Crisis Control Officer
CFFO	Financial Support
Head of R&D	Database Administration
Chief HR	Staff matters
GM, Operation	Communication

(d) EXTERNAL CRISIS CONTROL CENTRE

Given a major disaster where the site is destroyed or inaccessible, the Crisis Control Centres are at:

- The outsourced offsite backup environment.
- The home of the Chief Executive Officer; or
- The home of the CCO.

(e) BUSINESS SUPPORT UNITS (BSUS)

Along with the Crisis Control Unit, the Business Support Units also have "across all business units" functionality. In all major disaster situations the specific business units are reliant on the performance of the BSUs. Each BSU has defined areas of responsibilities in the event of a disaster. However in the event of any unplanned circumstances, the BSU's will fall directly under the control of the Crisis Control unit in terms of rearranged priorities or other changes to the plan.

The Business Support Units are shown below, together with senior management.

BSU (Directorate)	**Position**
Executive Office	Secretary
IT & System	Manager
Finance	Assistant
Human Resources	Assistant

VII. COUNTER DISASTER STRATEGY

Beaufond Plc implements standard security options.

From the BCP perspective the organisation has implemented logical access control, fire detection and fire prevention for the server room in line with accepted best practices.

1. KEY PERSONNEL DEVELOPEMNT

Personnel development is an ongoing organisational activity based on:

1) Effective recruiting;
2) Training;
3) Succession planning; and
4) Fast tracking of highly promising staff.

The above processes become effective 0over time and cannot be replicated in a disaster environment. At best, key personnel can be replaced with trusted outsourced resources, internal or external to the group.

2. RISK ANALYSIS

The ongoing risk analysis process under the control of the Crisis Control officer is to:

- Consider all potential disaster scenarios and potential impact on the business;
- Rank each scenario in terms of potential eventuality;
- Discard scenarios that are never likely to occur, or that we can do nothing about;
- Categorise and rank remaining disaster scenarios in terms of impact on the business; and.
- Define each potential disaster within each scenario category.

3. DETERMINE VULNERABILITY TO CONTROLLABLE FACTORS

Common threats include: Epidemic

- Earthquake
- Fire
- Flood
- Cyber attack
- Sabotage (insider or external threat)
- Hurricane or other major storm
- Power outage
- Water outage (supply interruption, contamination)
- Telecomm outage
- IT outage
- Terrorism/Piracy
- War/civil disorder
- Theft (insider or external threat, vital information or material)
- Random failure of mission-critical systems
- Single point dependency
- Supplier failure

4. Threat / Vulnerability Worksheet

Note: Priority risks are rated on a scale of 1 to 3, where 1 represents the highest level of risk

Possible Threat	Likelihood				Vulnerability				Priority Risks
	H	M	L	NA	H	M	L	NA	
ELEMENTS									
Earthquake			√				√		3
Tornado / Heavy Winds		√				√			3
Flooding		√					√		3
Fire	√				√				1
Severe Thunderstorm	√				√				1
Hail Damage		√					√		3
Lightning	√				√				1
Drought		√					√		3
PEOPLE									
Medical Outbreak		√			√				1
Civil Unrest		√				√			1
Industrial Action / Strikes		√			√				1
Denial of Access	√				√				1
Computer Crime	√				√				1
Industrial Sabotage		√					√		3
Bomb Threat / Blast		√			√				1
Transportation Accident		√				√			2
Unauthorised Access		√				√			2
Individuals Undocumented Knowledge	√				√				1

Possible Threat TECHNOLOGY	Likelihood				Vulnerability				Priority Risks
Telecommunications Failure									
Telephone Line Failure	√				√				**1**
Network Failure	√				√				**1**
Power Shortage / Failure	√				√				**1**
UPS Failure		√				√			**2**
Computer Hardware Failure									
Workstation Failure	√						√		**2**
Server Failure	√					√			**1**
Printer Failure	√					√			**2**
Computer Software Failure									
Upgrade compatibility	√					√			**1**
Over Customisation	√					√			**2**
Unlicensed Software		√				√			**2**
E-mail Retention & Deletion		√			√				**1**
E-mail Content	√				√				**1**
Document Loss or Destruction									
Legal Documents		√			√				**1**
Employee Records		√			√				**1**
Service Level Agreements		√			√				**1**
Data Backups & Restores &	√				√				**1**
Hacking & Virus Attack	√				√				**1**

5. COUNTER DISASTER MEASURES

Physical Access

A secure physical access system is in place where all staff and any visitors are signed in upon entrance to and exit from the Company premises.

Health and Safety

It is the responsibility of the Facilities Supervisor and the Health and Safety Committee to ensure compliance with the *HSE & CSR Policy* of Beaufond and to have at least one fire drill per annum.

Emergency telephone numbers for Police, Fire Department and Ambulance will be displayed throughout the building.

Fire Prevention

The premises security complies with Fire Safety Regulations. At present there are fire hoses and fire extinguishers at each end of the floors. A fire detection and prevention system has been installed in the server room, and the walls (dry walling) have fire retardant properties.

VIII. MAINTENANCE OF THE OVERALL BCP

The development of a detailed Overall BCP is an ongoing exercise. The business changes over time as does the staffs complement. It is therefore vital that any given recovery plan reflects the current status of the business. The counter disaster strategy is also reviewed regularly.

(a) BUSINESS IMPACT ANALYSIS

Members of the BCP project team led by the Crisis Control Officer regularly conduct in depth interviews and discussions with the senior management in each strategic business unit. This is done in order to ascertain the vulnerability of each unit to each applicable disaster scenario together with the potential business impact. These interviews are key to the maintenance of an effective recovery plan for the strategic business unit covering each disaster category.

(b) MINIMUM (POST DISASTER) REQUIREMENTS

It is equally important to establish the minimum requirements for each disaster category, in the post disaster situation. Relocation of staff to the off-site recovery centre may be necessary after a major disaster, in which case the facilities will be significantly more limited than the current environment.

IX. RECOVERY TEAMS AND ROLES

The cross-unit recovery functions will be orchestrated by the Crisis Control Unit, Each strategic business unit must however supply its own recovery teams for each disaster category, from the purely business perspective. The following considerations will apply:

- Definition of the roles in each recovery environment;
- Select staff and reserves to fill roles; and
- designate team leadership responsibilities

X. PUBLIC RELATIONS

Most disasters will impact clients, suppliers and staff in other units within the organisation. In the event of a major disaster the Crisis Control Unit will issue certain notification and assurances, such as press releases etc. in accordance with the agreed plan.

Outside of the corporate issues, each business unit must have plans and contact lists in place in order to communicate effectively with clients and suppliers in each disaster scenario.

XI. DEVELOPMENT OF THE PLAN

The documented outcome of the business impact analysis supported by the implemented counter disaster strategy, places the DRP project team and each business unit in a position where meaningful recovery plans can be developed for each disaster category.

Essentially the plan for each unit is based on:

- Rapid access to emergency contact lists;
- Clear and concise "to do" lists that have been prioritised, with responsibility allocations, for each disaster category and level;
- Well-trained and responsible recovery teams; and
- Communication, communication and more communication.

Training of the members of the recovery teams is an essential function of each business unit manager in association with the Crisis Control Officer.

XII. TRAINING

Training is an important aspect of the plan. It is crucial that the crisis control unit, business support units and business unit recovery teams have an intimate and up to date knowledge of the recovery procedures related to each disaster category. It is fair to say that the more complete the training, the less panic there will be in a disaster situation.

XIII. DISASTER DECLARATION

The members of the Crisis Control Unit will ensure that each member has the latest version of the recovery plans. If possible and required, the Crisis Control Unit will visit the site to evaluate the full extent of the disaster.

A disaster will be declared at the appropriate level and the recovery plans will be triggered. It is assumed that evacuation and relocation will be necessary.

XIV. ANNOUNCEMENT AND NOTIFICATION

Depending on the number of members of the Crisis Control Unit present, many of the following actions will take place concurrently:

- The member representing Human Resources may be mandated to arrange staff counselling or other actions to comfort and re-assure staff;
- Press releases will be prepared in line with the recovery plan and the appropriate media notified;
- Major corporate clients will be contacted and advised of the disaster and the recovery process, either immediately or at the earliest suitable time;
- The off-site disaster recovery centre will be notified in line with laid down procedures;
- Metro file will be instructed and authorised to deliver the latest back-up canisters to the off-site recovery centre, in accordance with agreed and documented procedures;
- The recovery team leaders and/or deputy leaders of each business support unit and strategic business unit will be contacted and notified of the disaster declaration.
- The recovery team leaders will be instructed and authorised to notify the members of their respective recovery teams and proceed with the implementation of their sections of the documented disaster recovery plan;

XV. DIRECTORATES

The individual Directorates are responsible for the development of their own business specific BCP plans, including notification of unit specific clients and service providers. From an overall recovery perspective it is important that each business unit provides the Crisis Control Unit with accurate and detailed post disaster requirements, as the entire plan is largely developed around these requirements and priorities.