BUSINESS CONTINUITY PLAN
CASE STUDY: CROWN PROPERTY BUREAU

ORAWAN PANKASEAM

A THEMATIC PAPER SUBMITTED IN PARTIAL
FULFILLMENT OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE
(TECHNOLOGY OF INFORMATION SYSTEM MANAGEMENT)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2014

Thematic Paper
entitled

BUSINESS CONTINUITY PLAN
CASE STUDY: CROWN PROPERTY BUREAU

……
Miss Orawan Pankaseam
Candidate

……
Asst. Prof. Supaporn Kiattisin, Ph.D.
(Electrical and Computer Engineering)
Major advisor

……
Asst. Prof. Adisorn Leelasantitham, Ph.D.
(Electrical Engineering)
Co-advisor

……
Prof. Banchong Mahaisavariya, Ph.D.
M.D., Dip Thai Board of Orthopedics
Dean
Faculty of Graduate Studies
Mahidol University

……...
Asst. Prof. Supaporn Kiattisin,
Ph.D. (Electrical and Computer Engineering)
Program Director
Master of Science Program in
Technology of Information System
Management
Faculty of Engineering
Mahidol University

Thematic Paper
entitled

BUSINESS CONTINUITY PLAN
CASE STUDY: CROWN PROPERTY BUREAU

was submitted to the Faculty of Graduate Studies, Mahidol University
for the degree of Master of Science
(Technology of Information System Management)
on
November 19, 2014

……
Miss Orawan Pankaseam
Candidate

……
Lect. Sotarat Thammaboosadee, Ph.D
(Information Technology)
Chair

……..…...
Asst. Prof. Supaporn Kiattisin, Ph.D.
(Electrical and Computer Engineering)
Member

……
Asst. Prof. Kairoek Choeychuen Ph.D.
(Electrical and Computer Engineering)
Member

……...……
Asst. Prof. Adisorn Leelasantitham, Ph.D.
(Electrical Engineering)
Member

…… ……
Prof. Banchong Mahaisavariya,
M.D., Dip Thai Board of Orthopedics
Dean
Faculty of Graduate Studies
Mahidol University

……
Lect. Worawit Israngkul,
M.S.(Technical Management)
Dean
Faculty of Engineering,
Mahidol University

ACKNOWLEDGEMENTS

Business Continuity Plan Case Study: Crown property Bureau would like completely. I thanks to my thematic advisor team, Supaporn Kiattisin, Ph.D. (Major advisor) and Adisorn Leelasantitham, Ph.D. (Co-advisor) for invaluable suggest, help and recommend throughout the course of this research

I also thank high-ranking executives and IT Staff of organization for help to testing Simulated Situation plan, evaluation of the plan and recommendations for the benefit of Business Continuity Plan.

I gratefully encouragement my parent, my friend and my co-worker for support of this research.

Orawan Pankaseam

BUSINESS CONTINUITY PLAN CASE STUDY: CROWN PROPERTY BUREAU

ORAWAN PANKASEAM 5336494 EGTI / M

M.Sc. (TEACHNOLOGY OF INFORMATION SYSTEM MANAGEMENT)

THEMATIC PAPER ADVISORY COMMITTEE: SUPAPORN KIATTISIN, Ph.D., ADISORN LEELASANTITHAM, Ph.D.

ABSTRACT

This research is qualitative research, which studies measures and processes in the creation of business continuity plans. The purposes of the research are to allow interrupted business processes and working systems to return to service within a specified period of time, create abilities to prevent and reduce risks in the information technology system, and successfully protect essential data of the organization.

The result of the plan is tested using four potential situations, which are Blackouts Caused by Exploded Transformers, Flooding, Political Demonstrations, and Disruptions to Critical Work. Hence, interviews were conducted by dividing the interviews into two groups, namely, high-ranking executives and IT staff, in order to determine the level of satisfaction in the following business continuity plan and set goals for the staff of the Information Technology Management Section, IT Department, Eighty-four percent of the high-ranking executives are satisfied with the business continuity plan, and the satisfaction of IT staff in the business continuity plan equaled 81.2 percent.

According to the research, staff members who are involved in the business continuity plan and the staff who have never participated in the plan should be encouraged to participate in the testing.

KEY WORDS: BUSINESS CONTINUITY PLAN / RISK / TESTING

93 pages

แผนสร้างความต่อเนื่องทางธุรกิจ กรณีศึกษาสำนักงานทรัพย์สินส่วนพระมหากษัตริย์
BUSINESS CONTINUITY PLAN CASE STUDY: CROWN PROPERTY BUREAU

อรวรรณ ปานเกษม 5336494 EGTI / M

วท.ม. (เทคโนโลยีการจัดการระบบสารสนเทศ)

คณะกรรมการที่ปรึกษาสารนิพนธ์ : สุภาภรณ์ เกียรติสิน, Ph.D., อดิศร ลีลาสันติธรรม, Ph.D.

บทคัดย่อ

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยทำการศึกษาจากมาตรฐานและกระบวนการในการจัดทำแผนสร้างความต่อเนื่องทางธุรกิจ เพื่อทำให้กระบวนการทางธุรกิจและระบบงานที่หยุดชะงักไปสามารถกลับมาให้บริการต่อไปได้ภายในระยะเวลาที่กำหนดและสามารถป้องกันและลดความเสี่ยงต่อระบบเทคโนโลยีสารสนเทศและสามารถรักษาข้อมูลที่สำคัญต่อองค์กรไว้ได้

ผลการศึกษาพบว่า จากการทดสอบแผนสร้างความต่อเนื่องทางธุรกิจทั้ง 4 สถานการณ์ คือ สถานการณ์ไฟฟ้าดับ/หม้อแปลงระเบิด สถานการณ์น้ำท่วม ชุมนุมทางการเมือง และระบบงานสำคัญหยุดชะงัก จึงได้สัมภาษณ์ถึงความพึงพอใจที่มีต่อแผนกับกลุ่มผู้บริหารระดับสูงและกลุ่มเจ้าหน้าที่สารสนเทศ พบว่า กลุ่มผู้บริหารระดับสูงพอใจการทดสอบแผน 84 % กลุ่มเจ้าหน้าที่สารสนเทศพอใจการทดสอบแผน 81.2 %

จากการวิจัยครั้งนี้มีข้อเสนอแนะว่า บุคลากรที่เกี่ยวข้องกับแผนและยังไม่เคยเข้าร่วมดำเนินการตามแผน ควรผลักดันและจัดให้บุคลากรดังกล่าวเข้าร่วมการดำเนินการทดสอบตามแผนที่ได้จัดทำไว้

93 หน้า

CONTENTS

CONTENTS (cont.)

CONTENTS (cont.)

CONTENTS (cont.)

LIST OF TABLES

LIST OF TABLES (cont.)

LIST OF FIGURES

LIST OF FIGURES (cont.)

CHAPTER I
INTRODUCTION

1.1 Preface

Today's hazards in information technology are increased by following the developments of information technology. The hazards created might be caused by multiple factors, including both internal and external factors such as personnel belonging to related organizations and their use of information technology, or persons outside organizations either intentionally or unintentionally using situations or events causing data in information technology systems to be disclosed, modified, destroyed, malfunctioning or other according to the intentions of the threat or risks created by natural disasters, e.g., fires, storms, floods, etc. Thus, in order to minimize the aforementioned hazards in information technology, it is essential that importance be given to plans of action to prepare for emergencies created by potential disasters.

For the above mentioned reason, the Information Technology Department of the Crown Property Bureau needs to analyze and organize work systems essential to the work of the Crown Property Bureau, including the evaluation of situations for internal and external factors creating risks or obstacles to the information technology system in order to provide guidelines for the formation of strategies for recovering information technology systems and contingency plans for incidents divided into the following three parts: pre-situational monitoring, responses to events occurring and post situational procedures, including the recovery of information technology systems to normal function.

1.2 Case Study: Crown Property Bureau [1]

The Crown Property Bureau is an organization that has shared a long relationship with the history and development of Thailand into a democracy with the

king as the head of state. It has also played important roles in the support and promotion of sustainable national development.

The Crown Property Bureau was established under the Royal Asset Structuring Act B.E. 2479 (Edition 1) by the division of royal assets into “His Majesty’s personal assets,” “crown property,” and “public property”. Crown property was put under the care of the Ministry of Finance which established an office and named it the “Crown Property Bureau” with status equal to that of a division (presently known as the Department of Treasury) under the Ministry of Finance. Some personnel and workers at the Office of the Privy Purse were transferred to the Crown Property Bureau and part of the office space for the Privy Purse in the Royal Palace was allocated for this purpose.

Later on, two additional revisions were made in the Royal Asset Structuring Act to suit the purposes of the announcement in the Royal Asset Structuring Act (Edition 2) B.E. 2484 on 7 October 1941 and the Royal Asset Structuring Act (Edition 3) B.E. 2491 on 18 February 1948 which upgraded the status of the Crown Property Bureau to become a juristic person responsible for managing the interests of His Majesty’s Personal Assets.

Hence, the Crown Property Bureau is determined to manage the assets under the Bureau’s responsibility to create sustainable benefits for communities, people, and society in general by adhering to the principle of reasonable development based on the concept of sufficiency in line with the social conditions and cultures of local communities along with the application of His Majesty’s statements and work principles to “understand, access and develop” in order to improve the quality of life of the people by promoting activities for sufficient and sustainable benefits for the Thai people and society.

Thus, the Crown Property Bureau has created concepts for executives and personnel to understand the foundations of sustainable corporate development in order to push the organization toward stable and sustainable work management.

Figure 1.1 Basis for sustainable development in Crown Property Bureau [14]

In line with this image, it is obvious that the Crown Property Bureau has observed the significance of basic factors such as information technology systems in providing personnel with the ability to use information technology as a tool in the work of respective departments to aid the organization in achieving its goals and driving the organization forward under the obligations and vision of the Crown Property Bureau successfully.

1.3 Background and Significance of the Problem

The Crown Property Bureau is aware of the risks, security and safety of data in information technology systems, which is very important to the organization and has been given ongoing work priority. Therefore, the Department of Information Technology, Crown Property Bureau, needs to seek preventive methods and practice guidelines in line with the situations occurring in order to ensure that the Crown Property Bureau's main work system is not interrupted. The analysis by the Crown Property Bureau of various situations and events can be summarized in terms of situations and effects as follows:

Table 1.1 Various situations and events of Crown Property Bureau

Year	Situation	Problem and Effects
2009	Political Unrest/Protests	- Crown Property Bureau personnel could not access work at the Bureau. - The Crown Property had to shut down, thereby preventing tenants from contacting the Bureau. - Safety risks to the Bureau's staff and office buildings, including the computer database center. - The Bureau's staff lost outside access to the Crown Property Bureau's system.
2011	Natural Disaster: Floods	- The perimeter surrounding the Crown Property Bureau was flooded, which prevented the staff from working. - The Crown Property was required to shutdown, thereby preventing tenants from contacting the Bureau. - Risks to the Bureau's networks and servers in the computer database center. - Service shutdown of all IT systems
2013-2014	Political Unrest/Protests	- The Crown Property Bureau's staff had occasional access to work, depending on the severity of the situation. - Tenants lost contact with the Bureau. - Safety risks to the Bureau's staff and office buildings, including the computer database center. - The Bureau's staff lost outside access to the Crown Property Bureau's system.

In previous situations, the Crown Property Bureau was unable to perform work under its obligations and vision, thereby constantly attracting the attention of high-ranking executives concerning the risks, safety and stability. High-ranking

executives observed the importance of information technology as an essential factor in making work possible, whether from inside or outside the Crown Property Bureau. Finally, in order to prepare the Bureau for emergencies or disasters, which will interrupt the work system, the Crown Property Bureau initiated the concept of preparing business continuity plans.

1.4 Research Objectives

1.4.1 Prepare the Crown Property Bureau's business continuity plans.

1.4.2 Use the business continuity plans in the Crown Property Bureau in order to create organized processes in response to and management of incidents.

1.4.3 Set clear responsibilities and duties in the management of and response to incidents.

1.4.4 Quick and effective response to situations encountered.

1.5 Scope of the Study

1.5.1 Study measures and processes in the creation of business continuity plans.

1.5.2 Set incident management plans.

1.5.3 Test incident management plans in order to be prepared and respond to situations encountered.

1.6 Expected Benefits

1.6.1 The Crown Property Bureau's executives and staff give importance to business continuity plans in order to be prepared to manage situations potentially causing damage to the organization.

1.6.2 The business continuity plans allows for interrupted business processes and work systems to return to service within a specified period of time.

1.6.3 The business continuity plans are capable of preventing and reducing risks to the information technology system and successfully protecting data essential to the organization.

1.7 Research Methods

1.7.1 Project Preparation

1.7.2 Research of Theories and Collection of Related Data

1.7.3 Business Impact Analysis and Risk Assessment

1.7.4 Set Goals for Operational Recovery

1.7.5 Business Continuity Plans

1.7.6 Communication Plans

1.7.7 Training and Testing of Business Continuity Plans

1.7.8 Revise and Modify Business Continuity Plans

1.8 Duration of Study

Table 1.2 Duration of Study

Activity	May 2014	June 2014	July 2014	Aug 2014	Sep 2014	Oct 2014
Project Preparation						
Research of Theories and Collection of Related Data						
Business Impact Analysis and Risk Assessment						
Set Goals for Operational Recovery						
Business Continuity Plans						
Communication Plans						
Training and Testing of Business Continuity Plans						
Revise and Modify Business Continuity Plans						

CHAPTER II
LITERATURE REVIEW

2.1 Introduction

The work of making business continuity plans requires the referencing of related theories and frameworks. The related theories and frameworks are applied to create suitability for the drafting of business continuity plans for each organization for ongoing business operations. The plans of each organization will differ depending on a variety of factors.

Thus, theories, standards and practice guidelines must be studied in order to obtain knowledge and understanding applicable to the Department of Treasury for use as a guideline for the prevention of work hazards and risks to work or obstructions to work systems when incidents occur.

2.2 Literature Review

Here are a few points that highlight the importance of business continuity planning: 93% of the companies that suffer significant data loss are out of business within five years (U.S. Bureau of Labor) A company that experiences a computer outage lasting more than 10 days will never fully recover financially. 50% will be out of business within 5 years. Average hourly downtime cost for many businesses is $18,000 [2]

Organizations in highly competitive industries are often compelled to respond dynamically to a competitor’s offerings. Under pressure to reduce the time to market for newly conceived products and services, business managers sometimes do not give advance notice to the infrastructure team to address capacity issues. This failure to align technological capability with business needs and growth projections often results in solution gaps, false expectations and performance issues that adversely

affect organizational reputation. These issues can be avoided by systematic planning and collaboration between business and IT. [3]

Business continuity and disaster recovery program that will minimize the impact of disasters. A current, detailed and flexible plan will protect your assets and allow your organization to survive. [4]

Due to the an overloaded system and damage to the communications infrastructure during the 9/11 attacks, many continuity plans were delayed or altered because of the lack of adequate communications. The need for redundant and effective communications has been an ongoing theme since the terrorist attacks. According to a Gartner report "those within the agency responsible for BCP must document and regularly update a broad range of contact information, including home, office, vacation home and mobile telephone numbers, work and personal e-mail addresses and paper numbers. [5]

Successful business continuity management relies on the expertise from within the organization - it is the people that understand the organization - its business, processes and business risks. However, the Guide does not assume everyone is an expert in the field of risk management so describes each phase of business continuity against an accepted, generic risk management framework. The Guide is divided into two major parts - the first part deals with business continuity management concepts in a risk management context; the second part identifies the processes and procedures required to be undertaken to produce a business continuity plan. A number of supporting pro-forma schedules, working papers and questionnaires have been prepared to facilitate the overall process described in the Guide. [6]

2.3 Risk management and Enterprise risk management Framework define [2]

Risk stems from uncertainty or unpredictability of the future. In commercial and business risk generates profit or loss depending upon the way in which it is managed. Risk can be defined as the volatility of the potential outcome.

Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.

Enterprise risk management is a process, effected by an entity s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Within the context of an entity s established mission or vision, management establishes strategic objectives, selects strategy, and sets aligned objectives cascading through the enterprise. This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:

2.3.1 Strategic: high-level goals, aligned with and supporting its mission

2.3.2 Operations: effective and efficient use of its resources

2.3.3 Reporting: reliability of reporting

2.3.4 Compliance: compliance with applicable laws and regulations.

Figure 2.1 COSO Enterprise Risk Management: Integrated Framework

Components of Enterprise Risk Management Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

2.3.5 Internal Environment: The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity s people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

2.3.6 Objective Setting: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity s mission and are consistent with its risk appetite.

2.3.7 Event Identification: Internal and external events affecting achievement of an entity subjective must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management s strategy or objective-setting processes.

2.3.8 Risk Assessment: Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

2.3.8.1 Qualitative Approach: A qualitative risk analysis prioritizes the identified project risks using a pre-defined rating scale. Risks will be scored based on their probability or likelihood of occurring and the impact on project objectives should they occur.

2.3.8.2 Quantitative Approach: A quantitative risk analysis is a further analysis of the highest priority risks during a which a numerical or quantitative rating is assigned in order to develop a probabilistic analysis of the project.

2.3.9 Risk Response: Management selects risk responses avoiding, accepting, reducing, or sharing risk developing a set of actions to align risks with the entity s risk tolerances and risk appetite.

2.3.10 Control Activities: Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

2.3.11 Information and Communication: Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.

2.3.12 Monitoring: The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them.

2.4 Good Practice Guideline 2010 [8]

Good Practice Guidelines (GPG) 2010 is intended for use by practitioners, consultants, auditors and regulators with a working knowledge of the rationale for BCM and its basic principles. The Good Practice Guidelines 2010 still covers the six phases of the BCM Lifecycle but now links them more directly to what are now defined as Professional Practices. The six Professional Practices are sub-divided into two Management Practices and four Technical Practices.

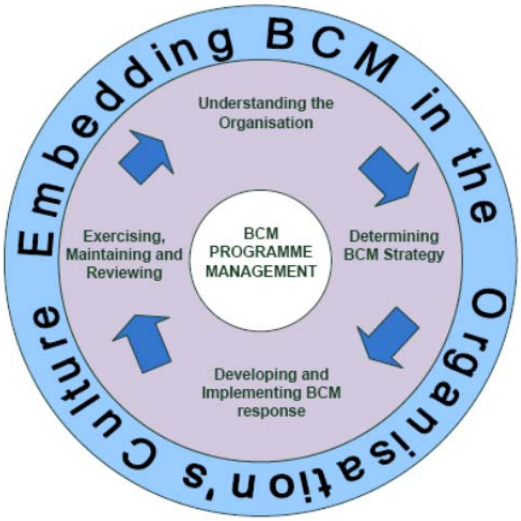

Figure 2.2 Business Continuity Management Life Cycle

2.4.1 BCM Programme Management

The BCM Policy is the key document that sets out the scope and governance of the BCM programme, and reflects the reasons why BCM is being implemented. It provides the context in which the required capabilities will be implemented, and identifies the principles to which the organization aspires and

against which its performance can be audited. A BCM programme needs to reflect the organization's strategy, objectives and culture to ensure that the programme is relevant, effective and appropriate. The organization will have a culture, but this may not be well documented or articulated by Top management. However, the organization's strategy and objectives will have been determined and agreed as part of the business planning and budgetary processes.

2.4.2 Understanding the Organization

Understanding the Organization is the professional practice within the BCM Lifecycle that reviews an organization in terms of what its objectives are, how it works functionally and the constraints of the environment in which it operates. The information collected makes it possible to determine how best to prepare an organization to be able to manage disruptions which might otherwise seriously or fatally damage it. The organization must make a prior, clear decision on whether the BCMS will cover the whole organization or just certain products or services. This sets the scope of the Business Impact Analysis (BIA), Continuity Requirements Analysis (CRA) and Evaluating Threats stages. The tools for understanding your business for Business Continuity purposes are:

2.4.2.1 Business Impact Analysis (BIA) – for evaluating the impact over time of a disruption to an organization's ability to operate

2.4.2.2 Continuity Requirements Analysis (CRA) – to estimate the resources, facilities and external services that each activity will require at both resumption and return to normal after a disruption

2.4.2.3 Evaluating Threats through Risk Assessment – to estimate the likelihood and impact on specific functions from known threats

2.4.3 Determining Business Continuity Strategy

Determining Business Continuity Strategy is the professional practice within the BCM Lifecycle that determines which BCM strategies will meet the BCM Policy and organizational requirements and selects tactical responses from available options. Determining Business Continuity Strategy' uses the information obtained

from the analyzes in the ‘Understanding the Organization’ stage of the BCM process to identify and select recovery and continuity options. This will enable the organization’s activities to become operational following an interruption, before the organization’s continued survival is threatened by their loss. It consists of three elements:

2.4.3.1 Identifying and Selecting Strategies

2.4.3.2 Identifying and Selecting Tactical Responses from Available Options

2.4.3.3 Consolidating Resource Levels

2.4.4 Developing and Implementing a BCM Response

Developing and Implementing a BCM Response is the professional practice within the BCM Lifecycle that implements agreed strategies through the process of developing a set of Business Continuity Plans. The key requirements for an effective response are clear procedure for the escalation and control of an incident. Communication with stakeholders. Plans to resume interrupted activities. Regardless of the cause the incident which causes a business interruption or impact, there must be a documented and fully understood incident response structure in place.

2.4.5 Exercising, Maintaining and Reviewing BCM

Exercising, Maintaining and Reviewing BCM is the professional practice within the BCM Lifecycle that seeks to ensure continuous improvement is achieved through the ongoing and scheduled actions. The activities undertaken in this section will be underpinned by the BCM Policy discussed in professional practice. The purpose of the Exercise Programme is to ensure that over a period of time:

2.4.5.1 All information in plans is verified

2.4.5.2 All plans are rehearsed

2.4.5.3 All relevant personnel (including deputies) are exercised

2.4.6 Embedding BCM in the Organization's Culture

Embedding BCM in the Organization's Culture is a dynamic and evolving process which is both complex and multifaceted. It must be constantly refined and shaped, so as to enable an organization to improve its strategic alignment and performance in the environment in which it operates. If the culture is appropriate then an effective strategy can be implemented. The established view of organizational culture is often portrayed as the combined assumptions, beliefs, values and patterns of behavior that are shared by members of an organization. These are often not consciously understood but when taken together they create the way an organization views itself, its place in its market and the environment in which it operates.

2.5 ISO 22301 Societal security - Business Continuity Management System – Requirement [9]

ISO 22301 is the world's first international business continuity management system standard. Previously published as the British Standard BS 25999, it is now widely accepted worldwide by various organizations as ISO 22301. This international standard specifies the requirements for setting up and managing an effective Business Continuity Management System for any organization, regardless of type or size.

ISO 22301 specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise. The requirements specified in ISO 22301 are generic and intended to be applicable to all organizations (or parts thereof), regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity.

This International Standard specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS). A BCMS emphasizes the importance of

2.5.1 Understanding the organization's needs and the necessity for establishing business continuity management policy and objectives

2.5.2 Implementing and operating controls and measures for managing an organization's overall capability to manage disruptive incidents

2.5.3 Monitoring and reviewing the performance and effectiveness of the BCMS

2.5.4 Continual improvement based on objective measurement.

2.6 The Plan-Do-Check-Act (PDCA) model [10]

This International Standard applies the “Plan-Do-Check-Act” (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's BCMS.

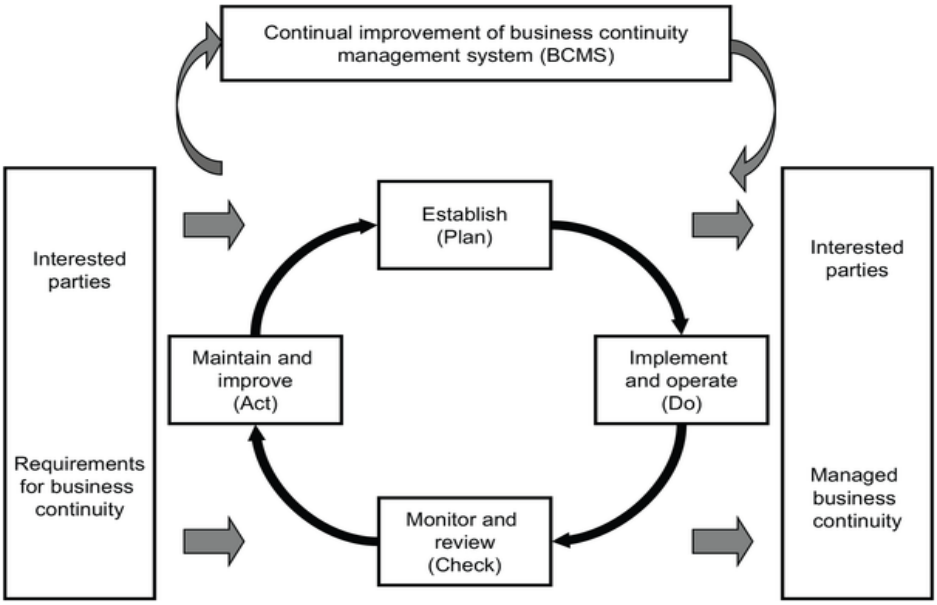

Figure 2.3 PDCA model applied to BCMS processes

In the Plan-Do-Check-Act model this International Standard cover the following components.

2.6.1 Plan: Establish business continuity policy, objectives, targets, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.

2.6.2. Do: Implement and operate the business continuity policy, controls, processes and procedures.

2.6.3 Check: Monitor and review performance against business continuity policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.

2.6.4 Maintain and improve the BCMS by taking corrective action, based on the results of management review and reappraising the scope of the BCMS and business continuity policy and objectives.

Figure 2.3 shows a business continuity management system that uses the need for business continuity of other related organizations through procedures, including critical processes, in order to achieve business continuity concurrent with needs.

2.7 Business Continuity Planning (BCP) [11]

Business continuity plans are written work plans establishing processes to support or recover work to normal function in order to enable businesses to work continuously. Companies must make business continuity plans in writing and receive approval from the company's board of directors, or high-ranking executives, or designated work committees. Furthermore, all business continuity plans should be kept by the parties responsible.

Business continuity plans must cover all essential company work, including work systems critical to the company that are provided by external service providers and constantly revised to be up to date in order to ensure that plans to work as needed. Furthermore, organizations should set details for methods of action in business continuity plans as suitable for the size and complexity of their respective businesses and covering all disruptions potentially occurring in any situation, including cases with effects on the business continuity that are long term or broad in nature. All sectors involved need to be involved in the drafting of business continuity plans in order to support the critical work of each respective department. The development of a BCP manual can have five main phases Analysis Solution design Implementation Testing and organization acceptance Maintenance.

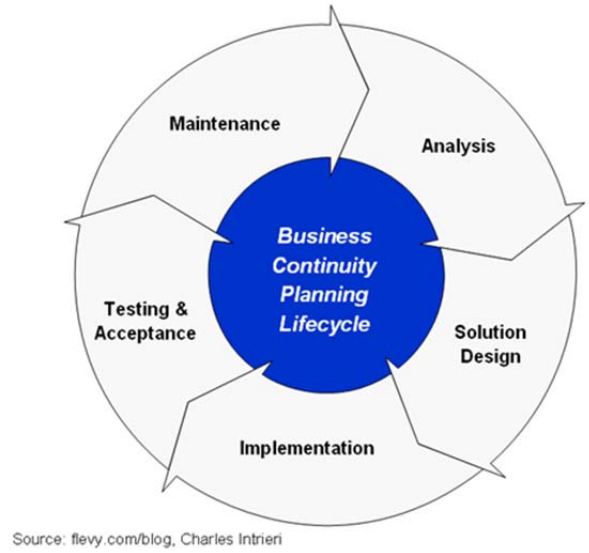

Figure 2.4 Business Continuity Planning Lifecycle

2.7.1 Analysis Phase the analysis phase in the development of a BCP manual consists of an impact analysis, threat analysis, and impact scenarios with the resulting BCP plan requirement documentation. An impact analysis results in the differentiation between critical (urgent) and non-critical (non-urgent) organization functions/ activities. A function may be considered critical if the implications for stakeholders of damage to the organization resulting are regarded as unacceptable. Perceptions of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if dictated by law. For each critical (in scope) function, two values are then assigned:

2.7.1.1 Recovery Point Objective (RPO) - the acceptable latency of data that will be recovered

2.7.1.2 Recovery Time Objective (RTO) - the acceptable amount of time to restore the function

2.7.1.3 The Recovery Point Objective must ensure that the Maximum Tolerable Data Loss for each activity is not exceeded. The Recovery Time Objective must ensure that the Maximum Tolerable Period of Disruption (MTPD) for each activity is not exceeded.

Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the business requirements for recovery of the critical function and the technical requirements for recovery of the critical function.

2.7.2 Solution Design Phase: The goal of the solution design phase is to identify the most cost effective disaster recovery solution that meets two main requirements from the impact analysis stage. For IT applications, this is commonly expressed as the minimum application and application data requirements and time frame in which the minimum application and application data must be available.

2.7.3 Implementation Phase: The implementation phase, quite simply, is the execution of the design elements identified in the solution design phase. Work package testing may take place during the implementation of the solution, however; work package testing does not take the place of organizational testing.

2.7.4 Testing and Organization Acceptance Phase: The purpose of testing is to achieve organizational acceptance that the business continuity solution satisfies the organization's recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws, or solution implementation errors. Testing may include Crisis command team call-out testing. Technical swing test from primary to secondary work locations. Technical swing test from secondary to primary work locations for Application test. Business process test. At minimum, testing is generally conducted on a biannual or annual schedule. Problems identified in the initial testing phase may be rolled up into the maintenance phase and retested during the next test cycle.

2.7.5 Maintenance Phase: Maintenance of a BCP manual is broken down into three periodic activities. The first activity is the confirmation of information in the manual, roll out to ALL staff for awareness and specific training for individuals whose roles are identified as critical in response and recovery. The second activity is the testing and verification of technical solutions established for recovery operations. The third activity is the testing and verification of documented organization recovery procedures. A biannual or annual maintenance cycle is typical.

BCP may be a part of an organizational learning effort that helps reduce operational risk associated with lax information management controls. This process may be integrated with improving information security and corporate reputation risk management practices.

2.8 Business Continuity Management Framework

Business Continuity Management Framework	1. Roles and responsibilities of the board of directors or high-ranking executives	
	2. Analysis and Evaluation of Impacts on Disruptions to Critical Work	2.1 Risk Assessment
		2.2 Business Impact Analysis
		2.3 Critical Business Function
	3. Setting Goals for the Recovery of Work to Normal Function	3.1 Maximum Tolerable Period of Disruption
		3.2 Setting strategies for the recovery of normal function
	4. Business Continuity Plans	
	5. Communication Plans	
	6. Training	
	7. Testing and Revision of Business Continuity Plans	

Figure 2.5 Business Continuity Management Framework

2.8.1 Roles and responsibilities of the board of directors or high-ranking executives

The board of directors or high-ranking executives must give importance to creating business continuity because they are responsible for setting risk management policies, scopes for creating substantial business continuity and strategies together with the allocation of resources and budgets, including the allocation of budgets for the creation of business continuity. The aforementioned board of directors and high-ranking executives can appoint other work committees involved, e.g., incident

management teams or BCM operational teams in order to delegate business continuity work to the committees.

2.8.2 Analysis and Evaluation of Impacts on Disruptions to Critical Work

The analysis of organizational impacts and risk assessments are used to evaluate the impacts on critical work disruptions as follows:

2.8.2.1 Risk Assessment (RA) assess risks by identifying risks with potential impact on the business to the point of disruption, single point of failure, assessment of risk impacts and the modification of processes in order to reduce the likelihood and effects of the aforementioned risks. Risks must be assessed at least once per year or when situations change as well as when internal or external factors can affect the organization, i.e. damaged information technology systems, temporary and permanent loss of critical staff, or damage caused by natural disasters, etc. During the risk assessment process, two factors are assessed, namely, the likelihood of the risk and the impact of the risk. In general, risk assessments take into consideration the controlled activities already functioning. Risk assessments can consider the likelihood and impacts of risks by categorizing the risks into five levels as shown in the table below.

Table 2.1 Shows the probability and risk impact assessment.

Rate	Level	Probability
1	Very Low	An event that is highly unlikely to occur, if ever.
2	Low	An event that is unlike to occur, perhaps once every 3 years.
3	Medium	An event likely to occur relatively infrequently, perhaps once a year.
4	High	An event that is fairly probable, and could be expected to occur several time a year.
5	Very High	An event that could be reasonably expected to occur at least every month or more frequently.

Rate	Level	Impact
1	Very Low	Data Asset remains functional for the business with no noticeable slowness or downtime.
2	Low	Impact on the data asset is small and limited. Would not cause any disruption in core functions.
3	Medium	Threat may cause some intermittent impact on the data asset, but would not lead to extended problems.
4	High	Serious impact on the data asset's functionality.
5	Very High	Catastrophic effect on the data asset.

Risks can be assessed and divided into five levels of risks with a total risk score of 25. Risk assessment results on the likelihood and impacts are used to produce the risk assessment matrix.

Table 2.2 Risk Assessment Matrix

Impact	Probability				
	1=Very Low	2=Low	3=Medium	4=High	5=Very High
Very Low (1)	1	2	3	4	5
Low (2)	2	4	6	8	10
Medium (3)	3	6	9	12	15
High (4)	4	8	12	16	20
Very High (5)	5	10	15	20	25

According to the table, risks are assessed by using issues or risks in each subject prioritized. The numbers obtained from the assessment are compared with the table in order to show the acceptability of risks (as shown in the table below). High-ranking executives of the organization must jointly assess risks and give importance to the aforementioned process.

Table 2.3 Risk Rating Matrix

Risk Level	Risk Rating	Consequence level	Mission Effects
Low	1-3		Expected losses have little or no impact on mission success.
Medium	4-9		Expected degraded mission capabilities in terms of required mission standards. Reduced mission capacity (if hazards occur during the mission).
High	10-16		Significantly degraded mission capabilities in terms of required mission standards. Not accomplishing all part of the mission or not completing the mission to standard (if hazards occur during the mission).
Very High	17-25		Mission failure if hazardous incidents occur in execution.

2.8.2.2 Business Impact Analysis (BIA) is an analysis of impacts on the organization's work in order to identify processes, procedures and critical activities. If incidents occur and cause disruptions, work might be affected. Consideration must be given to ordering the level of importance and urgency of work systems requiring recovery to normal function. Each work system analyzed for business impacts needs to be considered wholely in various aspects, namely, finance, image, legal, various regulations, etc.

2.8.2.3 Critical Business Function (CBF) apply Risk Assessment and Business Analysis when emergencies or incidents cause disruptions to critical work in order to establish clarity in identifying the importance of each work system in order to respond to emergencies or disruptions to ensure the organization can maintain function.

2.8.3 Setting Goals for the Recovery of Work to Normal Function

2.8.3.1 Maximum Tolerable Period of Disruption: Establishing a timeframe for setting strategy for the recovery of critical work systems is composed of the following:

- Maximum Tolerable Period of Disruption: MTD
- Recovery Time Objective: RTO
- Recovery Point Objective: RPO

In setting the aforementioned values, results are to be obtained from the business impact analysis, risk assessment and the prioritization of critical work. Furthermore, the aforementioned must be obtained from high-ranking executives or persons with decision-making authority.

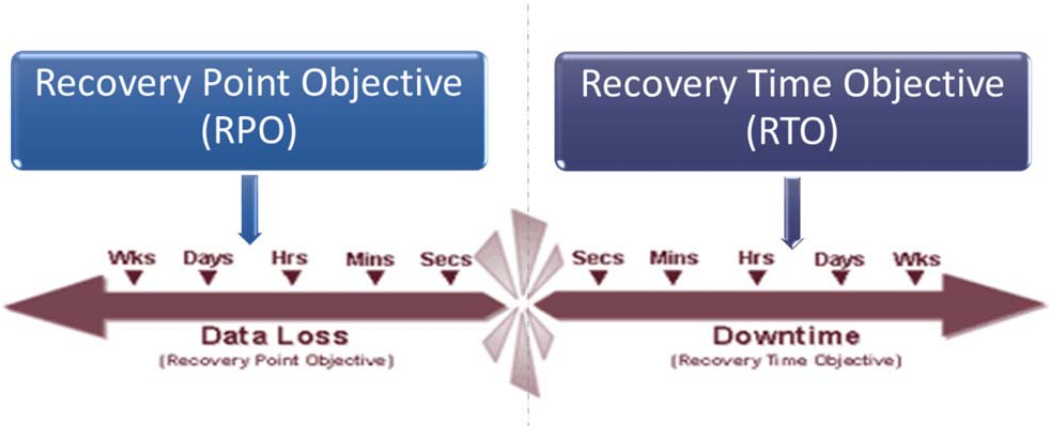

Figure 2.6 Maximum Tolerable Period of Disruption

2.8.3.2 Setting strategies for the recovery of normal function: six resources are available to support business processes and work when estimating the amount of resources necessary for the recovery of critical work of the organization in order to minimize impact from the incident making the resources unavailable, damaged, or insufficient for demands as follows:

Figure 2.7 Resource Level Consolidations

- People: the setting of corporate infrastructure and the setting of roles and responsibilities for people, including the setting of information technology departments with clear responsibilities for work systems, e.g., networks, servers, etc. in order for effective decision-making and communication during times of crisis.

- Premises: Backup premises should not be located near the primary premises, and the backup premises should be located in areas in which data is accessible conveniently and quickly during times of crisis. Backup premises also include good storage locations of data backup systems.

- Technology: Information technology necessary for information technology work systems, such as hardware components, software components, network accessories, etc. in order to allow for designs of backup work systems specified by the organization.

- Critical Information: Information technology data critical to the organization, for which critical information technology data must be set in order to backup data and prevent damaged or lost data.

- Stakeholders: Stakeholders can be divided into the following two parts:

- Internal departments of the organization are departments that drive processes and procedures in line with the information technology system recovery plan according to the specified work system prioritization.

- External departments of the organization are service provider departments of services, such as hardware work systems, software work systems, networking systems, etc. External departments need to be prepared or ready when incidents occur, and the departments must be able to specify the time for the recovery of services.

Supplier/Equipment factors are demands for equipment or other production factors to provide support for work to be able to proceed according to plans during emergencies.

2.8.4 Business Continuity Plans

Business continuity plans (BCP) are documented plans specifying procedures to support or recover work to normal function in order to ensure ongoing business operations. Organizations must draft business continuity plans in writing and receive approval from the organization's board of directors or high-ranking executives.

The first item that will aid the board of directors or high-ranking executives in making decisions for the business continuity plan are Business Impact Analysis and Risk Assessment. Business Impact Analysis and Risk Assessment are used to identify the primary work systems and resources critical to the organization when disrupted during incidents. Operational procedures and people responsible for operations are then set by clearly delegating the responsibilities of those responsible. Communication plans are also made with the people involved by specifying methods and modes of communication. The organization should drill the plans in order for the organization's personnel to have understanding of their responsibilities. Finally, the organization must revise the BCP plan in order to keep it up to date at all times to ensure that work proceeds as intended.

Thus the organization should set action details in the business continuity plan as suitable for the size and complexity of the organization's business with coverage of all disruptions potentially occurring in any situation, including cases of

long-term or widespread emergencies by instructing the departments involved to jointly draft business continuity plans in order to support the critical work of their respective departments.

2.8.5 Communication Plans

Communication plans are put in place to facilitate communication by members of the business continuity management committee and business continuity team according to the list appearing in the list data table during emergencies with the purpose of having the ability to manage communication between the personnel of each department after the announcement of an emergency or critical situation.

When incidents occur, the Call Tree procedure will report events back to the personnel involved and the business continuation management committee to organize meetings, acknowledge and assess the risks and impacts on the work and services, including resources critical to the management of business continuity.

2.8.5.1 Training is a procedure important to the assurance that the BCM process created by the organization is ready for actual plan exercise, along with testing the ability of the personnel and effectiveness of the plan in response to incidents. The testing format is as follows:

- Call Tree training is a drill on the reporting of emergencies to involved team members according to the list of names and mode of communication.

- Tabletop Testing is a simulated meeting to exchange the opinions of the departments involved. The plans for each procedure are considered for effectiveness in order to determine whether or not they are capable of meeting the goals of the organization.

- Simulation: Test by simulating lifelike situations together with planned drills.

- Full BCP Exercise means a full test in which situations are made to resemble real life situations as much as possible.

2.8.6 Testing and Revision of Business Continuity Plans

The organization must have assurance regarding the preparations of the business continuation plan along with receiving certification for accuracy with drilling and revision of the BCP plan, including annual revisions to keep the plan up to date at all times. In other words, once changes caused by various factors result in disrupted work caused by incidents, assurance must be provided that the organization's business continuation plan can be put to practice. Additionally, the organization should record test details and revisions of the business continuation plans.

2.8.7 Definitions of Technical Terms

Business Continuity Management (BCM) is defined as a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. [9]

Business continuity planning (BCP) involves planning and procedural aspects, encompassing emergency response, crisis communications, business continuity and disaster recovery. [12]

Incident management planning (IMP) involves developing a plan in writing. It also involves training staff in incident procedures, keeping good records, reviewing your response after an incident, and clearly identifying whose responsibility it is to take certain actions if an incident actually happens. [13]

Disaster recovery planning (DRP) is the technical component of BCP and focuses on the continuity of information and communication technology systems that support business functions. [12]

Disaster means events with high impacts and severity to the lives and property of the organization, i.e., fires, floods, sabotage, earthquakes, etc.

Disruption means events related to or having impact on the organization's information technology system divided into the following two types: 1. Events that disrupt information technology services and 2. Events that cause delays to the information technology system and affect the work or usage of users.

CHAPTER III
MATERIALS AND METHODS

3.1 Introduction

Business continuity plans are created to prevent and minimize risks for the business of an organization in order to avoid disruption by various incidents. Therefore, high-ranking executives or the incident management team of the Crown Property Bureau are required to set clear directions and objectives in order to prioritize activities or work systems according to their level of importance for the business and to be able to promptly set strategies in response to situations or incidents, thereby resulting in business continuity. High-ranking executives or the incident management team must drive for the training of persons involved in the business continuity plan, including training to build understanding of the plan's procedures, in order to evaluate the effectiveness and ability of the created plan. Importantly, the business continuity plan must be reviewed regularly in order for the plan to remain up to date in line with current situations.

Figure 3.1 Methodology Framework

3.2 Study of Organization Structure

The Crown Property Bureau is a juristic person responsible for the care and management of His Majesty's personal assets with determination to manage the assets under the Bureau's responsibility to create sustainable benefits for communities, people and society as a whole by adhering to the principle of reasonability based on a foundation of sufficiency according to the social conditions and culture of communities, along with application of His Majesty's statements and work principles "understand, access and develop" in improving quality of life, including the promotion of activities for the benefit of Thai people and society. [14]

Hence, the Crown Property Bureau has created concepts for executives and staff to understand the foundations of sustainable corporate development in order to drive the organization toward stable and sustainable management.

Figure 3.2 Basis for sustainable development in Crown Property Bureau [14]

Table 3.1 Processes leading to the Crown Property Bureau's Mission [14]

Crown Property Bureau	
Mission	An organization established to manage His Majesty's personal assets by considering the sustainable benefits of all parties involved.
Vision	A model organization of the management of assets for the sustainable benefits of the collective public.
Strategic Goals	An organization that has work practices and services provided internally and externally that meet international quality and standards.
Critical Components	An organization of learning with shared ideology and basic knowledge and ability, with leaders being required to have good leadership and overall management skills.
Basic Factors	Staff management, work procedures, work systems and information technology and infrastructures.

The Crown Property Bureau gives importance to information technology work systems because the work systems are basic factors required by the organization in order to assure that the organization drives the staff's work forward.

Table 3.2 Critical Business Function

System	Business Unit	Functions
Bonanza Investment	Finance Department	- Wealth Management - Investment Management
Property Costumer Management System: PCMS	Real Estate Management Department Community Management Department Special Projects Department Business Promotion Department	- Costumer Management - Rent Management - Records and Contracts
Exchange (E-mail)	All Crown property Bureau	- Receive-Send E-mail - Calendar
Human Resource Management System: HRMS	Personal Management Department Finance Department	- Personnel - Recruitment - Payroll - Benefits

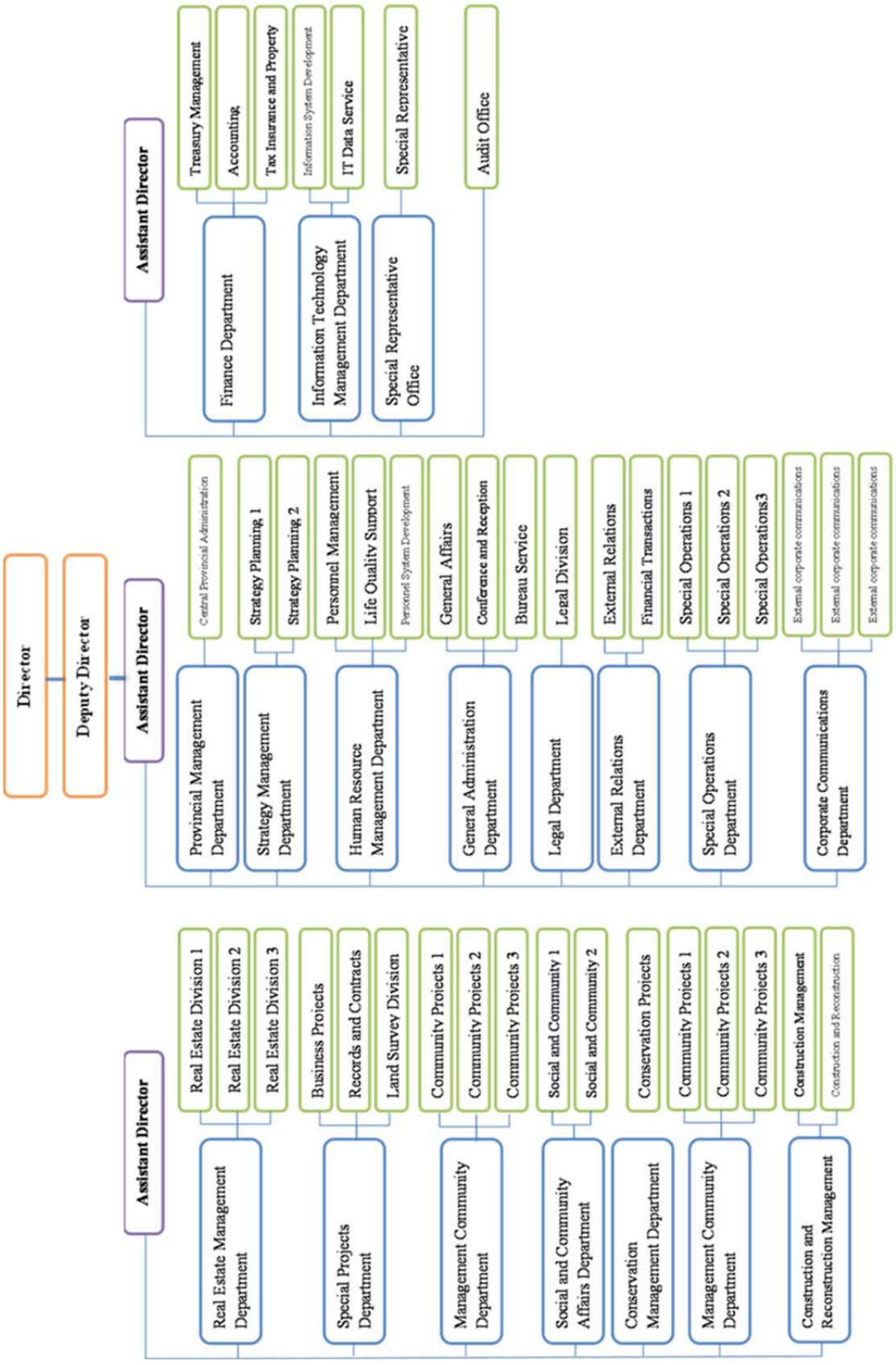

Figure 3.3 Organizational Structures Crown Property Bureau [15]

3.3 Risk Assessment

The impact analysis of information technology systems is performed in order to assess risks that might occur in each situation or disruptive situations, e.g., fires or crowd blockades. The impacts incurred can be considered in terms of the risk-creating factors in each situation that causes disruption to critical work systems. The impacts caused that cause the organization to incur damage or prevent the organization from operating must be analyzed.

Table 3.3 Analysis of Risks and Organization Impacts

No.	Risk Factors	Impact
1	Intrusions and Attacks	- Network System and Database Corruption - System can't provide - Data loss - Lack-Reliability IT Service
2	Political Demonstrations	- Server and Networking corruption - Denial of service - Data loss - The occupant cannot pay the rent - Lack-Reliability Organization
3	Disaster: - Blackouts/Exploded Transformers - Flooding	- Server and Networking corruption - Denial of service - Data loss - Close service company

According to the above table, risk factors affect impact on the information technology systems acting to support the work of the organization. Therefore, risk assessment must be performed in order to consider the impacts and severity level of

each situation, depending on the priority level of the information technology system required for the organization's work.

Once risks and organization impacts are analyzed, the impacts and probability of risk factors for each event are to be evaluated by completing the numbers of impacts and probability, depending on the severity level of each possible situation. The severity level is divided into five levels as shown in the Table below.

Table 3.4 Shows the probability and risk impact assessment.

Rate	Level	Probability
1	Very Low	An event that is highly unlikely to occur, if ever.
2	Low	An event that is unlike to occur, perhaps once every 3 years.
3	Medium	An event likely to occur relatively infrequently, perhaps once a year.
4	High	An event that is fairly probable, and could be expected to occur several time a year.
5	Very High	An event that could be reasonably expected to occur at least every month or more frequently.

Rate	Level	Impact
1	Very Low	Data Asset remains functional for the business with no noticeable slowness or downtime.
2	Low	Impact on the data asset is small and limited. Would not cause any disruption in core functions.
3	Medium	Threat may cause some intermittent impact on the data asset, but would not lead to extended problems.
4	High	Serious impact on the data asset's functionality.
5	Very High	Catastrophic effect on the data asset.

Afterwards, important risk factors are assessed for damage as shown in Table 3.2 by entering the numbers evaluated for risks into the Impact field. Probability is calculated as risk values according to the formula *"Probability * Impact = Risk Value"* in order to set management plans or measures to control risks from occurring at an unacceptable level. In addition, the numbers of the risk values are evaluated on the Risk Evaluation Table and the Acceptability Level Criteria Table. The aforementioned part will be used as criteria in deciding to exercise the business continuity plan.

Table 3.5 Risk Assessment and Risk Management Plans

Vulnerability	Threat	Likelihood	Impact	Risk Value	Managing Department
Blackout/ Transformer Explosion	- UPS equipment cannot supply power to networking machines for longer than 10 minutes. - Generators cannot provide service for more than 4 hours. - No drills for blackout situations.				- Shutdown of all information technology systems. - Prepare backup gasoline. - Perform a blackout drill once per year.
External Threats	- Damaged server computers and networking equipment. - The system fails to provide services. - Lost data.				- Back up data in order to prevent loss. - Design the system for safety.

Table 3.5 Risk Assessment and Risk Management Plans (cont.)

Vulnerability	Threat	Likeli hood	Impact	Risk Value	Managing Department
Flooding	- Water level at 30-40 centimeters from the floor level of the footpaths surrounding the building damages the insulation of the data center room. - Water levels of 40 centimeters and over from the level of the footpaths surrounding the building causes shutdown to the information technology system.				- Monitor the situation and remain alert. - Plan for the transfer of equipment to a safe location.
Fire	- Signal cables might be cut by fire. - If the fire exceeds one hour, equipment in the data center will be damaged. - No fire drills.				- Perform a fire drill once per year.

Table 3.5 Risk Assessment and Risk Management Plans (cont.)

Vulnerability	Threat	Likeli hood	Impact	Risk Value	Managing Department
Political Demonstrations	- The data center is at risk for dangers caused by politics. - Employees lose access to the Crown Property Bureau.				- Establish security measures. - Monitor the situation and remain alert.
Damaged Network Systems	- Internet link down: ISP cannot provide services. - Cut network signal cables.				- Follow-up on the status of the services for concurrence with the SLA agreement.
Technical Work Systems	- Data Back-up: the system might produce an error during data back-up. - Data Restoration: no regular data restoration tests to ensure readiness for situations.				- Set policies for backing up data. - Drill the Backup & Restore plan once per year.

Table 3.6 Risk Assessment Matrix

Impact	Probability				
	1=Very Low	2=Low	3=Medium	4=High	5=Very High
Very Low (1)	1	2	3	4	5
Low (2)	2	4	6	8	10
Medium (3)	3	6	9	12	15
High (4)	4	8	12	16	20
Very High (5)	5	10	15	20	25

Table 3.7 Risk Rating Matrix

Risk Level	Risk Rating	Consequence level	Mission Effects
Low	1-3		Expected losses have little or no impact on mission success.
Medium	4-9		Expected degraded mission capabilities in terms of required mission standards. Reduced mission capacity (if hazards occur during the mission).
High	10-16		Significantly degraded mission capabilities in terms of required mission standards. Not accomplishing all part of the mission or not completing the mission to standard (if hazards occur during the mission).
Very High	17-25		Mission failure if hazardous incidents occur in execution.

3.4 Business Impact Analysis and Recovery Time

Once disruption is caused by an incident, consideration must be given to the activities or work systems critical to the function of the organization in order to analyze and assess the situation in the respective activity or work system according to level of importance. Once the activities or work systems are prioritized, a period of time must be set for the return of the organization to normal function. The prioritization of activities or work systems and the setting of recovery times for activities and systems are set by high-ranking executives or the business continuity management committee.

Business impact analysis must prioritize activities or work systems then estimate the recovery time and input marks according to the acceptable recovery time of the respective activity or work system from disruptions as shown in the table below.

Table 3.8 Level of Maximum Tolerable Period of Disruption

System	Risk Level	Maximum Tolerable Period of Disruption			
		2 Hours	12 Hours	1 Day	2 Day
Server Services	Very High				
Network Services	Very High				
Backup Data	High				
UPS System	Very High				
CCTV System	High				
Internet Service	Medium				
Active Directory	High				
Exchange					
Intranet Service					
Investment System					
Human Resource Management System					

Table 3.9 Critical Business Function (CBF)

Priority	System	Recovery Time Object: RTO (Hour)
1	Exchange	
2	Bonanza Investment	
3	Human Resource Management System: HRMS	
4	Property Costumer Management System: PCMS	

3.5 Business Continuity Strategy

Due to the fact that critical activities or systems have different details for the resources used, whether the resources are external or internal to the organization, the recovery of activities or work systems to quick and timely function requires that the organization for preparing various resources be at hand in quantities sufficient to meet demands in order to support business continuity.

The preparation of resources necessary to the recovery of critical activities or work systems are divided in six main aspects, namely, people, premises, technology, information technology data, stakeholders and other equipment or factors. The details for each aspect are presented in the table below.

3.5.1 People

Table 3.10 Divisions within Crown Property Bureau

Divisions	System & Application	Note
- Finance Department	Bonanza Investment	
- Real Estate Management Department - Community Management Department - Special Projects Department - Business Promotion Department	Property Costumer Management System: PCMS	
- Personal Management Department - Finance Department	Human Resource Management System: HRMS	
- All Crown Property Bureau	Exchange	

Table 3.11 Vendors of Crown Property Bureau

Vendors	System & Application	Note
Outsourcing	Technical Support System	Control SLA
Internet Service Provider: ISP	Private Link	Control SLA
Internet Service Provider: ISP	Internet Link	Control SLA

3.5.2 Premises

Table 3.12 Requirements for premises

No.	Premises	Description	Note
1.	Backup Data Center Site	Reserve Server and Network	
2.	Build Operating Reserves	Working Reserve	
3.	Off Site Tape		

3.5.3 Supporting Technology

Table 3.13 Hardware Specification

No.	Hardware & Software	Type	Specifications
1.	Core Switch	Switch	
2.	Firewall	Firewall	
3.	Access Switch	Switch	
4.	Enclosure/Chassis	Blade Enclosure	
5.	Server	Blade Server	
6.	Storage	Disk Storage	
7.	Tape Library	Drive*2	
8.	Tape Backup	Tape	
9.	Rack	Rack Cabinet	

Table 3.14 Software feature

No.	Software	Type	Specifications
1.	MS Windows Server	Operating System	
2.	VMWare	System Software	
3.	MS Exchange Server	System Software	
4.	SW Backup	System Software	
5.	Oracle	Database System	

Table 3.15 Network Specification

No.	Technology	Type	Specifications
1.	Internet Link	Internet Service Provider	Bandwidth … Mbps.
2.	Private Link	Internet Service Provider	Bandwidth … Mbps.

3.5.4 Information

Table 3.16 Information Requirements

No.	Requirement	Detail	Note
1.	Network Diagram	Diagram Network System for Data Center to DR Site	Updated every 3 months.
2.	Server Diagram	Diagram Server for Data Center to DR Site	Updated every 3 months.
3.	Configuration Documentation	Detail of Install, Setting and Network System	
4.	Hardware Warranty Document	Start Date – End Date Service Level Agreement: SLA	
5.	Software Warranty Document	Start Date – End Date Service Level Agreement: SLA	

3.5.5 Equipment and Supplies

Table 3.17 Requirements of Equipment and Supplies

No.	Supplier/Equipment	Type	Mark
1.	Table / Chair		
2.	Conference Table		
3.	Cabinet		
4.	Computer		
5.	Printer		
6.	Power Plug		
7.	Mobile		

3.6 Contingency Plan and Communications

Drafted contingency plans are primary procedures allowing the business continuity plans of the organization to be successful according to the target recovery time of activities or work systems as specified in Table 3.9.

The drafting of contingency plans for business continuity plans references security management processes separated into three main parts that are critical to aiding the recovery time for situations to return to normalcy. The organization needs to set measures for the recovery of activities and work systems as follows:

- Before-incident monitoring
- During-incident response
- After-incident procedures

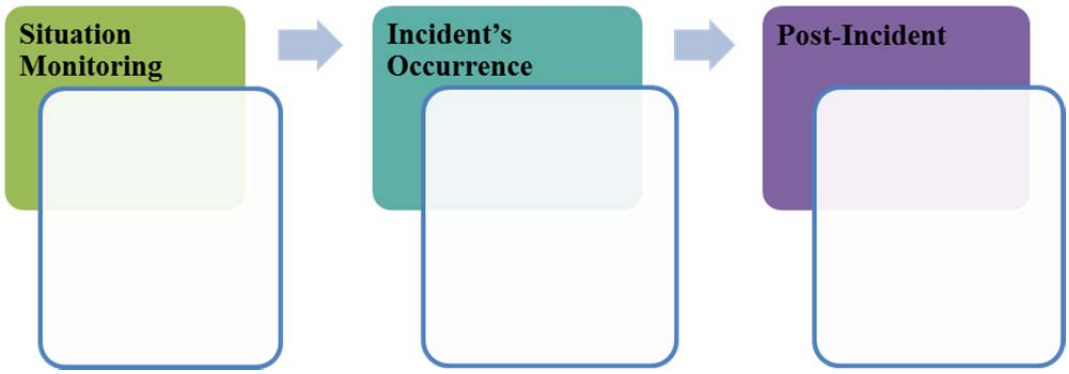

Figure 3.4 Security incident management procedures and controls

3.6.1 Before-Incident Monitoring

Before-incident monitoring is a process for preventing and alleviating damage caused by incidents in order to ensure that prioritized activities or work systems are able to function within a target period of time for the recovery of activities or work systems. The prioritization of procedures at this step is a measure that must be performed before the occurrence of incidents.

High-ranking executives or the business continuity management committee need to designate responsibilities for the monitoring and reporting of situations and safety in order to monitor the occurrence of incidents. If an unusual situation is discovered, the department that receives reports must be notified

immediately. In drafting plans, the details of the department that receives incident reports and the mode of communication should be specified in the table below.

Table 3.18 The show Emergency or disaster

Event	Event Notice	Phone Number	Time
Disaster Recovery	Security guard		Only 24 Hours
Disruption events	IT Call Center Team		**8.0 – 17.00**

3.6.2 During-Incident Response

In during-incident response, the person designated to report incidents is required to interview in order to gather the following minimum information:

3.6.2.1 Events

3.6.2.2 Name

3.6.2.3 Sector

3.6.2.4 Phone Number

3.6.2.5 Date and Time

3.6.2.6 Premises

3.6.2.7 Detail and Information

Once an incident occurs, the initial response is to control the situation from escalating to a severity level or taking actions toward decreasing the severity level back to normal. If the situation cannot be controlled and is not at an acceptable severity level according to situation severity evaluation criteria, separate the four severity levels as shown in the table below:

Table 3.19 Security and Safety Levels Evaluation Criteria of Situations

Severity Level	Incident Type and Severity	Procedure
1	Negligible incident (Follow normal management procedures)	• Small incident that does not affect critical situations. • The situation is expected to be resolved within a specified period of time. • The situation can be controlled and isolated with procedures for the management of disruptive incidents. Remarks: The System Recovery Team does not need to be notified.
2	Minor disruption to critical business process (Follow normal management) procedures)	• Small incidents affecting critical systems to the point of disruption. • The situation is expected to be resolved within a specified period of time. • The situation can be controlled and isolated with procedures for the management of disruptive incidents. Remarks: The System Recovery Team does not need to be notified.

Table 3.19 Security and Safety Levels Evaluation Criteria of Situations (cont.)

Severity Level	Incident Type and Severity	Procedure
3	Significant disruption (Exercise the system recovery plan with consideration of the situation)	• A moderately severe situation affecting critical situations to the point of disruption. • The situation is expected to be resolved within a specified period. • Close monitoring to prevent the situation from escalating or escalating in severity. • The situation is believed to be controllable and isolated by exercising the system recovery plan. Remarks: The System Recovery Team is transferred to take charge and order procedures.
4	Major disruption (Exercise the system recovery plan with consideration of the situation)	• An incident high in severity that impacts critical systems to the point of disruption. • The situation is expected to be resolved within a specified period of time. • Close monitoring to prevent the situation from escalating. • The situation is believed to be controllable and isolated by exercising the system recovery plan. Remarks: The System Recovery Team is transferred to take charge and order procedures.

If the severity level of the situation is assessed at 3 or 4, then the business continuity plan must be exercised, and the only person authorized to exercise the business continuity plan is the head of the business continuity management committee as shown in the table below.

Table 3.20 Priority of authority in Activate plan

No.	Priority	Position	Contact
1	Priority Number 1	Information Technology Management Department	Call: E-mail:
2	Priority Number 2	Information System Development Division Head	Call: E-mail:
3	Priority Number 3	Technology Management Section Head	Call: E-mail:

Thus, in order to prepare for the recovery of activities or work systems as priorities, roles and responsibilities, mode of communication and coordination of the team leader, teams of each department in the organization and external teams must be set in order to jointly recover the aforementioned activities or work systems to normal functions as shown in the table below.

Table 3.21 Name and Responsibility for Recovery System

Position	Name	Contact
Recovery Manager (1)		Call:
Recovery Manager (2)		Call:
Network Recovery Manager (1)		Call:
Network Recovery Manager (2)		Call:
Server Recovery Manager (1)		Call:
Server Recovery Manager (2)		Call:
Applications Recovery Manager (1)		Call:
Applications Recovery Manager (2)		Call:

Table 3.22 Information and communication for Team

Team	Name	Contact
Server Recovery Team		Call: E-mail:
Network Recovery Team		Call: E-mail:
Applications Recovery Team		Call: E-mail:
Call Center Team		Call: E-mail:

Table 3.23 Information and communication for External service providers

Name	Vendor	System	Contact
K.A	Company AA	Internet Service Provider	Call: E-mail:
K.B	Company BB	Internet Service Provider	Call: E-mail:

After the list of names and mode of communication in the business continuity plan are obtained, all six business continuity strategies must be exercised, namely, people, premises, technology, information technology data, stakeholders and other equipment and factors in order to ensure that critical activities or work systems continue to function.

3.6.3 After-incident procedures

This procedure involves the recovery of primary activities or work systems to a normal state. The persons authorized to order that the situation returns to normal are high-ranking executives or the chairman of the business continuity management committee. After the order is issued, the secretary of the business continuity management committee has to notify all people involved about the order, i.e. announcing that the recovery of the primary activities or systems are completed within

the set period of time, the return of operations from backup facilities to the primary facility and the return to normalcy.

3.7 Testing and Applying Plan

The testing of the business continuity plan requires that the format and type be set together with drilling courses in order to test and determine whether the plan can respond within the target recovery period of time for activities or work systems. Importantly, the plan must be reviewed and tested at least once annually in order for revisions to be made to keep the plan up-to-date and concurrent with situations. The details of the testing of the plan are to be recorded in the table below.

Table 3.24 Exercising, Maintaining and Reviewing BCM

Test	Type	Target Group	Date	Remark
Link Internet Down	Test System	IT	XX/XX/20XX	
Flood	Office Backup	All	XX/XX/20XX	

CHAPTER IV
RESULTS

4.1 Studying Organization Structure

The operational structure of the IT Department is conducted in each work section, including other departments within the organization involved in the procedures of the business continuity plan put in place as preparation for the occurrence of incidents to determine the procedures and actions that prepare the organization to respond to situations without disruptions to the organization's business function or work system. Whether or not and how severe situations will affect the organization's departments involves the following:

4.1.1 Interviewing IT People

The interview, analysis and collection of documents related to the management of emergency situations by the IT Department, including cases in which processes and procedures are at risk for disrupting the organization's business function or work system, is carried out by interviewing high-ranking executives all the way up to the operational level of the Information Technology Management Section in order to analyze the data obtained to create a business continuity plan for the critical work systems of the Crown Property Bureau as follows:

Business Unit	Description
Information Technology Management Section	Information Technology Infrastructure Services
Analysis and System Develop 1 Section	Business Application Support Services
Analysis and System Develop 2 Section	Core Business Application Services

4.2 IT Recovery Team Structure and Responsibilities

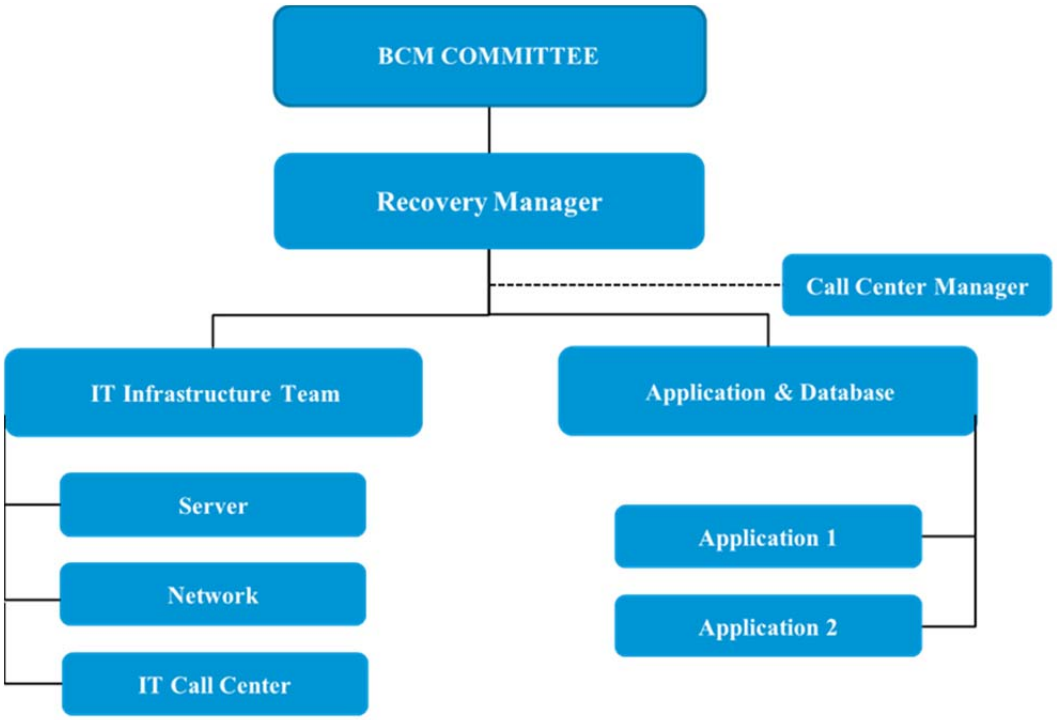

Figure 4.1 Structure of the recovery system.

4.2.1 Recovery Team Roles and Responsibilities

As the structure for the Recovery Team is set, it is necessary to set the roles and responsibilities for each position in order to assure that every member of the team is aware of their respective work scope and the work scope of other persons involved.

Table 4.1 Roles and Responsibilities

Position	Roles and Responsibilities
Recovery Manager	The Recovery Manager is the policy recipient of the Business Continuity Management Team (BCM) with the authority to appoint the Recovery Team and designate responsibilities for each team in order to be able to respond to incidents in time. The Recovery Team Leader is responsible for controlling and directing work in line with the goals and objectives of the business continuity plan and is the person responsible for periodically reporting the progress of situations to the BCM committee.
Call Center Manager	The Call Center Manager is responsible for the monitoring of disrupted situations. If the monitoring is outside working hours, the team leader providing service to users or designated persons must be contactable 24 hours a day. Reported incidents must be evaluated for severity, and the Recovery Team and the Recovery Team Leader must be notified.
Server Recovery Team	The Server Recovery Team is responsible for producing the list of servers, accessories and data critical to system recovery and the installation of system hardware, equipment and software. The Server Recovery Team is also responsible for recovering the system's data back to the time the disruption occurred.
Network Recovery Team	The Network Recovery Team is responsible for creating a list of systems, equipment, data and various firmware together with the installation necessary for system recovery. The system or equipment is installed in order to function as necessary.

Table 4.1 Roles and Responsibilities (cont.)

Position	Roles and Responsibilities
Applications Recovery Team	The Applications Recovery Team is responsible for the installation and modification of applications for the system to return to necessary function, and the Applications Recovery Team is responsible for system of the system's function, data checks and joint tests with users.
Call Center Team	The Call Center Team is responsible for reporting usage problems and analyzing reported problems in cooperation with the teams involved in order to resolve the reported problems together with coordinating with users to request usage tests.

4.3 The person authorized to execute the business continuity plan

The Business Continuity Management Team of the Crown Property Bureau has the authority to establish subcommittees or Recovery Teams responsible for the planning and ordering of operational procedures when incidents occur. Authority is given to the Recovery Team Leader to make decisions for the execution of the plan and occasional progress report if the incident is severe. Hence, the persons authorized to exercise primary and secondary plans must be specified respectively in cases where the primary person authorized cannot be contacted.

4.4 Situation Monitoring

Situations are monitored and observed in order to assess risks potentially affecting the work or disrupting the work system of the organization to determine the level of severity, along with analyzing and assessing the damages occurring, namely, fires, floods, etc. If the situation directly affects the organization and is high in severity, the person who encounters the situation must report to the personnel responsible and the recipient of the report must record the reported data, then investigate the situation occurring along with reporting to the Recovery Team Leader

and the team leaders of each respective work section in order to jointly monitor and assess the incident's severity. The risk assessment measure can be seen from Table 3.19: Measure of the Situation's Severity and Security.

4.5 When incidents occur:

The business continuity plan is executed only once a reported situation is sufficiently severe to disrupt function or work systems. The Recovery Team Leader must announce the execution of the business continuity plan and summon a meeting of the Recovery Team and other teams involved then the teams are to perform with duties as assigned in order for critical functions or work systems to be able to provide IT system services within to the determined time.

4.6 Situational Status Report

After the Recovery Team announces the execution of the business continuity plan, the team leader is required to explain the plan's details to all teams involved to be aware and discuss the plan's modification to adapt to current situations. The Call Center Manager has to coordinate and contact all teams involved in order to report situations and notify teams to take attendance and follow the plan as assigned. The reporting must begin with the primary person responsible. If the person cannot be contacted, then contact the secondary person responsible for each respective work section.

4.7 Business Continuity Plan Execution

The order for the operations of the business continuity plan on the occurrence of incidents as prepared in the practice guideline for the execution of the business continuity plan for different situations is shown in Figure 4.2.

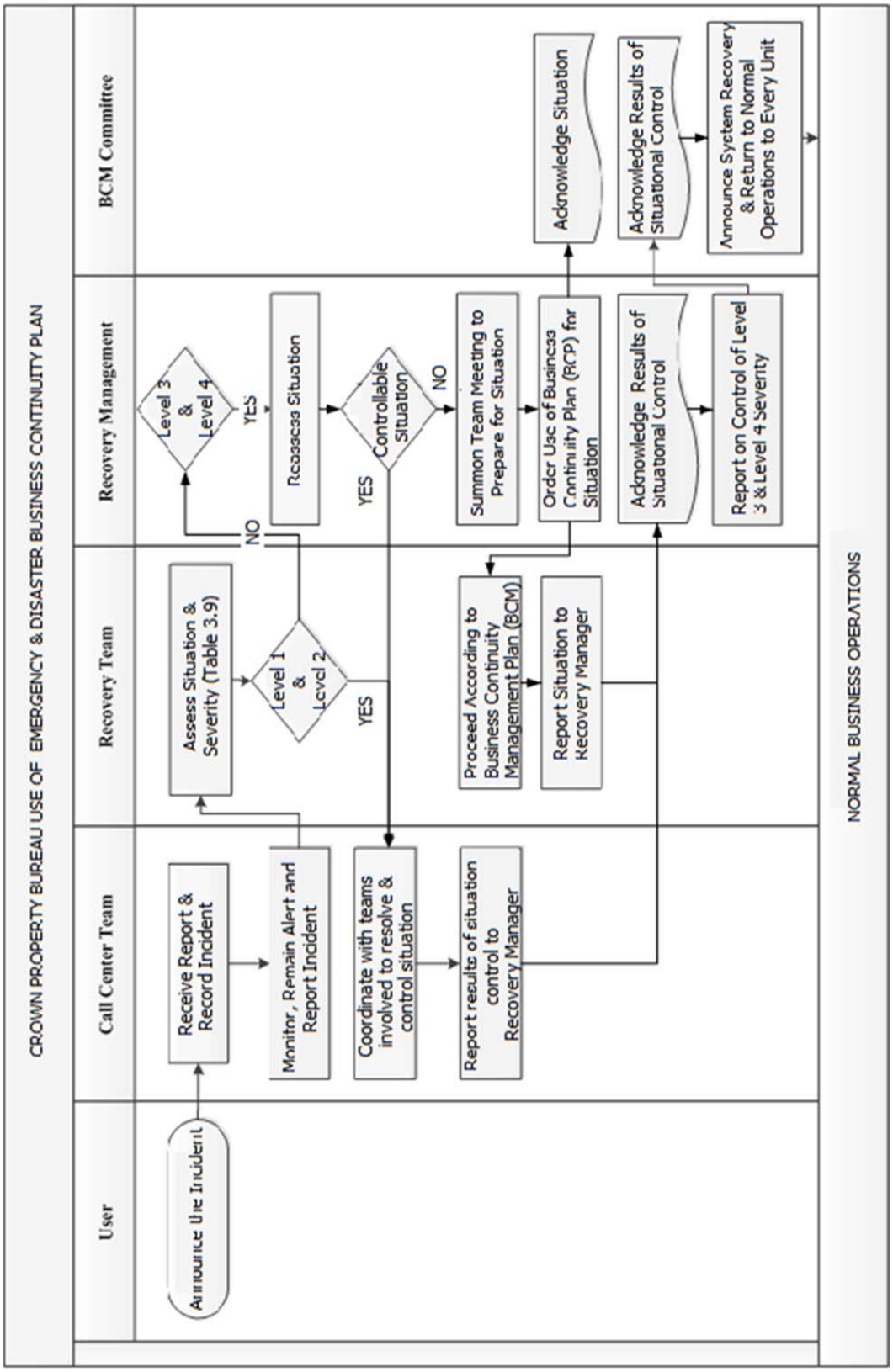

Figure 4.2 Practice Guideline for the Execution of the Business Continuity Plan upon the Occurrence of Incidents

4.8 Operation for returning to normalcy

Once the Recovery Team recovers the system, an announcement has to be made to all persons involved or all IT service users. The Recovery Team Leader must report the results of the recovery to the Business Continuity Management Team in order to request an announcement to notify the Crown Property Bureau staff about the return of the IT system to function according to the prioritization policies of work systems affecting the organization's business or function.

4.9 Execution of the Business Continuity Plan for Different Situations

According to the practice guidelines for the execution of the business continuity plan, the plan can be adapted for situations when incidents occur. Thus procedural plans have been prepared along with a simulation of potentially occurring situations to the Crown Property Bureau in order to test the effectiveness of the business continuity plan. The plan is tested in the following four potential situations:

- Blackouts/Exploded Transformers
- Flooding
- Political Demonstrations
- Disruptions to Critical Work

4.9.1 Blackouts/Exploded Transformers

4.9.1.1 Criteria for the plan's execution: The incident occurred with severity levels of three and four (according to Table 3.9) confirmation was received from the person authorized to execute the plan.

4.9.1.2 Operators: BCM Committee, Call Center Team, Recovery Manager, Recovery Team

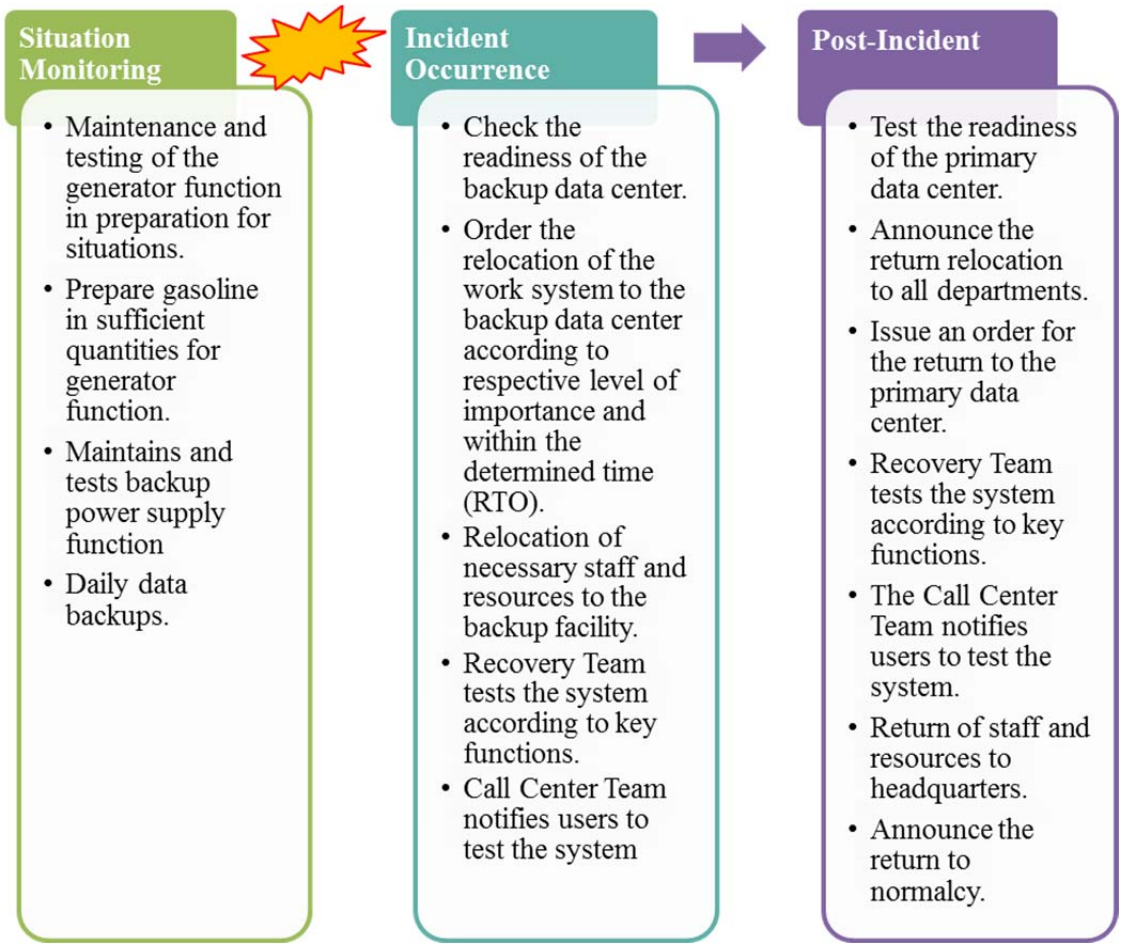

Figure 4.3 Order of operations for emergency plans upon the occurrence of blackouts or exploded transformers

4.9.2 Flooding

4.9.2.1 Criteria for executing the plan: The incident occurred with severity levels of three and four (according to Table 3.9) as confirmed by the person authorized to execute the plan.

4.9.2.2 Operators: BCM Committee, Call Center Team, Recovery Manager, Recovery Team

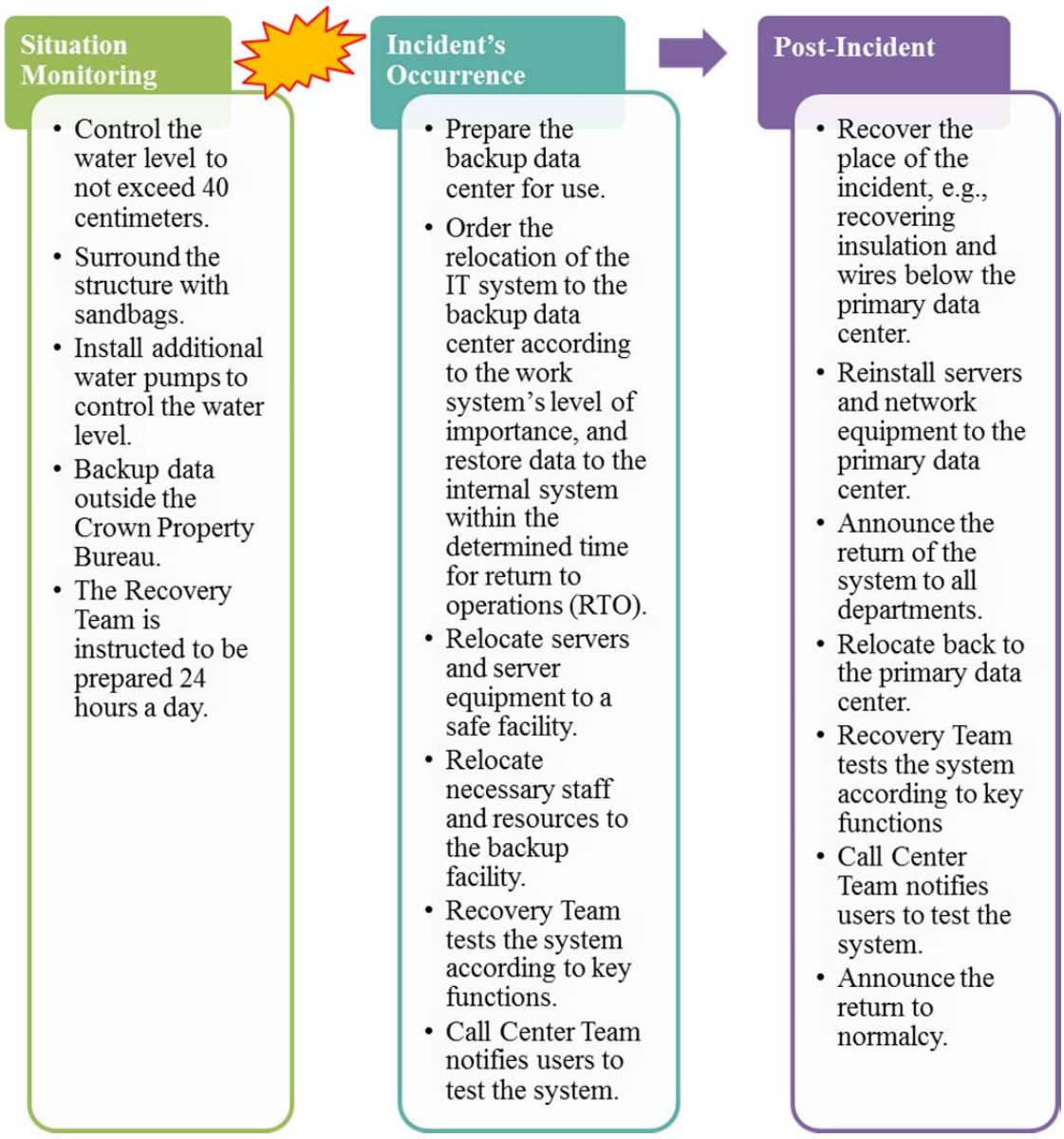

Figure 4.4 Order of operations for emergency plans upon the occurrence of flooding.

4.9.3 Political Demonstrations

4.9.3.1 Criteria for executing the plan: The incident occurred with severity levels of 3 and 4 (according to Table 3.9) confirmed by the person authorized to execute the plan.

4.9.3.2 Operators: BCM Committee, Call Center Team, Recovery Manager, Recovery Team

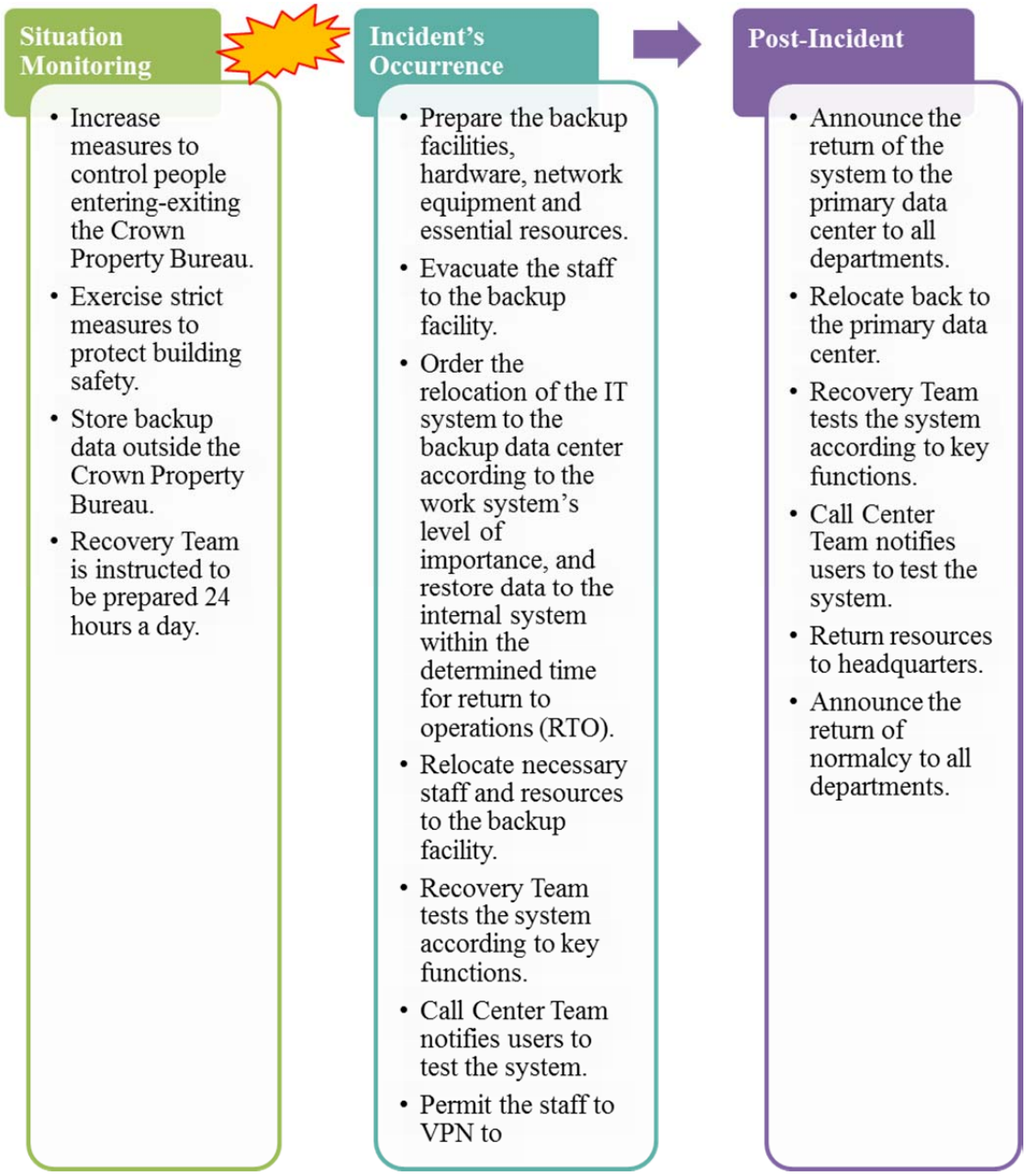

Figure 4.5 The order of operations for emergency plans upon the occurrence of political demonstrations.

4.9.4 Disrupted Critical Work

4.9.4.1 Criteria for executing the plan: The incident occurs with severity levels of three and four (according to Table 3.9) as confirmed by the person authorized to execute the plan.

4.9.4.2 Operators: BCM Committee, Call Center Team, Recovery Manager, Recovery Team

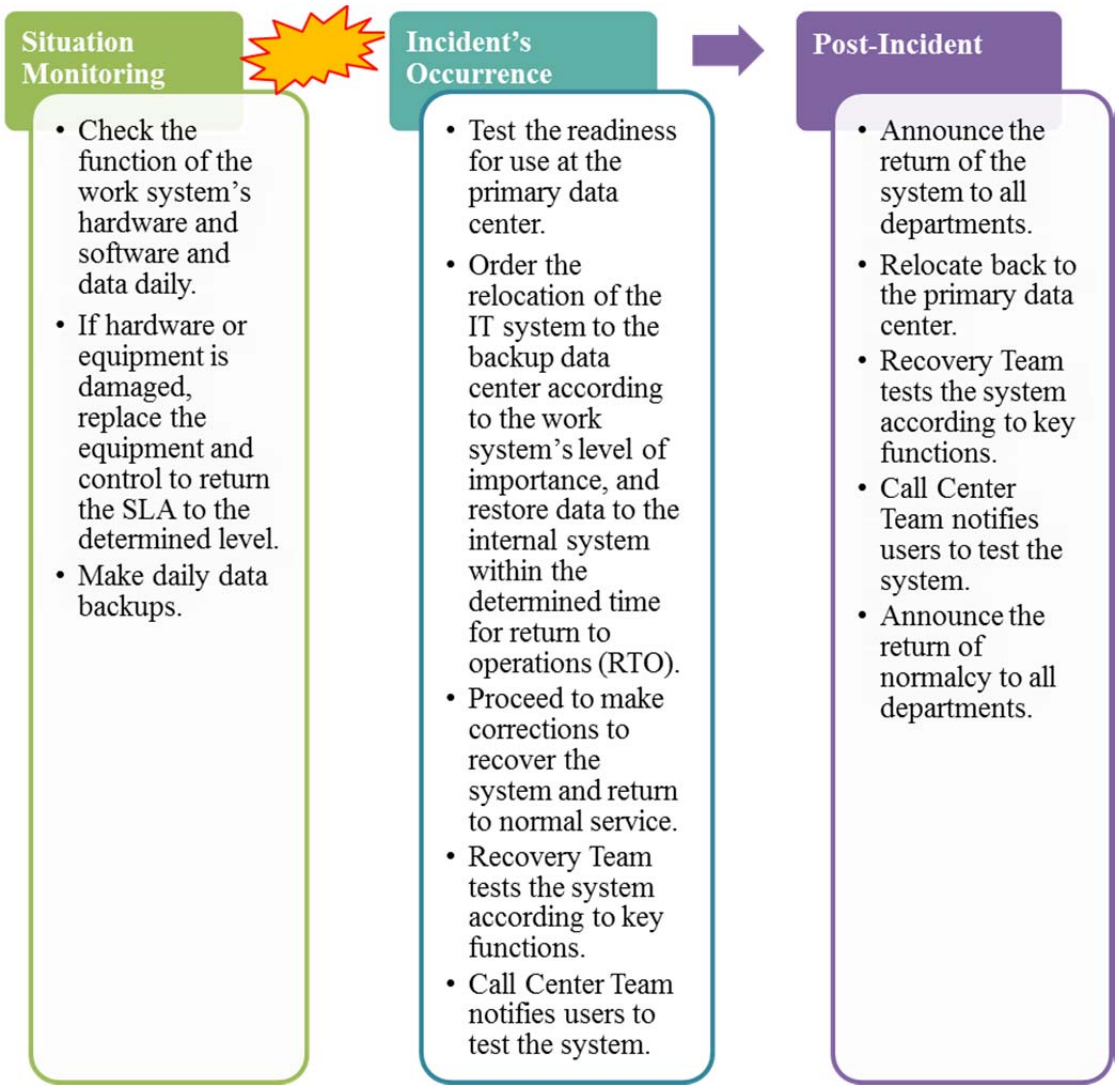

Figure 4.6 The order of operations for emergency plans upon the occurrence of disrupted work systems.

4.10 Test Results

4.10.1 Blackouts/Exploded Transformers

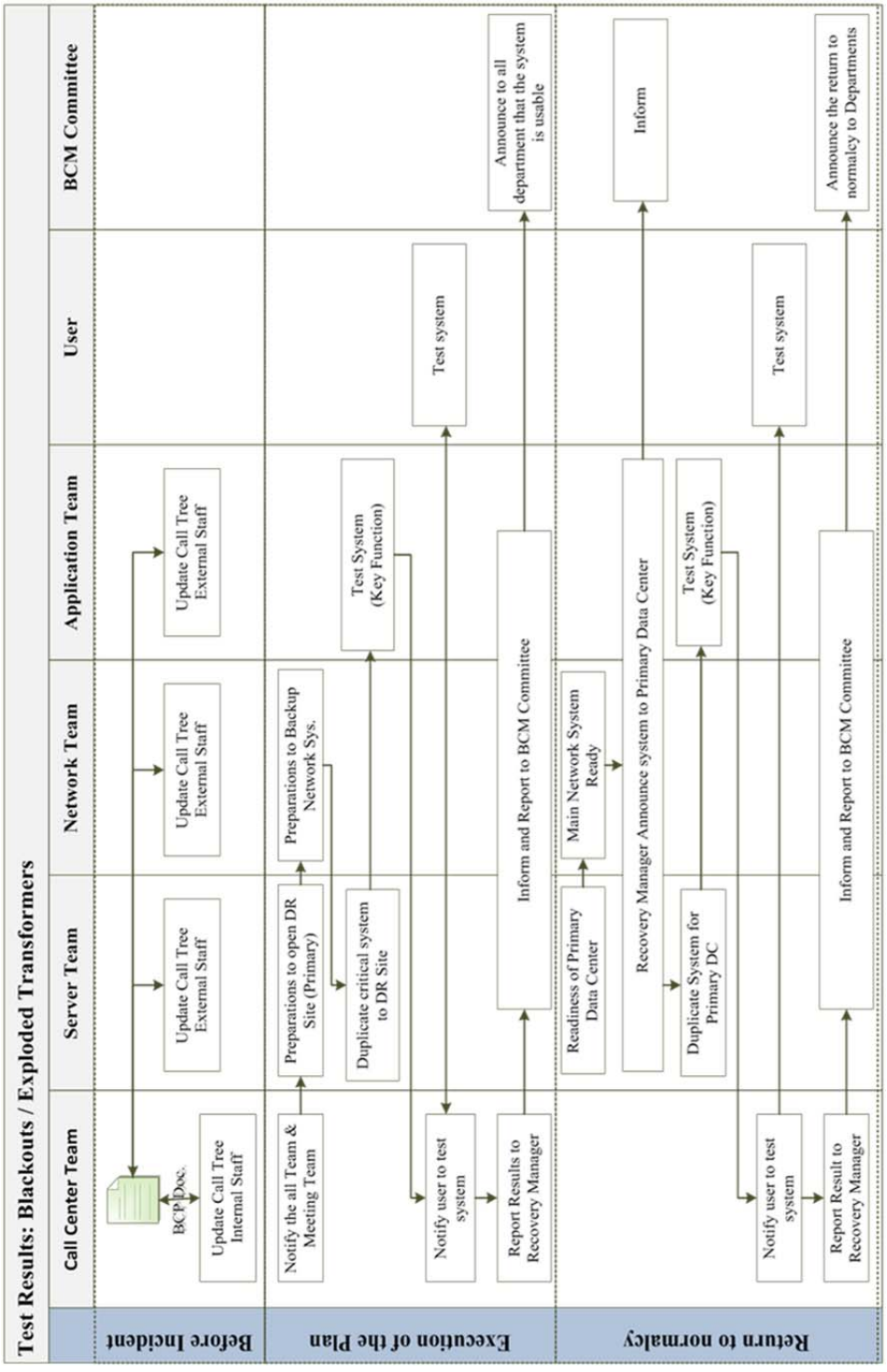

Figure 4.7 Test Results Blackouts/Exploded Transformers

4.10.2 Flooding

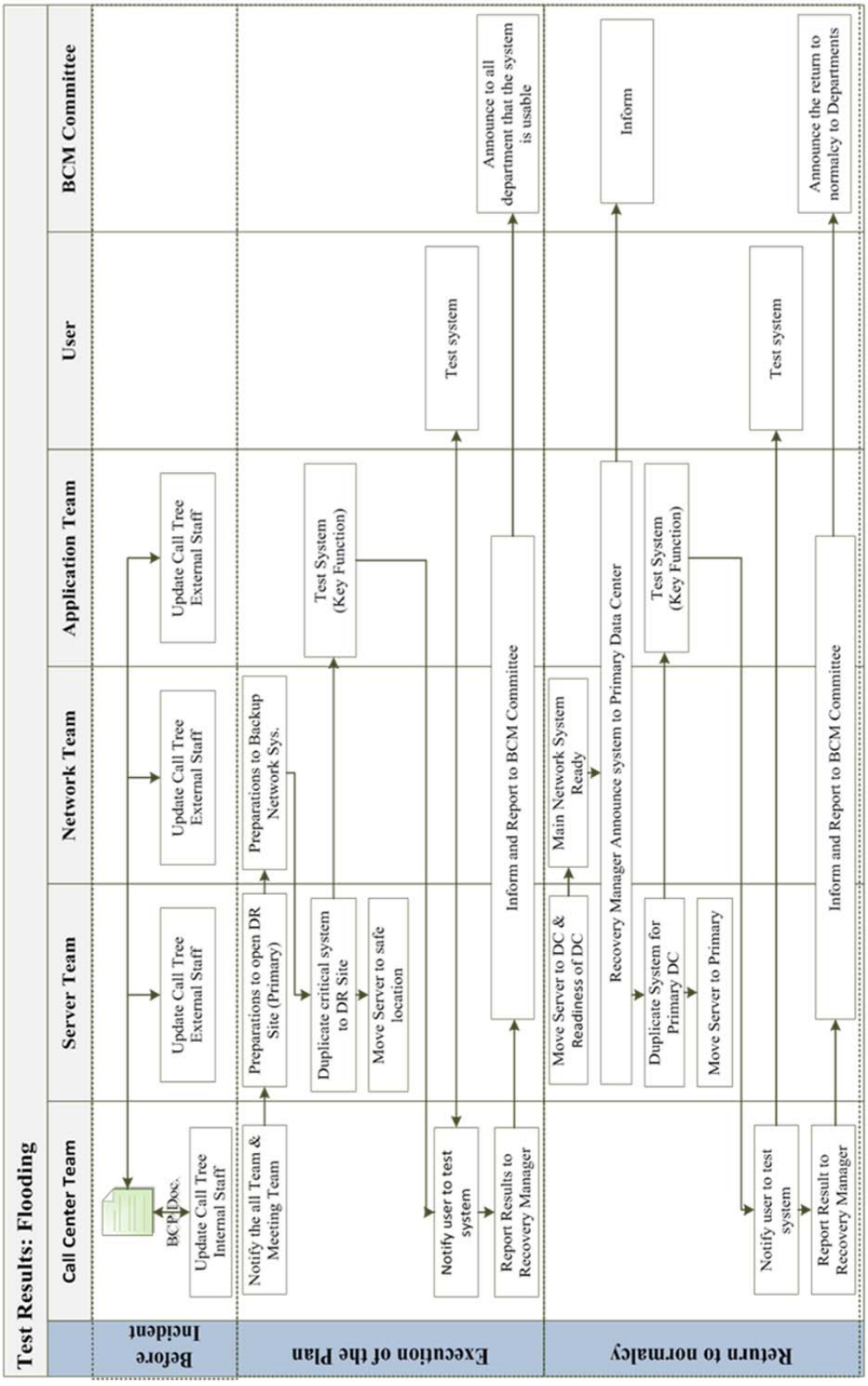

Figure 4.8 Test Results Flooding

4.10.3 Political Demonstrations

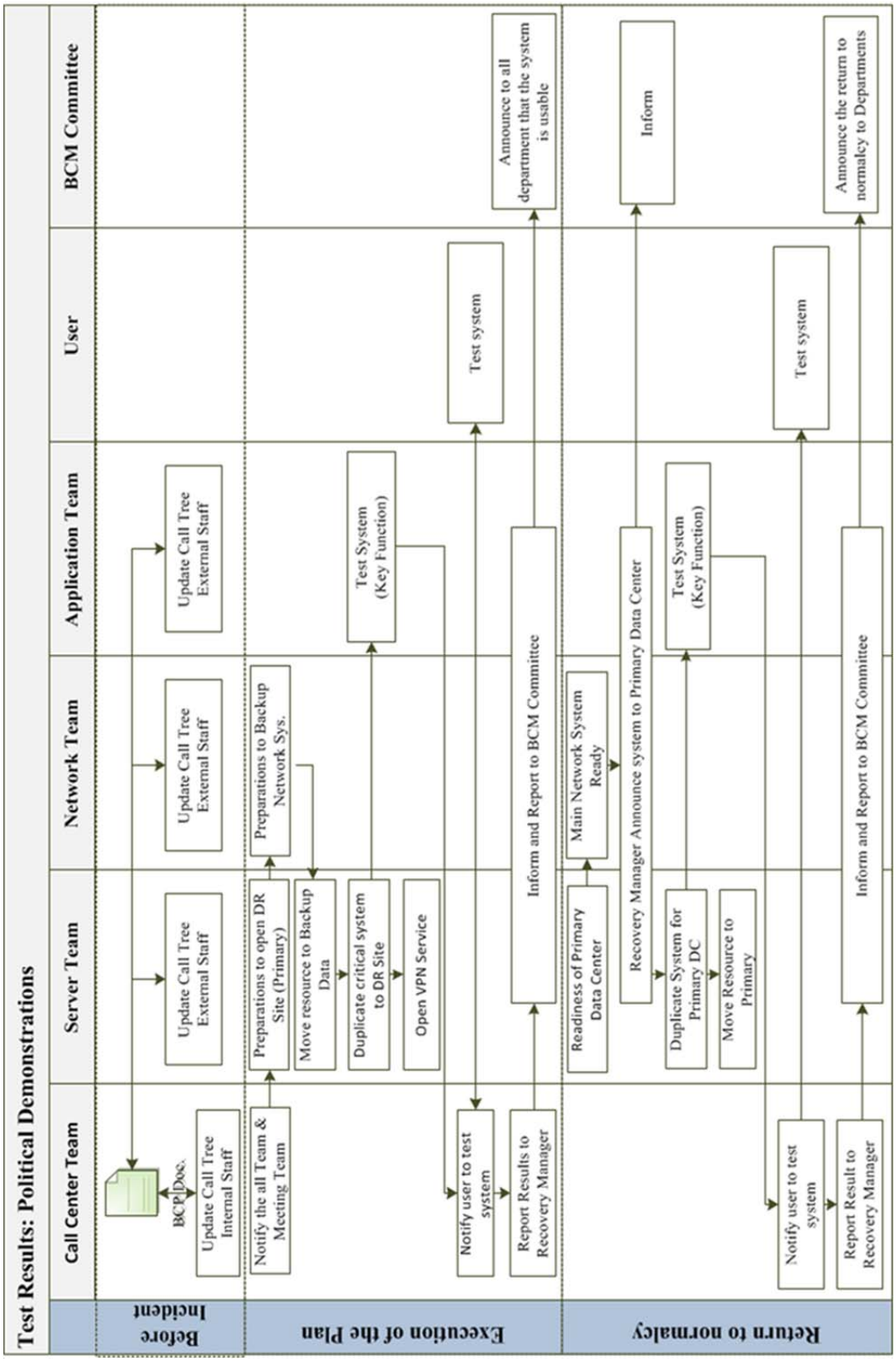

Figure 4.9 Test Results Political Demonstrations

4.10.4 Disruptions to Critical Work

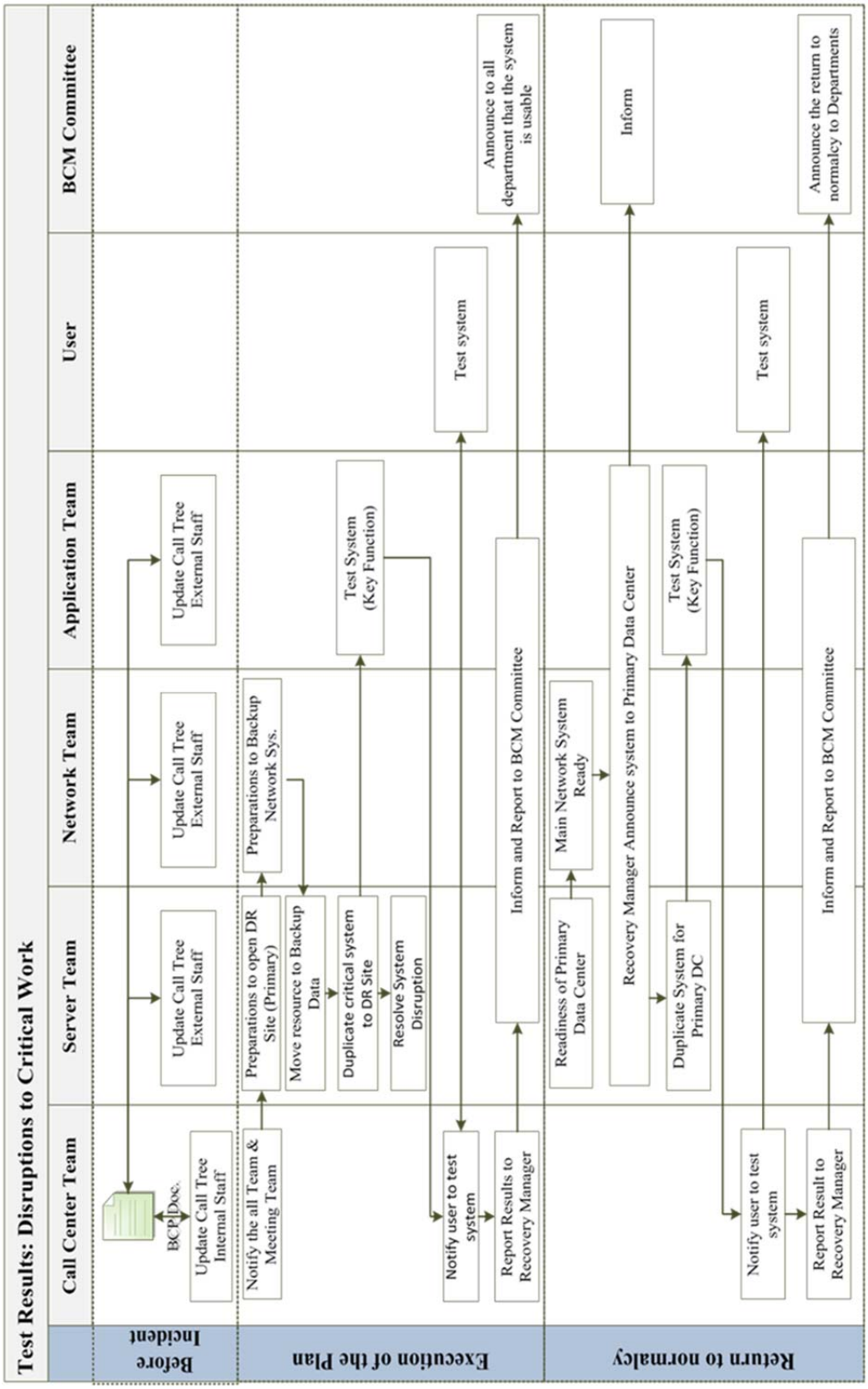

Figure 4.10 Test Results Disruptions to Critical Work

4.11 Evaluation of Business Continuity Plan Satisfaction

According to the business continuity plan developed by the Crown Property Bureau for incidents to create a level of confidence for the organization, staff and stakeholders, if unexpected events occur, critical work systems will be returned to normal function within a time determined by the organization or an acceptable timeframe as planned in order to ensure that the business continuity plan is effective and can respond to real situations.

Therefore, the business continuity plan was tested in different situations in order to use the test results to improve the plan for better concurrence with the objectives set by the organization. Hence, interviews were conducted in order to determine the level of satisfaction in following the business continuity plan and the level of satisfaction in the effectiveness of the work in accordance with set goals in the staff of the Information Technology Management Section, IT Department, by dividing the interviews into two groups, namely, 3 high-ranking executives and 25 IT staff, a total of 28 people interviewed. The topics interviewed to determine the satisfaction level in the testing of the plan are as follows:

- The organization’s image and credibility.
- Knowledge and understanding in operating under the business continuity plan.
- Clear setting of duties and responsibilities.
- Time taken for the system relocation to the data center as scheduled.
- Usability of the system after the system relocation.
- Ability to prevent and reduce damage to the Crown Property Bureau’s functions.
- Ability to prevent and reduce risks to the IT system.
- The suitability of the determined time for the system recovery.
- Suitability of the plans and procedures.
- Consistency with the policies of the IT Department.

4.11.1 Satisfaction Level

The interview for the satisfaction level of the testing of the business continuity plan of the Information Technology Management Section, IT Department, Crown Property Bureau is categorized according to the following satisfaction levels:

Table 4.2 Level of Satisfaction

Satisfaction Level	**Satisfaction Score**
Highest	5
High	4
Moderate	3
Satisfactory	2
Low	1

4.11.2 Evaluation and analysis of the level of satisfaction

The analysis of the satisfaction results according to the review calculated the percentage and mean of each answer of the people interviewed: $\text{Mean} = \frac{\text{Total Score}}{\text{Total Number of People}}$

Table 4.3 Analyzed Satisfaction Result obtained from High-Ranking Executives

Evaluation criteria	**Highest 5**	**High 4**	**Moderate 3**	**Satisfactory 2**	**Low 1**
1. The organization's image and credibility.	2	1			
2. Knowledge and understanding in operating under the business continuity plan.		1	2		
3. Clear setting of duties and responsibilities.		3			

Table 4.3 Analyzed Satisfaction Result obtained from High-Ranking Executives (cont.)

Evaluation criteria	Highest 5	High 4	Moderate 3	Satisfactory 2	Low 1
4. Time taken for the system relocation to the data center as scheduled.	1		2		
5. Usability of the system after the system relocation.		3			
6. Ability to prevent and reduce damage to the Crown Property Bureau's functions.	1	2			
7. Ability to prevent and reduce risks to the IT system.	1	2			
8. The suitability of the determined time for the system recovery.	1	2			
9. Suitability of the plans and procedures.	1	2			
10. Consistency with the policies of the IT Department.	2	1			

According to Table 4.7, the evaluation results of the high-ranking executives can be explained as follows:

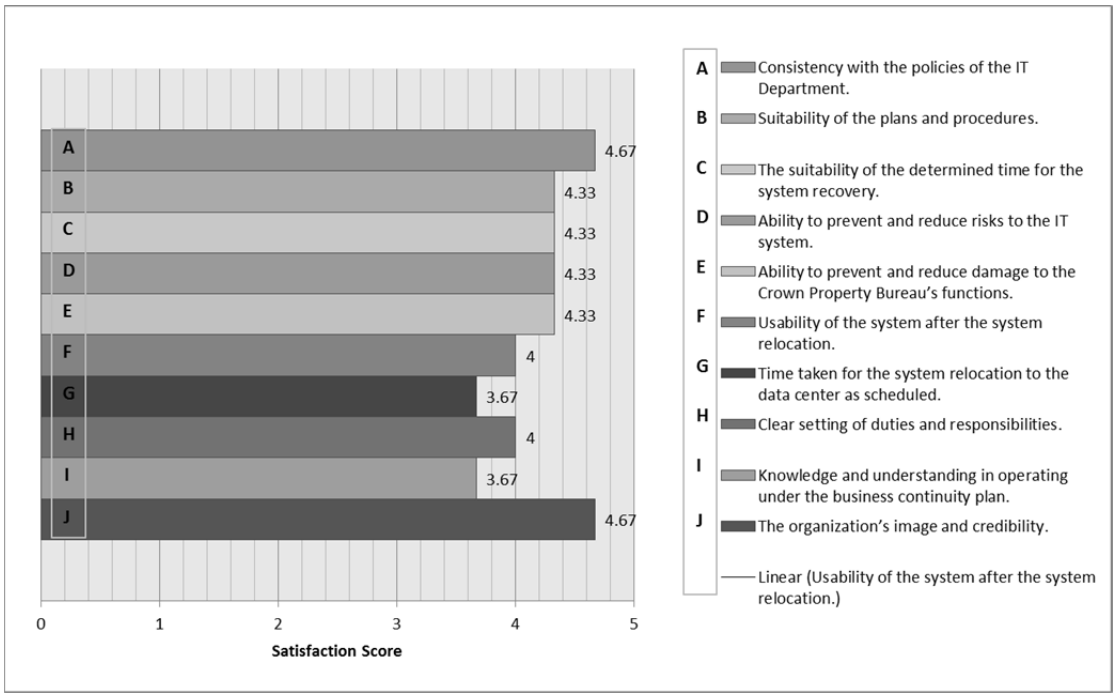

Figure 4.11 Evaluation and Analysis of satisfaction of 3 high-ranking executives

According to the evaluation and analysis of the mean satisfaction of 3 high-ranking executives were evaluated for on ten topics by which the following mean satisfaction scores were obtained: 4.67 for the organization's image and credibility; 3.67 for knowledge and understanding in operating under the business continuity plan; 4 for clearly set duties and responsibilities; 3.67 for time taken for the system relocation to the data center according to determined time; 4 for the usability of the system after the system relocation; 4.33 for the ability to prevent and reduce damage to the Crown Property Bureau's function; 4.33 for the ability to prevent and minimize risks to the IT system; 4.33 for the suitability of the determined time for the system recovery; 4.33 for the suitability of the determined time for the system recovery and 4.67 for the suitability of the determined time for the system recovery. When the overall satisfaction level of the high-ranking executives was calculated, the percent of satisfaction of the high-ranking executives to the business continuity plan equaled 82.6 percent.

Table 4.4 Satisfaction Results of the IT Staff

Evaluation criteria	Highest 5	High 4	Moderate 3	Satisfactory 2	Low 1
1. The organization's image and credibility.	11	14			
2. Knowledge and understanding in operating under the business continuity plan.	3	11	11		
3. Clear setting of duties and responsibilities.		18	7		
4. Time taken for the system relocation to the data center as scheduled.	11	14			
5. Usability of the system after the system relocation.		13	12		
6. Ability to prevent and reduce damage to the Crown Property Bureau's functions.	15	10			
7. Ability to prevent and reduce risks to the IT system.	13	12			
8. The suitability of the determined time for the system recovery.	1	13	11		
9. Suitability of the plans and procedures.	3	17	5		
10. Consistency with the policies of the IT Department.	4	21			

According to Table 4.8, the evaluation results of the IT staff can be explained as follows:

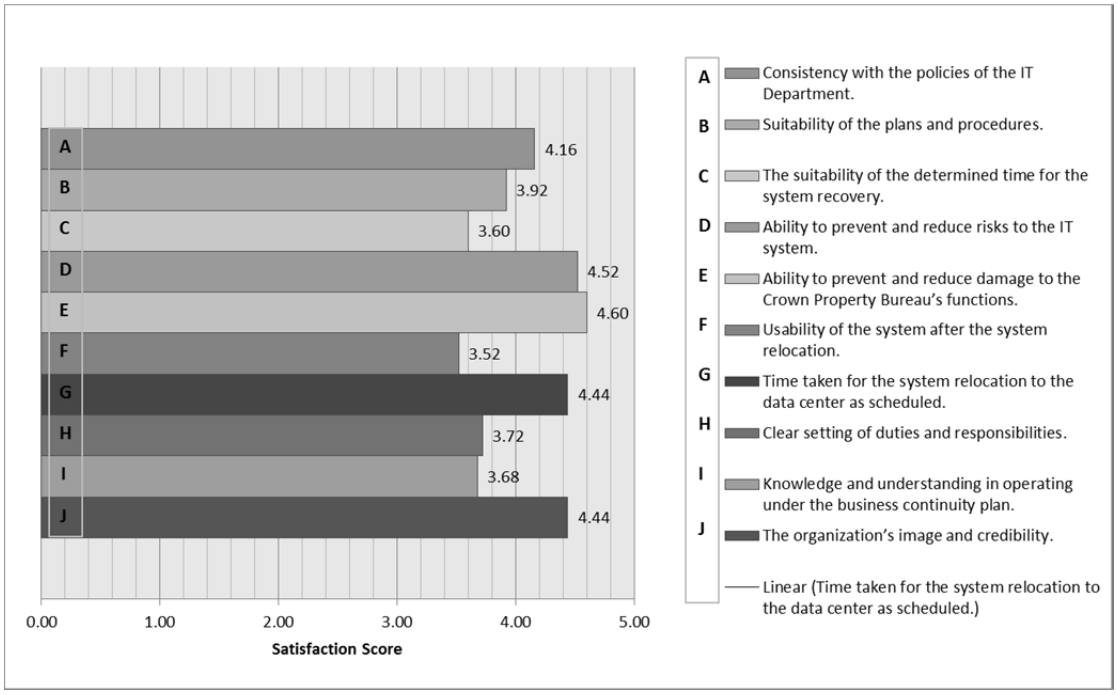

Figure 4.12 Evaluation and Analysis of satisfaction of 25 IT staff

According to the evaluation and analysis of the mean satisfaction of 25 IT staff were evaluated for on ten topics by which the following mean satisfaction scores were obtained: 4.44 for the organization's image and credibility; 3.68 for knowledge and understanding in operating under the business continuity plan; 3.72 for clearly set duties and responsibilities; 4.44 for time taken for the system relocation to the data center according to determined time; 3.52 for the usability of the system after the system relocation; 4.60 for the ability to prevent and reduce damage to the Crown Property Bureau's function; 4.52 for the ability to prevent and minimize risks to the IT system; 3.60 for the suitability of the determined time for the system recovery; 3.92 for the suitability of the determined time for the system recovery and 4.16 for the suitability of the determined time for the system recovery. When the overall satisfaction level of IT staff was calculated, the percent of satisfaction of IT staff to the business continuity plan equaled 81.2 percent.

4.11.3 Summary of Evaluation Results

The evaluation of the satisfaction results in the business continuity plan obtained by the interview of two groups of people, namely, high-ranking executives and the IT staff, obtained the following results:

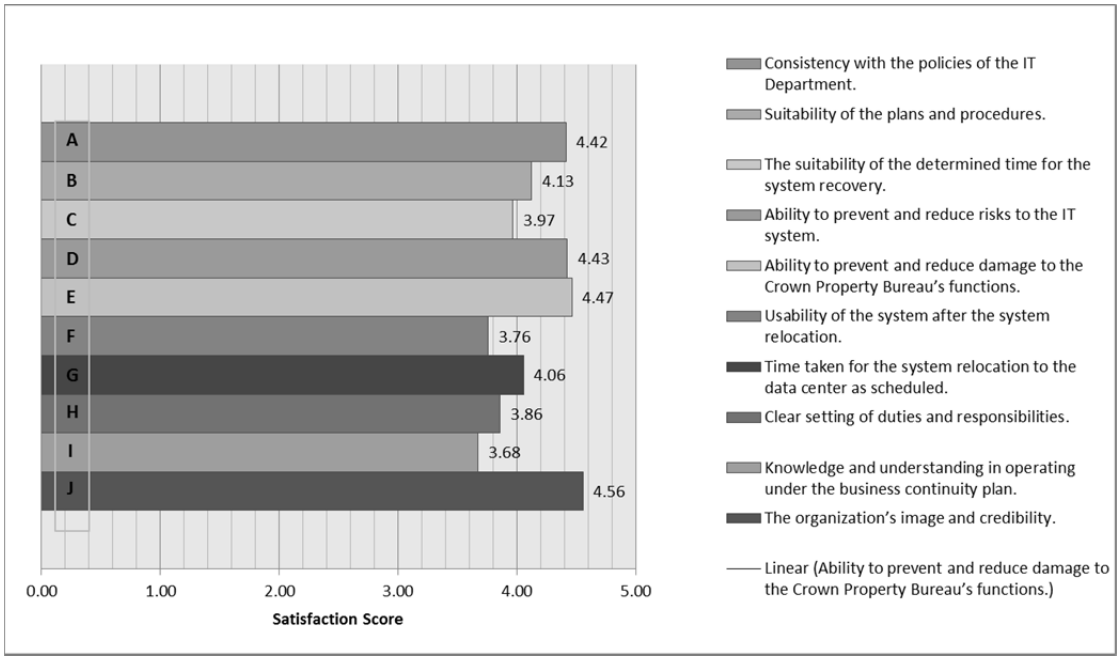

Figure 4.13 Evaluation and Analysis of satisfaction of both groups, a total of 28 people

According to the evaluation and analysis of the mean satisfaction of both groups, namely, 3 high-ranking executives and 25 IT staff, a total of 28 people were evaluated for on ten topics by which the following mean satisfaction scores were obtained: 4.56 for the organization's image and credibility; 3.68 for knowledge and understanding in operating under the business continuity plan; 3.86 for clearly set duties and responsibilities; 4.06 for time taken for the system relocation to the data center according to determined time; 3.76 for the usability of the system after the system relocation; 4.47 for the ability to prevent and reduce damage to the Crown Property Bureau's function; 4.43 for the ability to prevent and minimize risks to the IT system; 3.97 for the suitability of the determined time for the system recovery; 4.13 for the suitability of the determined time for the system recovery and 4.42 for the suitability of the determined time for the system recovery. When the overall satisfaction level of the high-ranking executives and IT staff was calculated, the

percent of satisfaction of the high-ranking executives and IT staff to the business continuity plan equaled 82.6 percent.

CHAPTER V
DISCUSSION AND CONCLUSION

The Business continuity plan for events where certain incidents or situations occur is the setting of operational procedures when situations severely affect the work systems critical to the business function of the Crown Property Bureau. If the business continuity plan is followed, unexpected situations can be handled and risks or damages affecting the organization's critical work can be reduced under the concept of risk management.

5.1 Research Summary

According to the study of the procedures of the business continuity plan, the Crown Property Bureau is in the phase of preparing backup facilities, including hardware and software as tools for the management of unusual situations. Nevertheless, procedures are not clearly prioritized in the drafting of the business continuity plan for persons involved with the management of abnormal situations and the management of unexpected events. The business continuity plan should be drafted in writing or a manual in order to aid procedures as follows:

- Exercise the business continuity plan in the Crown Property Bureau to create ordered processes for the handling and management of incidents.
- Set clear duties and responsibilities in the management of incidents.
- Quick and effective response and management to occurring events.

According to the study and test for creating a business continuity plan for the occurrence of incidents at the Crown Property Bureau Summary of satisfaction level for the test of the Crown Property Bureau's business continuity plan was evaluated in order to gain awareness of the plan's effectiveness and ability to meet the organization's needs. Furthermore, the evaluation of the business continuity plan can also be used to improve and develop the procedures of the plan for ease and

concurrence with the organization's needs. The satisfaction of the test of the business continuity plan is summarized by interviewing managers and staff of the Information Technology Development Division of the Department of Information Technology, divided into two groups, namely, 3 managers and 25 IT Department staff members. The topics for the interview are as follows:

- The organization's image and credibility
- Knowledge and understanding about operating under the business continuity plan
- Clearly set duties and responsibilities
- Time taken for system relocation to the data center as scheduled
- Usability of the system after the system relocation
- Ability to prevent and minimize damage to the Crown Property Bureau's functions
- Ability to prevent and minimize risks to the IT system
- The suitability of the schedule for the system recovery
- Suitability of the plans and procedures
- Consistency with IT Department policies

5.2 Research Limitations

According to the design for the business continuity plan for the occurrence of incidents, the following limitations were discovered:

5.2.1 Some managers give little importance to the drafting of the business continuity plan for incidents, possibly because the incidents have not yet occurred.

5.2.2 The staff members involved have no knowledge and understanding about the use of the business continuity plan.

5.2.3 The staff members involved have no awareness of situations posing severe risks that affect the function of the Crown Property Bureau.

5.3 Recommendations

According to the study and test for creating a business continuity plan for the occurrence of incidents at the Crown Property Bureau, areas of improvements for the plans were suggested. Therefore, the following recommendations are made for the benefit of interested persons as follows:

5.3.1 Managers and staff should have awareness of the effects causing severe risks if the organization encounters an incident.

5.3.2 Staff members involved with the business continuity plan who never took part in the plan should be encouraged to participate in the testing as planned in order to create understanding about the plan's operational procedures and for the staff to be able to put the plan into practice if incidents occur.

5.3.3 In order for the business continuity plan to be applied effectively, revisions to the plan must be done at least once annually, and the name list and contact information must be regularly updated.

REFERENCES

The Crown Property Bureau (2013). *ABOUT-CPB/History* [online], Available: http://www.crownproperty.or.th/en/ABOUT-CPB/History [accessed on 2013 Aug 25].

Prashanth Ananth, (2007), Business Continuity Planning, 1.

Rama Lingeswara, (2012), Key Issues, Challenges and Resolutions in Implementing Business Continuity Projects, 2.

Gluckman, David, (2000), Continuity....Recovery, 45.

Jennings Michael, (2002), The benefits of emergency notification systems, 54-55.

Canberra: Australian National Audit Office, (2002), Business continuity management: keeping the wheels in motion, 87.

Committee of Sponsoring Organizations of the Treadway Commission, (2004), Enterprise Risk Management 2004, 9-10.

HM Government, The Business Continuity Institute GOOD PRACTICE GUIDELINES 2010 Global Edition, 5-16.

ISO 22301:2012(en) (2012), Societal security Business continuity management systems Requirements.

The International Organization for Standardization, *Societal security — Business continuity management systems --- Requirements*, (2012). ISO 22301:2012(en) [online], available: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en [accessed on 2014 Jan 12].

Classle Learning is Social, Business continuity planning (BCP) [online], available: https://www.classle.net/book/business-continuity-planning-bcp [accessed on 2013 Oct 5].

Rama Lingeswara, (2012), Key Issues, Challenges and Resolutions in Implementing Business Continuity Projects, 1.

Queensland Government, (2013), Bus Incident Management Planning, Transport and Main Roads, March 2013.

The Crown Property Bureau (2013). *ABOUT-CPB/Mission* [online], Available: http://www.crownproperty.or.th/en/ABOUT-CPB/Mission [accessed on 2013 Aug 25].

The Crown Property Bureau (2013). Organization-Chart [online], Available: http://www.crownproperty.or.th/en/ABOUT-CPB/Organization-Chart [accessed on 2014 Feb 25].

APPENDIX

1. Blackouts/Exploded Transformers

Table A: Test Results: Blackouts/Exploded Transformers

Action	Team Responsible	Not Completed	Completed	Remarks
Before Incident				
1. Up-to-date Call Tree	Call Center Team			
2. Call Tree for external staff supporting the system's recovery.	Call Center Team Recovery Team			
Execution of Plan				
1. Notify the Recovery Team in the incident report and attend the meeting to prepare for the situation.	Call Center Team			
2. Make preparations to open the backup data center.	Recovery Team			
3. Make preparations for the backup network system.	Network Team			
4. Relocate critical work systems to the backup data center within the determined time for return to operations (RTO).	Server Team Application Team			

Table A: Test Results: Blackouts/Exploded Transformers (cont.)

Action	Team Responsible	Not Completed	Completed	Remarks
5. Test the system according to key functions.	Application Team			
6. Notify users to test the system.	Call Center Team			
7. Announce to all departments that the system is usable.	BCM Committee			
Return to normalcy				
1. Test the readiness of the primary data center.	Recovery Team			
2. Get the main network system ready.	Network Team			
3. Relocate the system back to the primary data center.	Server Team Application Team			
4. Test the system according to key functions.	Application Team			
5. Notify users to test the system's function.	Call Center Team			
6. Announce the return to normalcy to departments.	BCM Committee			

2. Flooding

Table B: Test Results: Flooding

Action	Team Responsible	Not Completed	Completed	Remarks
Before Incident				
1. Up-to-date Call Tree	Call Center Team			
2. Call Tree for external staff supporting the system's recovery.	Call Center Team			
Execution of Plan				
1. Notify the Recovery Team in the incident report and attend the meeting to prepare for the situation.	Call Center Team			
2. Make preparations to open the backup data center.	Recovery Team			
3. Make preparations for the backup network system.	Network Team			
4. Relocate critical work systems to the backup data center within the determined time for return to operations (RTO).	Server Team Application Team			

Table B: Test Results: Flooding (cont.)

Action	Team Responsible	Not Completed	Completed	Remarks
5. Relocate servers and equipment to a safe location.	Server Team Network Team			
6. Test the system according to key functions.	Application Team			
7. Notify users to test the system.	Call Center Team			
8. Announce to all departments that the system is usable.	BCM Committee			
Return to normalcy				
1. Test the readiness of the primary data center.	Recovery Team			
2. Get the main network system ready.	Network Team			
3. Relocate the system back to the primary data center.	Server Team Application Team			
4. Test the system according to key functions.	Application Team			
5. Notify users to test the system's function.	Call Center Team			

3. Political Demonstrations

Table C: Test Results: Political Demonstrations

Action	Team Responsible	Not Completed	Completed	Remarks
Before Incident				
1. Up-to-date Call Tree	Call Center Team			
2. Call Tree for external staff supporting the system's recovery.	Call Center Team Recovery Team			
Execution of Plan				
1. Notify the Recovery Team in the incident report and attend the meeting to prepare for the situation.	Call Center Team			
2. Make preparations to open the backup data center.	Recovery Team			
3. Make preparations for the backup network system.	Network Team			
4. Relocate essential resources to the backup data center.	Recovery Team			

Table C: Test Results: Political Demonstrations (cont.)

Action	Team Responsible	Not Completed	Completed	Remarks
5. Relocate critical work systems to the backup data center within the determined time for return to operations (RTO).	Server Team Application Team			
6. Open VPN service.	Network Team			
7. Test the system according to key functions.	Application Team			
8. Notify users to test the system.	Call Center Team			
9. Announce to all departments that the system is usable.	BCM Committee			
Return to normalcy				
1. Test the readiness of the primary data center.	Recovery Team			
2. Get the main network system ready.	Network Team			
3. Relocate the system back to the primary data center.	Server Team Application Team			

Table C: Test Results: Political Demonstrations (cont.)

Action	Team Responsible	Not Completed	Completed	Remarks
4. Return resources back to headquarters.	Recovery Team			
5. Test the system according to key functions.	Application Team			
6. Notify users to test the system's function.	Call Center Team			
7. Announce the return to normalcy to departments.	BCM Committee			

4. Disruptions to Critical Work

Table D: Test Results: Disruptions to Critical Work

Action	Team Responsible	Not Completed	Completed	Remarks
Before Incident				
1. Up-to-date Call Tree	Call Center Team			
2. Call Tree for external staff supporting the system's recovery.	Call Center Team Recovery Team			

Table D: Test Results: Disruptions to Critical Work (cont.)

Action	Team Responsible	Not Completed	Completed	Remarks
Execution of Plan				
1. Notify the Recovery Team in the incident report and attend the meeting to prepare for the situation.	Call Center Team			
2. Make preparations to open the backup data center.	Recovery Team			
3. Make preparations for the backup network system.	Network Team			
4. Relocate critical work systems to the backup data center within the determined time for return to operations (RTO).	Server Team Application Team			
5. Resolve the disruption to the work system to recover normal service.	Recovery Team			
6. Test the system according to key functions.	Application Team			
7. Notify users to test the system.	Call Center Team			

Table D: Test Results: Disruptions to Critical Work (cont.)

Action	Team Responsible	Not Completed	Completed	Remarks
8. Announce to all departments that the system is usable.	BCM Committee			
Return to normalcy				
1. Test the readiness of the primary data center.	Recovery Team			
2. Get the main network system ready.	Network Team			
3. Relocate the system back to the primary data center.	Server Team Application Team			
4. Test the system according to key functions.	Application Team			
5. Notify users to test the system's function.	Call Center Team			
6. Announce the return to normalcy to departments.	BCM Committee			

Table E: Analyzed Satisfaction Result obtained from High-Ranking Executives

Evaluation criteria	Highest 5	High 4	Moderate 3	Satisfactory 2	Low 1
1. The organization's image and credibility.					
2. Knowledge and understanding in operating under the business continuity plan.					
3. Clear setting of duties and responsibilities.					
4. Time taken for the system relocation to the data center as scheduled.					
5. Usability of the system after the system relocation.					
6. Ability to prevent and reduce damage to the Crown Property Bureau's functions.					
7. Ability to prevent and reduce risks to the IT system.					
8. The suitability of the determined time for the system recovery.					
9. Suitability of the plans and procedures.					

Table E: Analyzed Satisfaction Result obtained from High-Ranking Executives (cont.)

Evaluation criteria	Highest 5	High 4	Moderate 3	Satisfactory 2	Low 1
10. Consistency with the policies of the IT Department.					

BIOGRAPHY

NAME	Ms. Orawan Pankaseam
DATE OF BIRTH	2 May 1988
PLACE OF BIRTH	Bangkok, Thailand
INSTITUTIONS ATTENDED	Mahidol University, 2006-2009 Bachelor of Management (Management Information System) Mahidol University, 2010-2014 Master of Science (Technology of Information System Management)
HOME ADDRESS	1202 Soi 81, Phetkasem Rd., NongKhaem, NongKhaem, Bangkok 10160 Tel: 0895654141 E-mail: annneenaa@hotmail.com