International Journal of Disaster Recovery and Business Continuity
Vol.8, November (2017), pp.29-44
http://dx.doi.org/10.14257/ijdrbc.2017.8.03

Systematic Literature Review: Disaster Recovery and Business Continuity Plan for Core Banking Solution (CBS) Project

G. M. Faruk Ahmed

Islamic University Kushtia, Dept. of Computer Science & Engineering
farukiu@gmail.com

Abstract

After the independence, banking industry in Bangladesh started its journey with 6 nationalized commercialized banks, 2 State owned specialized banks and 3 Foreign Banks. In the 1980's banking industry achieved significant expansion with the entrance of private banks. At present there are ***56 scheduled banks*** *in Bangladesh in which 6 State Owned Commercial Banks (SOCBs) with large number of branches which are fully or majorly owned by the Government of Bangladesh (GoB). These SOCBs is serving its millions of customers in urban and rural areas across the country with its wider branch network and modern technological facilities. From these 6 SOCBs, considering a bank which uniform modernize facility for its Transaction from anywhere of the country. To perform these facilities continuously to the customer the Bank has setup latest technology with hardware equipment and world's remarkable software. At the same time Bank has taken different measures and setup for uninterruptable services to the customer and continues business of the bank. For this purpose Bank has established Data Center (DC), Data Recovery Center (DRC) and prepared a disaster recovery plan, business continuity plan to overcome any natural and artificial disaster.*

Keywords*: Core Banking Solution, Data Center, Data Recovery Center, Disaster Recovery Plan, Business Continuity Plan*

1. Introduction

The Business Continuity Plan (BCP) is the predefined mechanism that addresses any kind of disaster which may disrupt/discontinue the business process. This BCP covers the mitigation procedure or immediate and long term action plan to handle the disaster caused by calamities like earthquake, storm, cyclone, flood, heavy rainfall or any other natural calamity. These kind of disaster may cause of discontinue of business process due to failure or unavailability of ICT resources, network/WAN down, data loss, DC/DR down or non-synchronize error, major virus attack, or any other kind of disruption to the business process. It puts disaster planning in perspective and makes it more likely that after disasters we will be handled smoothly and ensures no loss or minimum loss and resume the business process in shortest possible time. Having a BCP enhances an organization's image with employees, shareholders and customers by demonstrating a proactive attitude. Additional benefits include improvement in overall organizational efficiency and identifying the relationship of assets and human and financial resources to critical services and deliverables. The purpose of developing a Business Continuity Plan is to ensure the continuation of the business during and following any critical incident that results in disruption to normal operational capability. This paper can be used to assist for undertaking a Risk Management Plan and Business Impact Analysis, and create Incident Response and Recovery Plans for Bank Business.

Received (June 15, 2017), Review Result (October 10, 2017), Accepted (October 11, 2017)

ISSN: 2207-8363 IJDRBC

2. Research Methods

2.1. Systematic Review

A systematic process of formulating study objectives, selecting, critically appraising, synthesising information and drawing conclusion from relevant studies in order to provide a reliable review using either quantitative or qualitative approach (Oxman, 1994; Boynton *et al.,* 1998). A review of the evidence on a clearly formulated question that uses systematic and explicit methods to identify, select and critically appraise relevant primary research, and to extract and analyse data. Statistical methods (m-a) may/not be used. To conduct the systematic review constituting three main phases planning the review, conducting the review, reporting the review. The main part of planning are to specify research question and develop a review protocol, review protocol most important part of systematic review.

2.2. Research Question

Global changes in business models, heavier reliance on information technology, and recent developments in disaster recovery technologies are forcing organizations to reformulate their DR solutions. Some of the lessons and best practices mentioned in this document can be utilized to create viable and successful DR and business continuity solutions for clients. One third of organizations have reported having an incident that required initiating their disaster recovery plan. Whether it's hardware failure, cyber-attacks or a weather event; a myriad of incidents are regularly impacting businesses and their associates – driving the need for disaster recovery and business continuity plans that are thorough and tested. These threats could not be any more real: Key questions explored in this paper

Q1). Risk management, and risks to priorities their management?
Q2). Incident response strategy?
Q3). Business continuity plan?

2.3. Review Protocol

The main components of the review protocol include data sources, search strategy, study selection strategy, data extraction method, and data synthesis. The first three components define the scope of the study and explain the motivation behind it. The last two components describe how the results and concluded.

2.3.1. Data Sources

Therefore use these libraries as our main resources:

- ❖ IEEE Explore
- ❖ ACM Digital Library
- ❖ UCL Library
- ❖ Science Direct
- ❖ Wiley International Science journal Finder
- ❖ Bangladesh Bank Website

Also helps of this two Search engine, Google and yahoo

2.3.2. Data Selection

Data selection is the most imported thing to systematic review any existing research review, lot of thing are irrelevant to our research questions. Study selection has to be including only studies that contain useful information for answering Data recovery

challenges. Limits of study that are strongly related to short time incident response challenges. In our future work plan to another systematic review which on the studies that are presented in form than scientific paper.

2.3.3. Data Extraction

Each primary study is analyzed on identifying and continuing business process smoothly. All identified challenges are documented in a spread sheet in terms of their names, description and rationale.

3. Overview of the Systematic Studies

Growing reliance on Information Technology, along with compliance and regulatory requirements has led many organizations to focus on business continuity (BC) and disaster recovery (DR) solutions. Availability has become a major concern for business survival. This document lays down some of the best practices and learning for implementing disaster recovery solutions. The information shared in this document is based on the experience, obtained during the execution of disaster recovery implementation projects. On May 21, 2015, OnRamp Founder Chad Kissinger and GCS Technologies President Joe Gleinser took part in a panel discussion titled “Disaster Recovery—Surprising Challenges.” In the course of this conversation, Mr. Gleinser briefly outlined his top three challenges for developing a successful Business Continuity/Disaster Recovery (BC/DR) plan. The top three challenges Mr. Gleinser identified were:

1. Making the Formation of a BC/DR Plan a Business Priority
2. Ensuring the Completeness of Planning
3. Going it Alone

For both business continuity and disaster recovery, the time to plan is before the emergency happens. Let’s take a more in-depth look at these three challenges to help us overcome them before disaster strikes.

3.1. Business Continuity Planning Process

The team incorporates the Prevention, Preparedness, Response and Recovery (PPRR) framework for Business Continuity Plan process. Each of the four key elements is represented by the following diagram.

Figure 1. Business Continuity Planning Process

- **Prevention - Risk Management planning**

Incorporates the Prevention element that identifies and manages the likelihood and/or effects of risk associated with an incident.

- **Preparedness - Business Impact Analysis**

Incorporates the Preparedness element that identifies and prioritizes the key activities of a business that may be adversely affected by any disruptions.

- **Response – Incident Response planning**

Incorporates the Response element and outlines immediate actions taken to respond to an incident in terms of containment, control and minimizing impacts.

- **Recovery - Recovery planning**

Incorporates the Recovery element that outlines actions taken to recover from an incident in order to minimize disruption and recovery times.

4. Prevention - Risk Management Planning

It is necessary to manage the risks by identifying and analyzing the things that may have an adverse effect on the CBS, Mobile and Agent Banking, RTG, Own Branded ATM and other related business and choosing the best method of dealing with each identified risks. Each identified risk must be analyze by probability of occurrence and assess the possible impact on business. After analysis evaluate of each risk will be calculated. The total process of Identification, Analysis, Evaluation and Recovery of risk on above project and business of the bank are defined by following sequence of steps.

- Step-01: Identify risks.
- Step-02: Analyze risks to assess their impacts.
- Step-03: Evaluate risks to priorities their management.
- Step-04: Treat risks minimizing their impact.
- Step-05: Develop and review our Risk Management Plan

4.1. Identify Risks

The following are the common identified risk that could impact our business.

- Natural Disaster : - Earthquake floods, storms.
- Human Disaster : - Violation, fire and sabotage.
- Technology : - System failure, Power Failure, Network failure, Data loss.
- Regulatory : - Violation of rules and regulation.
- Security : - Theft, fraud, technology intrusion, IP extortion.
- Support from Vendor : - Customization, Solution of Operation & System problem.
- Skill Manpower : - Unable to configure the system in critical position.
- Work Environment : - Work Place Health and Safety.

4.2. Analyze Risks to Assess Their Impacts

To analyses the above identified risk it is necessary to identify the assumption of frequency or probability of occurrence of each risk and assess the business or health effect of the risk. So level of risk in this plan is defined by the following formula.

Level of risk = consequence (assess business impact) x likelihood (probability or sequence) Level of risk is often described as

- Very Low
- Low
- Moderate
- High or
- Severe.

The consequence and likelihood are measures with the following scale in the plan.

4.2.1. Consequences Scale

Table 1

Level	Consequence	Description
4	Severe	Financial losses greater than Tk.10 Core and above
3	High	Financial losses between Tk.05 core to Tk.10 core
2	Moderate	Financial losses between Tk.01 core to Tk. 05 core
1	Low	Financial losses less than Tk.1.000

4.2.2. Likelihood Scale

Table 2

Level	Likelihood	Description
4	Very likely	May happens more than once a year.
3	Likely	May happens about once a year
2	Unlikely	May happens every 10 years or more
1	Very unlikely	Has only happened once
0	Not like	Never happen

4.2.3. The Risk Rating

The risk rating depending on likelihood and conscience scale as define above are calculated for identified risk defined in Step-1 are given below

Table 3

Sl. No.	Identified Risk		Consequence level	Likelihood level	Risk Rate
01	**Natural Disaster**	Earthquake	4	1	4
		Strom	4	1	4
		Flood	0	4	0
02	**Human Disaster**	Fire	4	2	8
		Sabotage	4	1	4
		Violation	0	4	0
03	**Technology**	System Failure	2	4	8
		Power Failure	2	3	6
		Network failure	1	4	4
		Data Loss	4	2	8

04	**Regulatory**	Not Sign-in	1	4	4
		Not Sign-out	1	4	4
		Violation of Rules	3	4	12
05	**Security**	Theft	2	2	4
		Fraud	3	2	6
		Technology Intrusion	4	4	16
06	**Support From Vendor**	Data Migration	2	4	8
		Customization	2	3	6
		Enhancement	2	4	8
		Operation Problem	3	4	12
		System Problem	2	3	6
07	**Skill Manpower**	Unable to configure the system in critical position	3	3	9
08	**Work Environment**	Healthy	1	3	3
		Safety	1	3	3

4.2.4. Evaluate Risks to Priorities Their Management

The team has defined the priorities the risk depending the rating point as follow:

Table 4

Risk rating	Description	Action	Reason
12-16	Severe	Needs immediate corrective action	• Violation of Rules • Technology Intrusion • Operation Problem
8-12	High	Needs corrective action within 1 month	• Fire • System Failure • Data Loss • Enhancement • Unable to configure the system in critical position
4-8	Moderate	Needs corrective action within 3 months	• Power Failure • Fraud • Customization • System Problem
1-4	Low	Does not currently require corrective action	• Earthquake • Strom • Sabotage • Network failure • Not Sign-in • Not Sign-out • Theft • Healthy • Safety
0-1	Very low	Not required to take action	• Flood • Violation

4.2.5. Treat Risks Minimizing Their Impact

According to the defined priorities risk some are fully recover, some are partially recover and rest are nor recoverable. The risk which are not recoverable but impact of business lose could be minimized by taking some precaution. Therefore the corrective actions to recover risk and minimize risk within three (3) month, one month and immediately are given below.

Risk Event	Action period
System failure	Needs immediate corrective action
Support from vendor	Needs corrective action within 1 month
Technology	Needs corrective action within 3 months

4.2.6. Develop and Review our Risk Management Plan

Risks do not always remain the same for a project and its related business. It needs to constantly monitor and review the strategies to manage risk. New risks may be created and existing risks may be increased or decreased. So that priority order of risks would be changed and risk treatment strategies will no longer be effective.

BCP Team will meet a meeting held on every half year for Review and update the Business Continuity Plan presided by Head of IT of the Bank. In the meeting existing identified risk will be reviewed and recovery point will be defined.

5. Preparedness - Business Impact Analysis

Businesses are constantly threatened with risks and preparedness is important to prevent the occurrence of risks from which causing the business disruption. A business impact analysis (BIA) predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during a risk assessment. The BIA should identify the operational and financial impacts resulting from the disruption of business functions and processes.

So it is necessary to identify the following points.

- The critical business function and process.
- What the operational and financial impacts to the business due to disruption.
- How long could the business survive without performing this activity?

5.1. Priority Ranking Scale of Operation and Financial Business impact.

Table 5

Priority Ranking	Description	Action Period
04	Very Important	Within the specified period
03	Important	Within 24 Hours
02	Less Important	Needs corrective action within a week
01	Not Important	Does not currently require corrective action

6. Responses-Incident Response Plan

Incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. An incident response plan includes a policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs.

There are six key phases of an incident response plan:

1. Preparation: Preparing users and IT staff to handle potential incidents
2. Identification: Determining whether an event is indeed a security and other incident
3. Containment: Limiting the damage of the incident and isolating affected systems to prevent further damage
4. Eradication: Finding the root cause of the incident, removing affected systems from the production environment
5. Recovery: Permitting affected systems back into the production environment, ensuring no threat remains
6. Lessons learned: Completing incident documentation, performing analysis to ultimately learn from incident and potentially improve future response efforts

An incident response plan can benefit an enterprise by outlining how to minimize the duration of and damage from a security incident, identifying participating stakeholders, streamlining forensic analysis, hastening recovery time, reducing negative publicity and ultimately increasing the confidence of corporate executives, owners and shareholders. The plan should identify and describe the roles/responsibilities of the incident response team members who are responsible for testing the plan and putting it into action. The plan should also specify the tools, technologies and physical resources that must be in place to recover breached information.

6.1. Identification of Incident List

Following are the security and other Incident list those may occurs

- Network failure
- Power failure
- Unauthorized access in the system
- Unauthorized Access in the premise
- Operational Problem
- Vendor Stop Support
- Environmental Disasters
- Fires
- External Threat (Virus, sperm, warm and hacker)
- Data and System loss

6.2. Evacuation Procedures

The objective of an evacuation plan is to provide a set of procedures to be used by site occupants in the event of a critical incident.

We have to:

- start with a floor plan of the site
- clearly identify the location of emergency exits
- develop strategies for providing assistance to persons with disabilities
- make sure that everyone knows what to do if evacuation is necessary
- select and indicate a meeting place away from the site

- Test the plan on a regular basis.

6.3. Action Plan for Office Hour Disaster

Following steps are to be taken during Office Hour Disaster:

- Protect Employees and Customers
- Activating Emergency Decision plan taken by ICT security Maintenance team evaluating the situation of disaster
- Contact Emergency Service Providers
- Safeguard critical assets
- Collect all the necessary items according to grab list
- Minimize Confusion and Delay
- Secure all doors and cabinets
- Secure essential department records and equipment
- Protect all sensitive documents/ files
- Restore Backup Data into the server as early as possible.
- Start live transaction immediately after restoration of the database and checking other relevant issues.
- Enter Lost or missing data into the system before the end of the day.

6.4. Action Plan for Outside Office Hour Disaster

- If disaster happens during processing of closure of business (COB) procedure necessary authority should be informed and restoration should be made immediately from backup to start the COB process again.
- In case of failure in resumption of database after disaster, data should be restored from the backup media (Tape) to make it available for the next working day.
- If any disaster happens in the main data center, action should be taken immediately to make the disaster recovery site act as the main data center.
- If any disaster happens in the inter-branch network, network service provider should be informed immediately. Work of the network service provider should be monitored until the network restores to normal operation.

6.5. Documents

The following Document must be maintain:

- List of employees with contact details – include home and mobile numbers, and even e-mail addresses. We may also wish to include next-of-kin contact details.
- Lists of customer and supplier details.
- Contact details for emergency services.
- Contact details for utility companies.
- Building site plan (this could help in a salvage effort), including location of gas, electricity and water shut off points.
- Evacuation plan.
- Latest stock and equipment inventory.
- Insurance company details.
- Financial and banking information.
- Engineering plans and drawings.
- Product lists and specifications.
- Formulas and trade secrets.
- Local authority contact details.

- Headed stationery and company seals and documents.

6.6. List of other Accessories with Responsible Officers

- Computer back-up tapes/disks/USB memory sticks or flash drives.
- Spare keys/security codes.
- Torch and spare batteries.
- Hazard and cordon tape.
- Message pads and flip chart.
- Marker pens (for temporary signs).
- General stationery (pens, paper, *etc*).
- Mobile telephone with credit available, plus charger.
- Dust and toxic fume masks.
- Disposable camera (useful for recording evidence in an insurance claim).

Special Instruction:

- Make sure this pack is stored safely and securely **on-site** and **off-site** (in another location).
- Ensure items in the pack are checked regularly, kept up-to-date, and in good working order.
- Remember that cash/credit cards may be needed for emergency expenditure.

6.7. Immediate Response Checklist

Table 6

INCIDENT RESPONSE	✓	ACTIONS TAKEN
Have it:	❑	
• Assessed the severity of the incident?	❑	
• Evacuated the site if necessary?	❑	
• Accounted for everyone?	❑	
• Identified any injuries to persons?	❑	
• Contacted Emergency Services?	❑	
• Implemented your Incident Response Plan?	❑	
• Started an Event Log?	❑	
• Activated staff members and resources?	❑	
• Appointed a spokesperson?	❑	
• Gained more information as a priority?	❑	
• Briefed team members on incident?	❑	
• Allocated specific roles and responsibilities?	❑	
• Identified any damage?	❑	
• Identified critical activities that have been disrupted?	❑	
• Kept staff informed?	❑	
• Contacted key stakeholders?	❑	
• Understood and complied with any regulatory/compliance requirements?	❑	
• Initiated media/public relations response?	❑	

6.8. Emergency Kit

If there is damage to the building or if it must be evacuated and operations need to be moved to an alternative location, the emergency kit can be picked-up and quickly and easily carried off-site or alternatively stored safely and securely off-site. Document within the plan what is contained within your emergency kit and when it was last checked.

6.9. Disaster Declaration

After declaring disaster BCP will be automatically activated. All persons related to BCP will start their activities according to BCP without making delay.

7. Backup and Restore Management

Backup is the most important procedure to prevent loss of data in the case of accidental deletion/corruption of data, system failure in case of natural and artificial disaster as defined in identified risk in **Risk Management planning** and to permit timely restoration of archived data in the event of any disaster. Bank should establish a formal Data Backup and Recovery Policy to continue business without interruption. The Policy and procedure are below.

1. **Disaster Recovery Policy**
2. **Backup Policy**
3. **Backup environments and scheduling**
   (i) Data Backup:
   (ii) System Backup:
   (iii) Network Configuration Backup
4. **Backup Utilities and Storage**
5. **Backup Recovery Abilities**
6. **Backup Monitoring and Controlling Document.**

8. Recovery

A recovery plan help to respond effectively if an incident or crisis affects the business. It aims to recover in minimum time and minimize losses. The recovery plan contains information relating to planning for recovery as well as the resumption of critical business activities after a crisis has occurred. It also outlines the time frame in which we can realistically expect to resume usual business operations. Developing a recovery plan gives us a chance to consider how we will get our business back on track if we do experience a crisis. It should include:

- strategies to recover our business activities in the quickest possible time
- a description of key resources, equipment and staff required to recover our operations
- The recovery time objectives
- A checklist we can use after a crisis has passed and it is safe to return to our premises.

8.1. Team Member of BCP

Implementation and operation of Core Banking Solution (CBS) is one of the important projects of the Bank. At the same time Mobile and Agent Banking, RTGS and Own Branded ATM operation also important project. Considering the above project the Bank need to build a committee to prepare a Business Continuity Plan. The committee will update and revised the plane as per impact and requirement of the project and

related business of the Bank.

The Team Member of the BCP will be as follow:

Table 7

SL. No	Name	Designation and Contacts	Position
01	Name of the Head of IT	Head of IT Contract No(Mobile,Tel.,Email)	Chairman
02	Name of the Sr. System Analyst	Sr. System Analyst Contract No(Mobile,Tel.,Email)	Member
03	Name of the Systems Analyst	Systems Analyst Contract No(Mobile,Tel.,Email)	Member
04	Name of the Programmer	Programmer Contract No(Mobile,Tel.,Email)	Member
05	Name of the Hardware Engineer	Hardware Engineer Contract No(Mobile,Tel.,Email)	Member
06	Name of the Network Engineer	Network Engineer Contract No(Mobile,Tel.,Email)	Member
07	Name of the Assistant Programmer	Assistant Programmer Contract No(Mobile,Tel.,Email)	Member
08	Name of the Assistant Hardware Engineer	Assistant Hardware Engineer Contract No(Mobile,Tel.,Email)	Member
09	Name of the Assistant Network Engineer	Assistant Network Engineer Contract No(Mobile,Tel.,Email)	Member

8.2. Plan, Maintain and Review

At present Bank has planned to recover the critical situation within the time objective. The key factor in the successful implementation of the plan during an emergency are:

i). Maintaining and monitoring the Backup Devices in Data Center (DC) & Data recovery Site (DRS) on regular basis.

ii). Maintaining and Monitoring the Power Devices, UPS and Generator in Data Center (DC) & Data recovery Site (DRS) on regular basis.

iii). Maintaining and Monitoring the Data Communication Line among branches, Data Center (DC) & Data recovery Site (DRS) on regular basis.

iv). Ensure regularly Data Backup, System Backup and Video Footage Backup of CCTV Camera at On-site and Off-site location in defined media.

v). Maintaining and Monitoring the Access log in DC and DRS.

vi)Maintaining and Monitoring the Video Footage of CCT Camera of DC and DRS

vii). Training of the officer and Staff on schedule basis who are involved in an emergency at the site

viii). Update the List of Vendor Support Team with contract Number.

ix). Update of Emergency help Number of Fire Services, Police Station and Hospital.

x). Pay Attention to Officer and Staff change in DC and DRS.

It is necessary to ensure and regular review and update the plan to maintain accuracy and reflect any changes inside or outside the DC and DRS. After an event it is important to review the performance of the plan, highlighting what was handled well and what could be improved upon next time. Record details for plan reviews in the table below:

Table 8

Review Date	Reason for Review	Changes Made

8.3. Vendors & Service Providers Contact

This is the list of vendors and their providing services. Whenever necessary they are contacted to provide the required services.

SL. No	Service	Name	Company Name	Contacts
01	**Hardware Service**			
02	**Network Service**			
03	**Database Service**			
04	**CBS Service**			
05	**UPS & AC**			

8.4. Others Emergency Contact

The following emergency service provider's contacts must be carried by the employees of ABC for the purpose of emergency use in case of any disaster/incident

Table 9

Service Name	Address	Contact Numbers
Internal emergency contact	Duty Officer	
	Medical Center	
	Generator	
	Fire Control Room	
	Emergency Medical Contact	
Fire Brigade Hot line		
Police Station	Police Station 1	
	Police Station 2	
Police Hot Line		
Ambulance Services	Day-Night Ambulance Service	
	Hot Line	
Hospital	Hospital Name 1	
	Hospital Name 2	

8.5. References and Related Documents

Table 10

SL. No.	Ref. Book and Document Name	Store Location
01	Specification Of Hardware	

02	Specification of Software	
03	List of IP Address	
04	Maintenance Log Book	
05	Backup Log Book	
06	Key Register Book	

9. BCP Testing

Testing the BCP is the only way to see if the goals set have been met. These tests will throw up inconsistencies, incorrect information (if any) and points where the actual and expected results differ. The team can brainstorm on the gaps found and revise the plan accordingly. This would lead to yet another test cycle.

Planning a BCP test will involve defining the following:

- Test Scenario - defining the disaster that is to happen as a part of the testing.
- Test Plan - defining the audit schedule, the set of test scenarios, the type of exercise or the participants, *i.e.*, the primary team, or a mix of primary and alternate teams.

The test exercise can be a checklist exercise or a tactical exercise.

Checklist exercise involves a structured walkthrough. The team comes together with a prior knowledge of the test scenario. Each member plays a designated role and walks through the activities assigned to him/her in the continuity plan.

Tactical exercise involves an actual simulation. There will be a coordinator for each test,who will announce the intermediate events for the scenario — as if they were happening. The team goes through the entire plan, performing all the activities, from notification to restoration. If this exercise is a planned or notified exercise, then it will be generally designed in such a way that the activities of the entire team are covered. Surprise simulations can also be performed. It is usually the last type of exercise in the testing of the continuity plan and gives a picture of the actual preparedness of the team.

While testing the BCP, the following activities are performed.

- Prepare a test plan, choose the test scenario(s) and state the expected results
- Execute the plan
- Document the test results
- Review the actual results and report gaps and/or slippages
- Circulate the results and the report among the team
- Identify the changes that are to be made to the BCP to cover gaps and overcome
- observed slippages
- Train the team (this is an activity performed whenever the BCP undergoes an update)

The **Test Plan** would normally contain the following information.

- Test plan identification
- Test scenario(s) selected
- Type of exercise, *e.g.,* walkthrough, surprise simulation, *etc*.
- List of participants
- Sections of the BCP operations that are to be executed
- Expected results and expected timeframes for achieving them
- Actual results and actual elapsed time
- Gaps and slippages observed

- Recommendations

10. Review of BCP

The BCP must be reviewed periodically. It is mandatory to review it when a system is added to the production, a system in production is changed, a process that falls in the scope of the plan changes, or there is a change in the schedule of the business activities. Besides these events, a change in the contact person list can also trigger an update.

Review of the BCP may also happen with the intention of improvement, *e.g.*, in the course of documenting the lessons learnt during the testing exercises, the organization revising its continuity goals and deciding to move up on the "availability" spectrum, or when an alternative method of doing things has been evaluated to give better results. So, maintenance of the BCP is done with the intention of both change and improvement. Every revision to the plan must be followed by a distribution to the BCP team, a training update and a testing exercise.

11. Conclusion

Even though Business Continuity Planning appears to primarily deal with technology, it is equally associated with business. It is true that the operational aspect involves technology, but knowledge of technology alone is not sufficient for this exercise. It includes activities in risk management, crisis management, identification of business processes, impact analysis, cost benefit analysis, storage management, network management, continuity planning, recovery planning, training, communication and coordination. The team involved in business continuity planning should ideally be a cross-functional team with adequate domain knowledge, expertise in system and recovery management and skills in planning.

Key Finding

Business interruptions can occur anywhere, anytime. Massive hurricanes, tsunamis, power outages, terrorist bombings and more have made recent headlines. It is impossible to predict what may strike when. In today's 24x7x365 world, it has become mandatory to prepare for such disaster scenarios. With the ever increasing dependence on banks for both electronic and traditional banking services, it has become almost mandatory for the banking industry to plan for 'Business Continuity'.

References

[1] Editorial Staff of Searchstorage.com, Bank avoids data disaster on Sept. 11. SearchStorage.com 6 mar. 2002. Disponivel em: <http://searchstorage. techtarget.com/tip/0 289483 sid5-gci808783 00.ht ml>. Acesso em: 3 jan. 11.
[2] Disaster/Emergency Management and Business Continuity Programs, **(2013)**.
[3] H. Packard, hp AlphaServer technology helps Commerzbank tolerate disaster on September 11. hp.com jul. 2002. Disponivel em: <http://h71000. www7.hp.com/openvms/brochures/commerzbank/comm erzbank.pdf?jumpid=reg-R1002- USEN>. Acesso em: 3 jan. 11.
[4] Availability Digest, Commerzbank Survives 9/11 with OpenVMS Clusters. Availability Digest jul. 2009. Disponivel em: <http://www. availabilitydigest.com/public-articles/0407/commerzbank. pdf>. Acesso em: 3 jan. 11.
[5] K. Parris, "Who Survives Disasters and Why Part 2: Organizations", www2.openvms.org/kparris/ 2010. Disponivel em: <http://www2.openvms.org/ kparris/Bootcamp-2010-Disasters-Part2-O rganizations.pdf>. Acesso em: 3 jan. 11.
[6] https://www.scribd.com/document/306738427/BCP-of-Several-Bank.
[7] Egenera, "Case Study: Commerzbank North America. Egenera 2006", Disponivel em: <www.egenera.com/1157984790/Link.htm>. Acesso em: 3 jan. 2011.

[8] J. Minkel, "The 2003 Northeast Blackout-Five Years Later", Scientific American 13 ago. 08. Disponivel em: <http://www.scientificamerican.com/ article.cfm?id=2003-blackout-fiveyears- later>. Acesso em: 6 jan. 11.
[9] "Electricity Consumers Resource Council (ELCON)", The Economic Impacts of the August 2003 Blackout. ELCON 09 fev. 2004. Disponivel em: <http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blac kout.pdf>. Acesso em:, **(2009)**.
[10] "U.S.-Canada Power System Outage Task Force", Final Report on the August 14 2003 Blackout in the United State and Canada: Causes and Recommendations April 2004. Disponivel em: <https://reports.energy.gov>.

Authors

G. M. Faruk Ahmed, he graduated in Computer Science and Engineering from Islamic University, Kushtia, Bangladesh in the year 2009. Master of Computer Science from Stamford University Bangladesh in the year 2012. Life Member of Bangladesh Computer Society (BCS). At present, he is working as a Programmer in the Rupali Bank Ltd. Bangladesh which is a Government bank in Bangladesh. His interests Research area is Data Warehouse, Big data, and ICT Security. He has been an author of three International journal papers.

