



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

-

-

GIAC Security Essentials  
Certification (GSEC)  
Practical Assignment  
Version 1.4c  
Option 1

Corporate Business Continuity Program (BCP)  
in global economic climate:  
Best Practices Guide

Submitted by: Jackie Teh  
Location: Penang, Malaysia  
February 25th, 2005

## ABSTRACT

Disaster may strike anytime! One never knows when a disaster may strike, what form it may take, its severity, how long it may last, or its impact. Therefore it is essential for us to prepare ourselves before any emergency happens to recover the business operation in corporate as soon as possible after a disaster. In today global economic climate, a business and government organizations a survival always depends on some mission critical systems based continuously within IT. Organizations have to consider the security and resilience of their people, systems, assets and networks, as this all contribute to generate revenue and also allow the organization to stay competitive in the digital networked economy. [1]

This paper focuses on giving organization guidelines for the best practices in a Business Continuity Program (BCP). This paper begins with an introduction on Business Continuity, then briefly explains about why, where, when, how Business Continuity is needed; and who are the team members running the Business Continuity Program. The paper will also discuss about characteristics of BCP and Management Support for BC. The BC Program model including its life cycle and 3 main activities, risk assessment, prepare & response to emergency and test response to emergency will be discussed in this paper. Lastly, the document also includes of recommendations on Best Practices for Business Continuity Program in Corporate environment.

© SANS Institute 2000-2005

## TABLE OF CONTENTS

### COVER PAGE

### ABSTRACT

i

### TABLE OF CONTENTS

ii

### LIST OF FIGURES

iv

### 1 INTRODUCTION

1.1 INTRODUCTION TO BUSINESS CONTINUTIY	1
1.2 WHY BC IS USED	2
1.3 WHO IS THE TEAM MEMBERS IN DOING BCP	2
1.4 WHEN BCP IS NEEDED	3
1.5 WHERE TO DO BC WHEN DISASTER OCCURS	4
1.6 HOW TO TO IMPLEMENT BCP	4
1.7 CHARATERISTICS OF BDRP	5

### 2 management support

2.1 MANAGEMENT COMMITMENT	5
---------------------------	---

### 3 BUSINESS CONTINUITY PROGRAM MODEL

3.1 what is bcp life cycle	6
3.2 analysis phase	7
3.3 planning phase	8
3.4 development phase	8
3.5 production phasE	8
3.6 the 3 major activities use to develop and maintain bc	8

### 4 business continuity RISK ASSESSMENT

4.1 RISK ASSESSMENT	10
4.2 RISK MITIGATION	10
4.3 IMPACT SEVERITY DEFINITION	11

### 5 PREPARE AND RESPONSE TO EMERGENCY

5.1 Team CONTACT LISTS	11
5.2 TEAM ROLE & RESPONSIBILITIES	11
5.3 emergency response plan	12
5.4 Business recovery Plan	13
<b>6 TEST RESPONSE TO EMERGENCY</b>	
6.1 self audit for bc plans	14
6.2 bc drills PLaN	14
<b>7 rECOMMENDATIONS</b>	
7.1 RECOMMENDATIONS ON BEST PRACTICES	15
<b>CONCLUSION</b>	15
<b>REFERENCES</b>	16

## LIST OF FIGURES

Figure 1 “Who is in BCP participants list”	3
Figure 2 Importance of BDRP characteristics	5
Figure 3 Business Continuity Model	7
Figure 4 Summary of BCP Life Cycle & its activities	9
Figure 5 Risk Assessment Worksheet	10
Figure 6 Risk Mitigation Worksheet	10
Figure 7 Impact Severity Definition Sample	11
Figure 8 ER member Role & Responsibilities	11
Figure 9 ERP checklist	12
Figure 10 BRP checklist	13
Figure 11 Drill plan	14

# 1 INTRODUCTION

## 1.1 INTRODUCTION TO BUSINESS CONTINUITY PROGRAM (BCP)

According to wikipedia.org, the free encyclopedia on the web, Business Continuity Planning is a methodology to create a printed manual that a organization will use to resume partially or completely resume interrupted critical function(s) within a predetermined time after a disaster or disruption. [2]

Whereas the Disaster Recovery is the ability of an infrastructure to resume operations after a disaster has passed. [3]

Business Continuity is not just about disaster recovery. Business Continuity is a business process that requires you to proactively evaluate risks and develop mitigation plans. Anything that, if disrupted, threatens your ability to do business is a risk to be considered. For instance, if you are dependent on a single supplier or you are located in an area subject to power brown-outs or black-outs, you should be considering your options.

No one can anticipate what will cause a disaster. It is not the cause but the impacts on businesses and the community that have to be considered and planned for. The BCP is to ensure we can keep the core business running during these unexpected times. It is an integral approach to doing business. By consolidating BCP into all of your decisions and programs, you can achieve a sustainable program with less effort!

The Business Continuity Program targeted to provide continuous availability as required in any emergency and extraordinary event. It develops business continuity strategies and tactics, identifies document recovery requirements for critical business applications, and also manages backup and archival processes for critical data.

Before an incident or disaster happens, organizations should proactively review threats, risks and their impacts to primary business functions; implement contingencies; develop emergency response processes and develop business recovery processes. During a crisis happens, organizations will be able to respond to the emergency and fix the problem, and to keep the critical functions operational.

The 4W (Why, Who, When and Where) and 1H (How) are used to explain the Business Continuity in next section.

## 1.2 WHY BC IS USED

Expect the best, but prepare for the worst. In today evolving global economic climate, there are many hidden risks and threat which is not visible sometime.

The 911 terrorist attacks which happened in 2001 was wake up call for management to start looking into this Business Continuity Planning. Most recently, one of the biggest natural disaster, the 9.0 magnitude earthquake and resulting tsunami affected many countries and has killed at least 135,000 peoples since 26 Dec 2004.

Therefore, a Business Continuity Program is good measure to ensure organizations benefits in the following areas: [4]

- To ensure employees safety as employees are the most valued resource of any organization.
- To reduce the impact of business events on customers.
- To protect the corporate assets.
- To fulfill insurance, legal and regulatory requirements.
- To proactively prevent negative impact beyond the organization.
- To show an effective and efficient governance to stakeholders, markets and the media.
- To defend the organization's reputation and public trust.

[4]

## 1.3 WHO ARE THE TEAM MEMBERS IN DOING BCP

In today's globalized economy today, most organizations successful accomplishments are delivered by team works effort. Therefore a vital Business Continuity Program also requires a group of people to accomplish its objective. People are the most important element in the Business Continuity Program. People are responsible for risk assessment analysis, business impact analysis, decision making, process development, implementation, program rehearsal, program auditing, and program enhancements.

In this paper, several main players creating a BCP are briefly stated below. Organizations are not constrained to recommend players, in fact the size of the team depend on the size and nature of the business organization in the environment.

*Business Continuity Program Manager* is the main person whom is responsible for developing and maintaining the continuity program for the organization. He or she has to ensure the existence of continuity plans for all critical business units are in place. He/She also needs to provide the



direction for the corporate business continuity program and make sure each business unit has up to date and tested business continuity plans. He or she also influences all business organization projects including business continuity plans in their development phases. He or she negotiate service agreements with external organization to provide business continuity to the organization. [5]

*Business Continuity Analyst* is another important key player to work with business unit representatives to complete a business impact analysis, documenting business functions and preparing Business Continuity plans. He/She analyze and document that business impact of critical business functions in Business Continuity program. He or she also coordinate the Business Continuity Testing process and work with each business unit representatives for verifying the program quality. He or she has to provide training assistance to business users in the corporate. His or her participation in customer relationship meeting is good for establishing and maintaining an effective working relationship with the business community in an organization. [6]

*Business Continuity Trainer* is responsible for developing training methodologies, materials and delivering the full user training for the staffs in the organization. He or she will evaluate the methodology and align with BC program manager and BC analyst to close the gap and improve the business continuity process. [7]

This paper also suggested the following template to keep track of those functional group(s), person name, and group's information.

Group Name	Individual(s) Engaged	Individual(s) Contact Number	Group's BC Information

Figure 1 "Who is in BCP participants list"

#### **1.4 WHEN BC IS NEEDED**

The Business Continuity (BC) is needed when there is a disruption happened to the organization's business at any time for the following events: [8]

- Application Errors (such as OS crash Database corrupt)
- Hacking Activity (such as unauthorized people gain access)
- Hardware Failure (such as Hard disk crash)

- Human Errors (such as unpleasant employee sabotage or strike)
- Interruption of commercial power supply (such as power trip in plant)
- Malicious Software Activity (such as Trojan Horses, Worms, Viruses)
- Natural disasters (such as Flood, Earthquake, Land Slide, Tsunami)
- Terrorist Attacks (such as 911 incident in 2001) [8]

## 1.5 WHERE TO DO BC WHEN DISASTER OCCURS

Organizations have several options to consider when selecting their recovery alternatives. Large corporations usually can consider to set up different physical sites in addition to a single primary site. For instance, corporation A can have primary data center at site A in any location in United States, and then set up an alternate site is planned at site B at any country in Asia or Europe. The primary and alternate sites setup process shall be classified as confidential and information shall only available to internal corporate Business Continuity Program staffs. Smaller organizations can consider setting up their recovery facilities with a business continuity service provider, or in other words, outsourcing to a vendor to perform the data backup and recovery in BC process.

Both options above have their advantages and disadvantages. The BCP manager has to analyze, and decide which option to use prior to implementation.

The advantages of having alternate recover sites at different physical location are:

- Business backup and recovery requirement are clearly defined and able to be executed by internal BC staffs if there is any emergency happens.
- Confidential information which is highly classified within the organization is handled by internal staffs compare to outsourcing.

Some disadvantages of this option are:

- The cost to setup redundant sites with similar equipment, network capacity, as well as the training of skilled support personnel may be high.
- Annual maintenance may be high if the scale of critical business application is growing.

Advantages of using a vendor'ssupplied backup site are:

- The total cost (including maintenance) may lower as organizations are only required to pay a lump sum fees to vendor annually.

Disadvantages when using a vendor's supplied backup site are:

- The confidentiality threat may negatively impact an organization's competitive advantage if confidential data were to be leaked to a competitor by the vendor either intentionally or unintentionally.

## 1.6 HOW TO IMPLEMENT BCP

Section 3 of this paper will discuss in more detail about the BCP model.

## 1.7 CHARACTERISTICS OF BUSINESS DISASTER RECOVERY PLAN

Many people assume the success of a Business Disaster Recovery Program (BDRP) success is dependent on increased funding for maintenance and development of the BDRP. In the article from the Continuity Central, a survey respondents were asked to rank the overall importance or unimportance of 10 BDRP characteristics. Below is a table showing the top 5 characteristics of a Business Disaster Recovery Program. [8]

Management Support	3.23
Easy to Communicate to Others	3.19
Comprehensive	3.13
Employee Awareness	3.10
Employee Training	3.00

Figure 2 Importance of BDRP characteristics on a scale of 1 to 5, 1 being "entirely unimportant" and 5 being "entirely important." [8]

## 2 MANAGEMENT SUPPORT

### 2.1 MANAGEMENT COMMITMENT

Referring to the survey for characteristics of the Business Disaster Recovery Plan in section 1.7, the importance of management support is the highest importance among 5 characteristics. [8]

Therefore the success of BC program is depends heavily on management's

commitment and the determination to be prepared for disasters that could potentially interrupt the business. The management of corporate shall create Corporate Business Continuity strategies, to understand the different needs for support, and to demonstrate their commitment to Business Continuity.

Management should require BCP as a compulsory class for new hires in an organization to attend. A refresher training class should become a compulsory class for existing employees at least once per year. Through training classes, the employee awareness about the BCP can be increased.

Here are some of tips to help an organization get started:

- Understand your organization's current level of readiness by identifying your organizations' core business functions and their priority. Determine what BC plans exist today and determine gaps (if any) for further improvement. It is good to consider all the areas needed to run your business and perform a Business Continuity impact analysis.
- Establish BC as part of good discipline for ensuring the group has a strong link the Business Continuity Program, to create clear ownership of the Business Continuity function, which fully supported by General Manager, defining a schedule for implementing BC activities in the corporate.
- Locate a high level BC strategy in place by identify the best approach to address the gaps and place the priorities, draw out a timeline for the program, to ratify the strategy with group management, to ensure that BC team you have choose understands the management priorities, timelines, available resources and budget.
- Review and update your plans quarterly. The business climate in this IT age is rapidly changes, therefore reviewing all key contact information to ensure it is up to date, performing an internal audit on all of the business continuity plan components in each business units.
- Performing an annual risk and impact assessment to be certain that the plans are as robust as possible. Maintain a revision log for all updates in a control document and incorporate information from actual disasters and discuss for area of improvements.

### **3 BUSINESS CONTINUITY PROGRAM MODEL**

A Business Continuity Program model is discussed in this section.

#### **3.1 WHAT IS BCP LIFE CYCLE**

Every model or system in the real world has its life cycle and BCP is not an exception. The figure 3 has illustrates a Business Continuity Program Life Cycle with 3 main activities which require management support. Without management support, employee training and awareness, any good model may not be able to execute effectively and efficiently. The BCP Life cycles are divided into 4 phases, namely is *Analysis, Planning, Development and Execution*. The 3 main activities are *Risk Assessment, Prepare & Response and Test Response*.

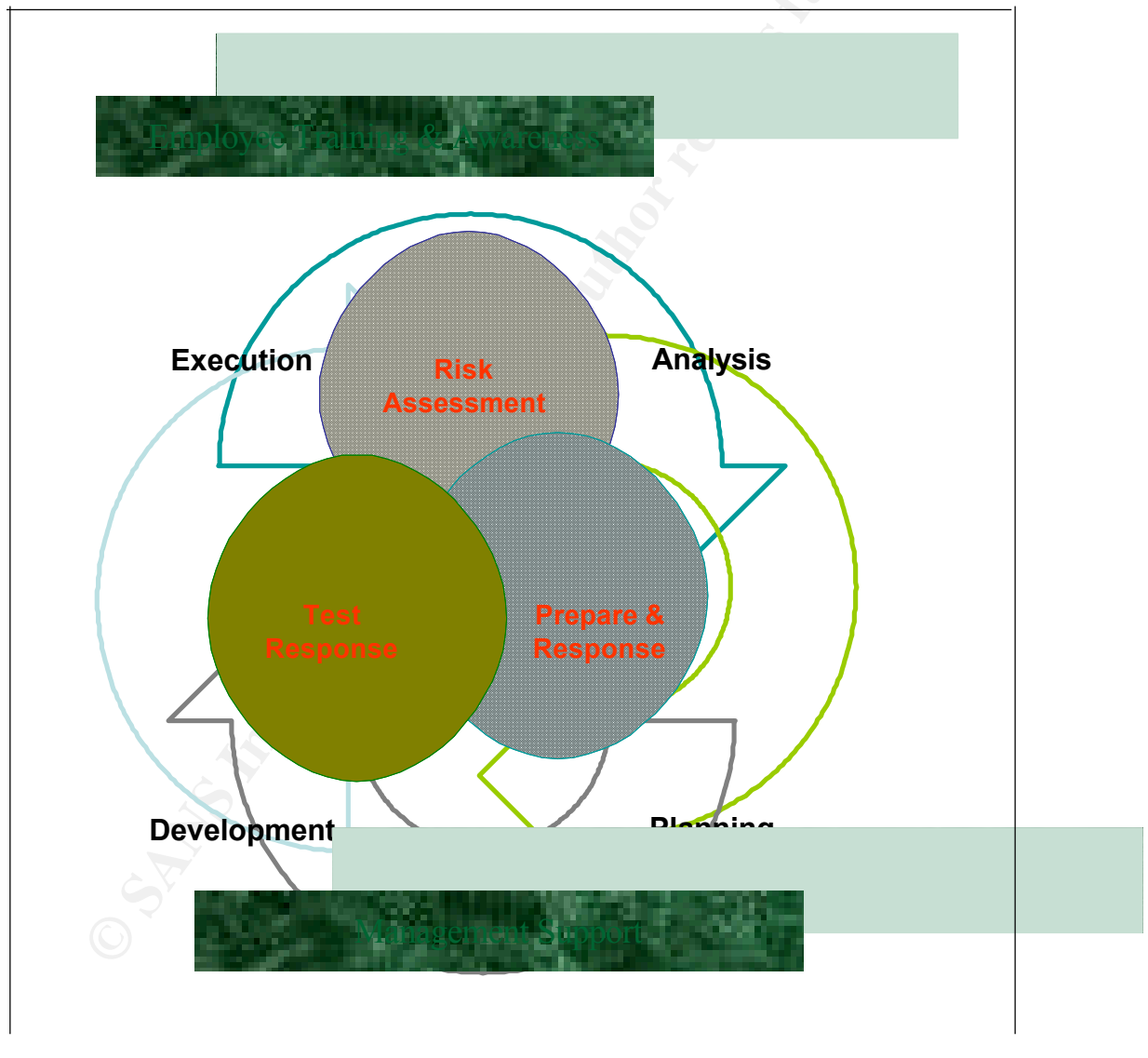


Figure 3 Business Continuity Model

### 3.2 ANALYSIS PHASE

During the Analysis Phase, a project team details the high-level objectives

and determines the business value of each objective. An analysis of these objectives will provide the basis for the Business Continuity Program. The main activities in this analysis phase are to identifying high-level alternatives for Business Continuity (BC), including of capital and headcount required, to adjusting Return of Investment (ROI) program as a result of implementing BC requirements, and to completing a risk assessment. The results of this phase is BC alternatives, an updated ROI and a completed risk assessments.

### **3.3 PLANNING PHASE**

In the Planning Phase, the BC team defines specific technologies for development. In addition, the BC team also defines and maps out BC plans by identifying a strategy for ensuring Business Continuity, creating disaster recovery architecture, and listing all resources that required supporting the BC strategy. The following BC activities shall be included in the Planning Phase of the BC strategy, identifying failure points that may require BC plans, identifying resources needed to support the strategy, and designing and validating disaster recovery architecture. The result recovery support model and resources required for developing, deploying and maintaining the disaster recovery and BC effort.

### **3.4 DEVELOPMENT PHASE**

In the Development phase, the team builds the technologies required for the BC program, and also builds in the capability for disaster recovery. The activities in this phase include building the BC Disaster Recovery capabilities, to testing and validating the capabilities and documenting and validating all related plans.

### **3.5 EXECUTION PHASE**

During the Execution phase, the BC team shall update fully all plans and transfer all supporting documentation to the operations owners. The activities and results for this phase are included of all related documentation, stored in a central depository, all plans are transferred to appropriate owners, and an initialization of the audit process.

### **3.6 THE 3 MAJOR ACTIVITIES USE TO DEVELOP AND MAINTAIN BC**

*1<sup>st</sup> activity is Risk Assessment.* Assessing risks is essential prior to creating a solid BC process. It is also as part of an ongoing BC maintenance effort.

Analyze each known threat to the business to determine their impacts and to minimize that impact if possible for a new BC plan. Performing yearly evaluations and environmental scans to identify new and emerging threats, and then determine additional impacts and changing the similarities for an existing BC plan. The key result of this activity are risk assessment, risk mitigation strategy and risk mitigation plan.

*2<sup>nd</sup> activity is Prepare Response.* Create an Emergency Response Plans and Business Recovery Plans to reduce the severity of impact, ensuring the Crisis Communications are defined, selecting and training the Response Management Team. The key results of this activity are readiness of the Emergency Response Plan, the Business Response Plan and Mitigation of Risks.

*3<sup>rd</sup> activity is Test Response.* Every plan without testing may not reflect their effectiveness and efficiency. Therefore in this activity includes conducting drills to test the Business Continuity response, exercising the organization's emergency communication plan and emergency leadership. The audit of Business Continuity response is included in this activity. The key result of this activity are a review of the internal audit review, performance of test drills, and the BC environment audit.

The summary of section 3 is summarized in Figure 4 below

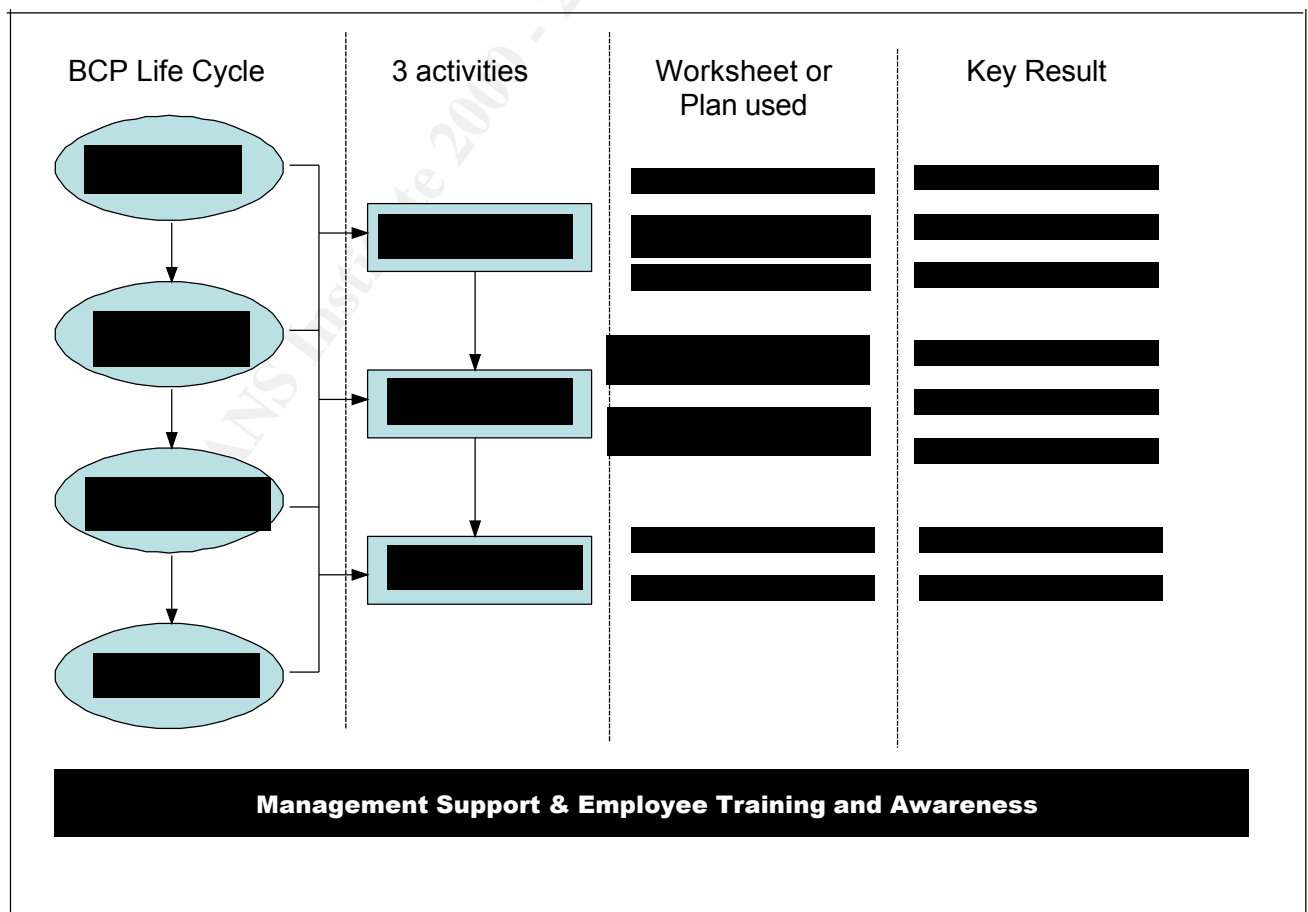


Figure 4 Summary of BCP Life Cycle and its activities

## **4 BUSINESS CONTINUITY RISK ASSESSMENT**

This process is used to perform risk assessment of the organization. It is followed by a development of a risk Mitigation Plan to reduce risks that could cause the business failures before any disaster occurs in the environment.

### **4.1 RISK ASSESSMENT**

The Risk Assessment worksheet illustrated in Figure 5 below is to identify potential risk prior to any disaster occurring in the business corporate environment.

Purpose	Write down the purpose here
Objective	Write down the objective here
Scope Range	What is the scope range covered in this business?
Organization Impacts	What are the description of the impact and their duration of the threat? Refer to Impact Severity Definition for the impact category
Step 1	Identify the Primary Business Functions in this step here
Step 2	Examine the Primary Business Functions in this step here
Step 3	Verify Prior Risk Assessment in this step
Step 4	Determine the Unique Impacts in this step
Step 5	Determine which Existing Resources are in place
Step 6	Identify the potential Risk Mitigation Area in this step
Step 7	Continue to next Risk Mitigation Worksheet

Figure 5 Risk Assessment Worksheet

### **4.2 RISK MITIGATION**

The Risk Mitigation worksheet illustrated in Figure 6 below is used to mitigate potential risks from the risk assessment.

Step 1	Review Risk Assessment in this step
Step 2	Risk Mitigation Mapping to identify Impact Severity and their Similarity in this step
Step 3	Identify risk mitigation strategy in this step
Step 4	Determine the feasibility of the option and the ROI (Return on Investment) in this step
Step 5	Make the Risk Mitigation proposal in this step
Step 6	Complete the Risk Mitigation Plan in this step
Step 7	Periodically review and evaluate the Risk Mitigation Plan with Top Management until all the gaps are closed or improved

Figure 6 Risk Mitigation



## Worksheet

### **4.3 IMPACT SEVERTIY DEFINITION**

The standard impact severity definition is defined in the figure 7. It is depends on level of criticality to the organization to determine the risk versus impact in the risk assessment and risk mitigation plans.

High	The most severe impact is defined in this category
Medium	The average severe impact is defined in this category
Low	The minor impact is defined in this category

Figure 7 Impact severity definition

## **5 PREPARE AND RESPONSE TO EMERGENCY**

In this section, the emergency response plan and checklist is discussed.

### **5.1 TEAM CONTACT LISTS**

A contact list should include the Emergency Response Team, the Business Response Team and the Emergency Management Team Contact lists must be prepared and documented prior to any crisis. This document shall treat as confidential under the organization's privacy policies. The usage of this contact list shall limited to an authorized personal during any emergency happens in corporate. The contact list shall include the role of the person, his or her primary contact information, and secondary contact information during any emergency.

### **5.2 TEAM ROLE & RESPONSIBILTIES**

Every team has a defined roles and responsibilities in each organization. The Emergency Response Team, Business Recovery Team and the Emergency Management Team also need to have clearly defined role and responsibilities. Below is a sample of ER team member roles and responsibilities. The list can be modified to include position that is specific to your organizations needs. The roles and responsibilities should be clearly define before a crisis occurs. The Emergency Response Team is focused on crisis response at the immediate stage whereas the Emergency Management Team focused on decision making to ER Team and the Business Recovery Team is focused on the process to recover the business operation in the shortest time. The organization's management should give

*Response Management Team* a full decision making authority during crisis. This is to ensure the unit of command is properly executed in the crisis to avoid conflict during crisis incident. [10]

Role	Responsibilities
ER Team Manager	Manages all crisis/issue during crisis
Communication Leader	Drives to create communication material for internal employee, whereas the external audience has to communicate through Public Affair
Position 3	Responsibilities #3 (you can added that specific to your organization'

Figure 8 ER Team member roles & responsibilities

### 5.3 EMERGENCY RESPONSE PLAN

The emergency response team is a group responsible for immediately responding to an incident at the beginning of the disaster. A sample of Emergency Response Plan is provided below to briefly touch on their action, and it can be modified to include any items that are specific to your organization's requirements. This paper does not include Emergency Management Team Plan however the organization can design according to their own requirements. [10]

Emergency Response Execution	<ol style="list-style-type: none"> <li>1. Execution is triggered promptly</li> <li>2. Emergency Response Team members contacted</li> <li>3. Emergency Response Team meeting location confirmed</li> <li>4. Emergency Response Team report event status</li> <li>5. Establish links to ER and Business Recovery Teams</li> </ol>
Emergency Response Team Activities	<ol style="list-style-type: none"> <li>1. Problem Identified and Damage Assessment</li> <li>2. Recommend solutions and communicated to Business Recovery and Emergency Management Team.</li> <li>3. Replacement of Software or Hardware (if necessary)</li> <li>4. Data Recovery from offsite records (or from recover service provider, depends on organization backup strategy)</li> <li>5. Testing replaced equipment and ensure it is run able</li> </ol>

Back to Normal Operations	<ol style="list-style-type: none"> <li>1. To validate readiness to return to normal operations such as data integrity, safe working environment, hardware availability.</li> <li>2. To communicate the "Back to Normal" status to Emergency Management Team</li> <li>3. Critical Business processes resumed</li> <li>4. Call Meeting and Report the results to Emergency Management Team</li> <li>5. Update the improvement plans</li> </ol>
---------------------------	--

Figure 9 ERP checklist

## 5.4 BUSINESS RECOVERY PLAN

Business Recovery Team is responsible to recover the business operation within the shortest possible time after the disaster. A sample of Business Recovery Plan is provided below. It can be modified to include any items that are suited to your organization's requirements. [10]

Business Recovery Execution	<ol style="list-style-type: none"> <li>1. Execution is triggered promptly</li> <li>2. Business Recovery Team members contacted</li> <li>3. Business Recovery Team meeting location confirmed</li> <li>4. Business Recovery Team report event status</li> <li>5. Establish links to Emergency Management Teams</li> </ol>
Business Recovery Team Activities	<ol style="list-style-type: none"> <li>1. Alternate workarounds executed</li> <li>2. Recommend solutions and communicated to Emergency Management Team.</li> <li>3. Replacement of Software or Hardware (if necessary)</li> <li>4. Data Recovery from offsite records (or from recover service provider, depends on organization backup strategy)</li> <li>5. Tested replaced equipment and ensure it is run able</li> </ol>
Back to Normal Business Operations	<ol style="list-style-type: none"> <li>1. To validate readiness to return to normal operations such as data integrity, safe working environment, hardware availability.</li> <li>2. To communicate the "Back to Normal" status to Emergency Management Team</li> <li>3. Document the Damage Assessment &amp; Recovery Costs</li> <li>4. Call Meeting and Report the results to Emergency Response Team</li> <li>5. Update the improvement plans</li> </ol>

Figure 10 BRP checklist

## 6 TEST RESPONSE TO EMERGENCY

Every system without audits, tests and drills will not be able to evaluate its capabilities, gaps and area of improvements. Therefore, it is essential that a periodical self audits, tests and drills should be conducted in the corporate environment prior to any crisis happening. The following section provides an example of a self audit for Business Continuity Plans, and BC drills plan.

### 6.1 SELF AUDIT FOR BUSINESS CONTINUITY PLANS

In the self audit, there are several questions to review the result of BC plans result. The following are some of sample questions sample. You can define more to suit your organization's self audit requirement. [10]

- Is the review implemented at least one per year?
- How many types of result validation are done?
- How corrections or improvements are implemented?
- Who does the reviews?
- Who are the participants?
- Is the plan getting input from all internal business partners?
- Do you have drills for the employees, systems and processes?
- What processes are used to organize, run and assess drills?
- Are the improvement plans being closed?
- Are the results of BC plans mitigating a risk?
- More to go (per your organization's self audit requirement...)

### 6.2 BC DRILLS PLAN

No plan in this world is perfect if no rehearsal being done prior to the event. In this section, the BC Drills plan is discuss here. Organizations can design their own scenario to suit their drill's requirements and expected the results. This template is for guideline that purpose. The drill crisis shall consists of when and where the drill is to be performed, who are the participants, the drill scenario and details, the current issue in the drill, and lastly is the expected test results from the event. [10]

*Drill Date*

*Drill Time*

*Audio Bridge Meeting Number*

*Meeting Room Number*

*Participant Name List*


<b>Item #</b>	<b>Drill Plan Area</b>	<b>Drill Plan Information</b>	<b>Remarks</b>
1	Disaster/Crisis Scenario	Date, Time, Short Description of the Disaster simulated	comment#1 is write here
2	Scenario Details	Description of the scenario details such as building evacuation, network connectivity, IT services availability	comment#2 is write here
3	Current Issue	Description of existing issue in the simulated scenario	comment#3 is write here
4	Assumptions made	Description of the related assumptions made to the scenario	comment#4 is write here
5	Affected Scope Range	Description of the scenario affected scope range	comment#5 is write here
6	Initial Briefing	Brief Communication on the scenario to floor and begin test here	comment#6 is write here
7	Expected Test Result#1	Short Description of Expected Result#1	comment#6 is write here
8	Expected Test Result#2	Short Description of Expected Result#2	comment#8 is write here
9	Expected Test Result#3	Short Description of Expected Result#3	comment#9 is write here
10	Expected Test Result#4	Short Description of Expected Result#4	comment#10 is write here

**Figure 11 BC DRILLS PLAN TEMPLATE**

## **7 RECOMMENDATIONS**

### **7.1 RECOMMENDATIONS ON BEST PRACTICES**

A lots of BC related articles has been published on the Internet. This section lists some recommendations on Business Continuity Program Best Practices. [11]

- Optimize the use of vendor disaster recovery facilities to handle peak processing requirements. (With a proper of information security agreement with vendor to be signed)
- Identifying disaster recovery requirements compliance in production acceptance processes.
- Define standards on the level of disaster recovery required by each category of applications from critical, moderate, office and etcs.
- Communicate with stakeholders about the disaster recovery requirements and expectations.
- Ability to do integrated testing and recovery across each business unit using IT capabilities.
- Employee Awareness and Training must be implemented through periodical drills.
- Test and evaluate BCP at least twice times per 12 months.
- Update BC plans, emergency management team contact list, emergency response team and the business recovery team contact list at least twice a year. [11]

## **CONCLUSION**

Today business has moving into globalization climate. Every disaster have no smell, it may strike at any time at anywhere. Therefore it is vital for business corporate to have business continuity program proactively prior to

any disaster may strike to reducing or avoiding severe impact or losses to the employee's life, assets, and organization's reputation. There will be an additional cost for corporate to plan, setup, implement, testing and maintaining the Business Continuity Program however the benefits returns are intangible. The best practices are some recommendations in the section 7 are for Business Continuity Program, and it is not the limit to every organization to follow exactly, however organization may come out their best process for their own IT and business environment. These best practices are for guide purpose. It is well worthy for an organization having such plans to ensure business is recover within shortest time and creating return on investment to their stakeholders and continue to excel in their reputation to the public.

## References

- [1] Business Continuity, Overview from global IT and networking services  
URL: [http://www.btglobalservices.com/business/global/en/products/business\\_continuity/index.html](http://www.btglobalservices.com/business/global/en/products/business_continuity/index.html)
- [2] Definition of Business Continuity Planning at wikipedia  
URL: [http://en.wikipedia.org/wiki/Business\\_continuity\\_planning](http://en.wikipedia.org/wiki/Business_continuity_planning)
- [3] Definition of Disaster Recovery at wikipedia  
URL: [http://en.wikipedia.org/wiki/Disaster\\_recovery](http://en.wikipedia.org/wiki/Disaster_recovery)
- [4] Business Continuity and Crisis Management at the Business Continuity Institute articles.  
URL: <http://www.thebci.org/frametrial.html>
- [5] The description of position of Business Continuity Manager  
URL: <http://www.continuitycentral.com/jobs386.htm>
- [6] The description of position of Business Continuity Analyst  
URL: <http://www.continuitycentral.com/jobs380.htm>
- [7] The description of position of Business Continuity Trainer  
URL: <http://www.continuitycentral.com/jobs382.htm>
- [8] Introduction to Business Continuity Planning, Practical paper at SANS  
URL: <http://www.sans.org/rr/whitepapers/recovery/559.php>
- [9] Business continuity explored...refer to figure 1a in the article  
URL: <http://www.continuitycentral.com/news01619.htm>

[10] MIT Business Continuity Plan - Master  
URL: <http://web.mit.edu/security/www/pubplan.htm>

[11] Business Continuity Best Practice related article at Page 8 onward  
URL: <http://www.intel.com/intelpress/chapter-book4.pdf>

© SANS Institute 2000 - 2005, Author retains full rights.