

Unofficial Translation  
by the courtesy of The Foreign Banks' Association  
**This translation is for the convenience of those unfamiliar with the Thai language.  
Please refer to the Thai text for the official version.**

---

**BANK OF THAILAND**

January 23, 2007

To Managers

All Commercial Banks

No.: ThorPorTor. ForNorSor. (21) Wor. 118/2550 Re: Submitting Policy Statement on Business Continuity Management (BCM) and Business Continuity Plan (BCP) of Financial Institutions.

To enhance the efficiency of operational risk management of financial institutions, Bank of Thailand (BOT) hereby issued this Policy Statement on Business Continuity Management (BCM) and Business Continuity Plan (BCP) of Financial Institutions for their boards of directors and senior management to use as guidance in developing Business Continuity Management which shall include establishing policies, standards and operating procedures of the entire organization to ensure that in the event of disruption to the operations, critical business functions could continue or resume within reasonable period.

However, such Policy Statement merely provides general framework for Business Continuity Management and Business Continuity Plan for financial institutions. It is prudent that each financial institution adapts the framework and further develops details to commensurate with the nature and complexity of its operations. To ensure readiness, financial institutions are requested to prepare BCP to safeguard their institutions against any other unusual events deemed appropriate.

Please be informed and comply accordingly.

Yours sincerely,

(Mrs. Tarisa Watanagase)

Governor

Enclosure: Policy Statement of Business Continuity Management and Business Continuity Plan of Financial Institutions.

Prudential Policy Department

*BOT Notification No. 118-2550 (23-01-07)*

Tel. 0-2283-6827, 0-22836836

Fax 0-22835938

Remarks: ( ) Bank will arrange clarification meeting on.....at.....

( X) No clarification meeting is to be arranged.

## **Policy Statement**

**Re: Business Continuity Management (BCM) and Business Continuity Plan (BCP) of Financial Institutions.**

January 2007

Prepared by

Operational and Liquidity Risk Division

Prudential Policy Department

Financial Institutions Policy Group

Bank of Thailand

Tel. (02) 283-6827, 283-6836, 356-7339

Fax (02)283-5938

E-mail: [PreyanuC@bot.or.th](mailto:PreyanuC@bot.or.th); [BanchaM@bot.or.th](mailto:BanchaM@bot.or.th)

[PhanaraL@bot.or.th](mailto:PhanaraL@bot.or.th); [SiriratP@bot.or.th](mailto:SiriratP@bot.or.th)

## **Executive Summary**

This Policy Statement contains the guidance and key issues to the preparation of BCM and BCP of financial institutions. Each financial institution must determine how to adapt it and establish details commensurate with its business nature and complexity.

### **Critical Practices which Financial Institutions should observed:**

- The board of directors and senior management of financial institutions shall be responsible to formulating strategies and policies regarding BCM and to provide support of sufficient resources as well as conduct risk assessment to ensure good control of such Business Continuity Plans. The Business Continuity Plan shall become a part of overall organizational Risk Management Program.
- Financial institutions should identify their Critical Business Functions; assess relevant risks and impacts which may arise from any disruption to Critical Business Functions. They shall also specify recovery time objectives in the event of such disruption and set recovery strategies for operational recovery pertaining to each Critical Business Function.
- Financial institutions should provide documented Business Continuity Plans to cover all Critical Business Functions and those key Outsourcers.
- Financial institutions should test and review Business Continuity Plans for all Critical Business Functions at least once a year or when there was significant change to risk factors which could cause disruptions to Critical Business Functions.
- In the event of a disruption to any Critical Business Function, the financial institution concerned should notify the Bank of Thailand at the first opportunity but not exceeding 24 hours. In addition, detailed report of the event, procedures and period expected to resolve the problems as well as when the operations may return to normal shall also be reported to the Bank of Thailand.
- Financial institutions should complete the Policy covering Business Continuity Management and Business Continuity Plan within 12 months from the date this Notification. Any financial institution failed to meet this deadline is required to report to Bank of Thailand the reasons of such delay and provide regular progress reports until completion.

## Contents

<b>Topic</b>	<b>Page</b>
Introduction	1
Objectives	1
Scope of Policy Statement	2
Definitions	3
Contents	4
Roles and Responsibilities of the Board and Senior Management of Financial institutions	4
Analysis and Assessment of Impacts from Disruption to Critical Business Functions	4
Setting Recovery Objectives	5
Preparation of Business Continuity Plans	6
Communication and Training	7
Testing and Reviewing of Business Continuity Plans	7
Reporting to Bank of Thailand	9
Appendix: Examples of Disruptive Events	10

Unofficial Translation

by the courtesy of The Foreign Banks' Association

**This translation is for the convenience of those unfamiliar with the Thai language.**

**Please refer to the Thai text for the official version.**

---

## **Policy Statement**

### **Re: Business Continuity Management (BCM) and Business Continuity Plan (BCP) of Financial institutions**

---

#### **Introduction**

At present, all financial institutions are facing several critical risks. Operational risk is one of the crucial risks for any financial institution. Though well-planned control system has been implemented in most institutions, there are still many unpreventable risks such as accidents, natural disasters, fire, flood, acts of terrorists and epidemic. One vital tool to reduce severity of such mishaps is Business Continuity Management (BCM) and Business Continuity Plan (BCP)

In the past, Bank of Thailand (BOT) has issued Policy Statement to provide Contingency Plan for Information Technology (IT Contingency Plan) on October 12, 2005 which enables financial institutions to achieve certain levels of preparedness. In addition, Basel Committee on Banking Supervision (BCBS) also recognizes the necessity and importance of Business Continuity Management and recently issued "The Joint Forum: High-level Principles for Business Continuity in August 2006.

#### **Objectives**

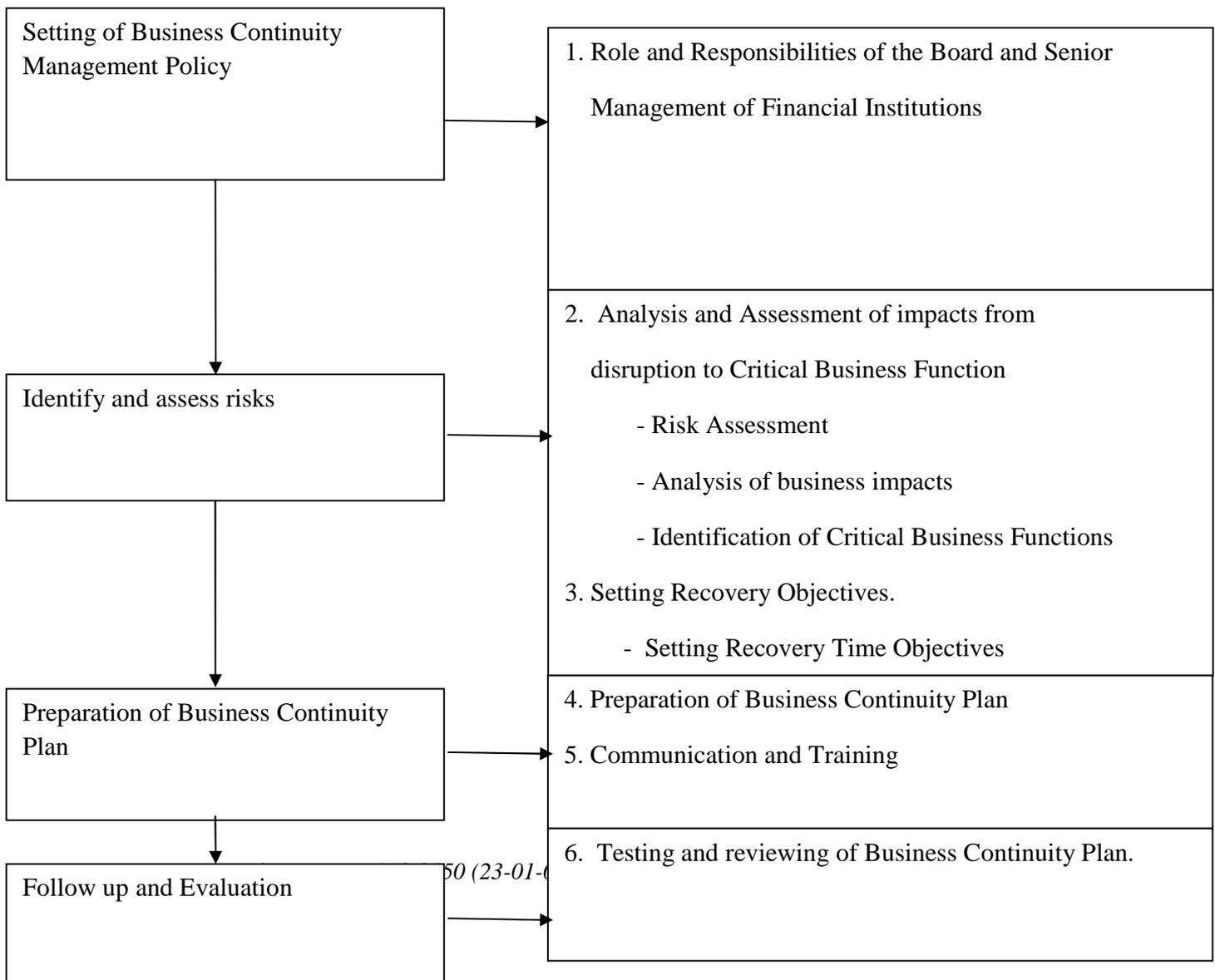
BOT prepared this Policy Statement to provide the board and senior management of financial institutions with a tool to set up their Business Continuity Management which include the issuance of policies, standards and operating procedures for their organizations to ensure that in if any disruption to Critical Business Functions should occur, the organization could continue to operate or could recover their operations within appropriate period of time which help mitigating business impacts to financial system, legal standing or good corporate image.

Financial institutions shall prepare their Contingency Plan for Information Technology which is a part of Business Continuity Management and Business Continuity Plan in accordance with Policy Statement regarding Contingency Plan for Information Technology (IT Contingency Plan) dated October 12, 2005 and/or subsequent revisions.

**Scope of Application**

This Policy Statement addresses directions and major requirements regarding Business Continuity Management and Business Continuity Plan from which financial institutions should apply and develop detailed procedures commensurate with the nature and complexity of their businesses as follows:

**Business Continuity Management: BCM**



## **Definitions**

“Board” means board of directors of the financial institution or, in case of foreign bank branch, authorized management committee.

“Key Outsourcers” means a natural or juristic person, either local or international, who provides services pertaining to Critical Business Functions for the financial institution.

“Business Continuity Management (BCM)” means guidance for establishing policies, standards, operating procedures for the entire organization to ensure that when disruption occurs, operations can be recovered within reasonable period.

“Business Continuity Plan (BCP)” means written plans to spell out working steps and operating procedures to recover operations when disruption occurred.

“Critical Business Functions” means those functions which once disrupted could significantly impact operations, business, reputation, status and performance of financial institutions.

“Business Impact Analysis: (BIA)” means process of analysis and evaluation, in both quantitative and qualitative terms, of impact or damages caused by operational disruptions.

“Recovery Objectives” means the setting up of objectives to recover operations which comprises of Recovery Time Objectives and Recovery Strategy.

“Recovery Strategy” means a direction guiding appropriate responses and actions in the event of major operational disruptions.

“Recovery Time Objectives (RTO)” means time period which could be tolerated during the operational disruptions.

“Alternate Sites” means a back-up site to run operations when there was operational disruption to the main site causing it to be unable to function normally.

## **Content**

### **1. Board and Senior Management Responsibilities**

The Board and senior management shall be responsible for formulating strategies and policies regarding Business Continuity Management of their financial institution, and shall allocate sufficient resources to support the program. However, the Board may delegate operational duties to a working committee or senior management. Such delegation shall be documented. The senior management shall be responsible for establishing the organizational structure, reporting relationship and defining clear job responsibilities of concerned people pertaining to approved Business Continuity Management policies. Moreover, the Board and senior management should evaluate Business Continuity Risks and Controls and embrace BCM into overall organizational risk management program. For large financial institutions with complex operations, it would be prudent to set up a specific BCM unit.

### **2. Analysis and Assessment of Impacts from Major Operational Disruptions**

Financial institutions shall analyze and assess the impact from Major Operational Disruptions in order to prioritize the operations as well as allocation of resources for effective operational recovery, should there be any disruption. The following items should be included:

#### **2.1 Risk Assessment**

1) Assessment of risk of possible disruptions to Critical Business Functions should be conducted at least once a year. Possible disruptive events which could impact financial institution on a short, medium and long term basis should be identified along with probability of each event or upon significant changes either from internal and external factors which could potentially impact the financial institution. (Examples of possible disruptive events are in the Appendix.)

2) Existing risk controlling processes should be analyzed and improved by providing necessary resources to ensure prompt and effective control of disruptions should they occur. There should also be evaluation and control on such process on a regular basis.

## **2.2 Business Impact Analysis**

Financial institutions shall conduct BIA of any possible event that may occur in every Critical Business Function to understand relationship of the function and impacts from possible disruptions to such function. The analysis will help financial institutions to prioritize operations and allocate appropriate resources to effectively recover any disruption. The BIA should take into account impacts on all stakeholders in both quantitative and qualitative terms such as possible loss of revenue, incurred expenditure, impact to reputation, and creditability of such financial institution, etc. This will enable prioritization as well as proper allocation of both internal and external resources for each Critical Business Function.

## **2.3 Analysis and Identification of Critical Business Functions**

Financial institutions should analyze and identify Critical Business Functions which could have material impact on their business, reputation and performance, should such functions be disrupted. Clear written criteria should be established on how to identify Critical Business Functions.

## **3. Setting Recovery Objectives**

### **3.1 Setting Recovery Time Objectives**

Financial institutions should develop RTO of each Critical Business Function, prioritize the Critical Business Functions and specify corresponding RTO. Such RTO requires approval by the Board and senior management of the financial institution.

### **3.2 Recovery Strategy**

Financial institutions should use the BIA results to set appropriate Recovery Strategy aiming at achieving established objectives by allocating sufficient resources and budgets for each working unit concerned to successfully deploy such Strategy. The financial institutions may also consider obtaining insurance coverage to lessen the impact/damage if such disruption should occur. Nevertheless, insurance coverage should not be considered a substitute for BCM as insurance was not intended for business recovery.

#### **4. Business Continuity Planning**

A Business Continuity Plan (BCP) is a documented tool to provide step by step procedures to support or recover operations and help keeping business running without disruption. BCP may include the repair or rebuild of work system, facilities or damaged utilities so that they could function and support continued business. All working units concerned must participate by providing their own BCP for their functions to be an integral part of overall BCP. A copy of this plan shall be kept by the person in charge of BCP and another copy kept as back-up off the premises.

BCP must cover all Critical Business Functions including Key Outsourcers concerned. It shall be updated regularly to be readily useable to achieve its objective when needed. It should at minimum cover the following items:

- 1) Detailed procedures to recover operations within specified timeframe when there was disruption impacting Critical Business Functions.
- 2) Required resources for operations such as headcounts, computers, telephones, facsimile machines, office equipment, contracts, insurance policy, etc.
- 3) Communication plans for all relevant parties both within the financial institution and those external parties. (Please refer to Section 5.1.)
- 4) Plan of setting up Alternate Sites where considered necessary. The Alternate Site, however, should be located at a distance which would not be impacted by same mishap and should not utilize the same sources of utilities to prevent large scale impact. This Alternate Site shall be readily operational and able to be operated for an extended period of time if necessary. For branches of foreign banks which volume of business do not justify an Alternate site, a branch in another country may be used provided that proper back-up procedures was established.
- 5) In the case where a financial institution relies on an Key Outsourcers, the financial institution must ensure that BCP of the Outsource is consistent with its BCP.

## **5. Communications and Trainings**

### **5.1 Communications**

Financial institutions should have communication plans for all relevant parties, both internal and external, and evaluate impacts on related overseas parties when disruption occurred such that prompt notification may be announced in order to prevent any panic situation among general public. The communication plan should indicate responsible persons, scope of authority, communication procedures and channels, level of disclosure, names and telephone numbers of employees and relevant external parties. A Call Tree format is recommended to provide clear communication guide among internal and external parties and/or those in other countries when such disruption could widely impact international financial system.

### **5.2 Trainings and Public Relations**

Financial institutions should provide regular BCP trainings for employees and those concerned, which shall include every Critical Business Function and overall organization to ensure that employees and those concerned are well aware of their personal role and responsibility should such operational disruption occur.

Financial institutions should disseminate information on BCP by clearly outlining communication procedures and methods for the awareness of their employees and relevant parties. Furthermore, financial institutions should establish customer relations procedures and methods in the event of a disruption, in order to reinforce confidence among stakeholders that the financial institution is able to continue to provide normal services.

## **6. Testing and Reviewing**

6.1 Financial institutions should set clear testing and reviewing schedules for BCP corresponding with their current status, policies and strategies. In addition, testing of BCP for all Critical Business Functions should be conducted at least once a year or material change in risk factors which could trigger operational disruption to ensure that BCP is effective and practical at all time. Nevertheless, financial institutions may choose their own testing procedures suitable to the business nature and select frequency by taking into account such factors as criticalness of business functions, their role as financial center, major changes and/or internal and external factors, etc. Financial institutions should require all relevant parties on every level to participate in the testing of BCP.

6.2 Testing and reviewing of BCP shall at least cover the following items:

- (1) Purpose and scope of testing
- (2) Simulating events for testing
- (3) Time period for entire testing
- (4) Employee evacuation procedures
- (5) Communication plan
- (6) Critical data back-up and retrieval
- (7) Readiness of building/facilities and resources needed for testing
- (8) Readiness of Alternate Site to be operated within specified timeframe
- (9) Recovery of Critical Business Functions

6.3 Financial institutions should collect and compare actual testing results against targets and perform Gap Analysis so that BCP could be evaluated and improved. All testing results and Gap Analysis shall be reported to the Board.

6.4 Financial institutions should arrange to have evaluation and reviewing of BCP by outside experts or by independent and knowledgeable internal team. The results of such evaluation and reviewing shall be reported to the Board. Moreover, the BCP shall be updated at least once a year or when there is significant change that impacts the BCP such as large scale civil unrest, epidemic, change of personnel in charge of BCP, etc. Information and disseminated documents to employees and general public should also be updated accordingly.

6.5 In case financial institutions rely on Key Outsourcers or major utilities providers such as electricity, water or telecommunication companies, financial institutions should conduct BCP testing with such organizations. If testing could not be arranged with such principal Outsourcers or providers, financial institutions must ensure that the principal Outsourcers and providers are able to provide continued services in case of operational disruption. Otherwise, financial institutions should have back-up plans to support above-mentioned services/products from alternate sources.

### **Reporting to the Bank of Thailand**

When there was disruption to Critical Business Functions which materially impacted their depositors or clients, financial institutions shall notify the Bank of Thailand at the first opportunity within 24 hours from the instant of such disruption by informing the respective Central Point of Contact (CPC) of the financial institutions and relevant departments as well as submitting detailed report of the disruptive event such as location/site involved, time and date, details of event, corrective actions and timeframe needed to resolve such disruption. Once the Critical Business Function was recovered, the financial institution shall also notify the Bank of Thailand.

Written BCM and BCP shall be completed by all financial institutions within 12 months from the date of this Notification. Should any financial institution fail to meet this deadline, it shall report to the Bank of Thailand the reason of such delay and provide progress reports until completion.

Furthermore, financial institutions should additionally study IT contingency plan related and BCM related guidance issued by such organizations such as Basel Committee on Banking Supervision (BCBS), Federal Financial Institutions Examination Council (FFIEC) and Business Continuity Institute (BCI).

---

## Appendix

### Examples of Disruptive Events

<b>Economy/physical</b>	<b>Human Resource</b>	<b>Reputation</b>	<b>Natural Disaster</b>	<b>Human-made Disaster</b>
*Labor unrest  *Inability to access operational site and utilities  *Damage to IT system and facilities preventing employees to operate normally	*Lost of key executives and personnel  * Key executives and personnel were not available  * Massive absence of employees	* Facing severe litigations  * Negative rumor and adverse publicity for the organization	* Flood * Fire * Storm * Tsunami * Volcanic eruption * Severe epidemic such avian flu	*Acts of terrorism such as bombing or arson  *Hostage taking