Policy Statement
Re: Business Continuity Management (BCM) and Business Continuity Plan (BCP) of Financial Institutions

3 August 2008

Prepared by
Financial Institutions Business and Accounting Policy Office
Regulatory Policy Department
Financial Institutions Policy Group
Bank of Thailand
Tel. 0-2283-6876, 0-2356-6803
Fax 0-2283-5983
E-mail: BOPTeam@bot.or.th

Unofficial Translation
With collaboration between the Bank of Thailand and the Association of International Banks
This translation is for convenience of those unfamiliar with the Thai language.
Please refer to the Thai text for the official version.

Policy Statement of Bank of Thailand
Re: Business Continuity Management (BCM)
and Business Continuity Plan (BCP) of Financial Institutions

---

1. Rationale

Currently, financial institutions have encountered risks in various aspects. Operational risk is considered one of the significant risks for financial institutions. Even though financial institutions may have an efficient control system, there still are some risks that are unavoidable such as accident, natural disaster, fire, flood, sabotage and epidemic, etc. The essential tools to relief the severity of such incidences are Business Continuity Management (BCM) and Business Continuity Plan (BCP).

The Bank of Thailand has imposed this Policy Statement for financial institutions' board of directors and senior management to use as a guideline in setting out BCM as well as setting out of operational policy, standard and procedures for an entire organization so that whenever there is an incidence that brings the operation to a halt, the critical business functions (CBF) may continue or resume within an appropriate timeframe. A good BCM will reduce effects to financial institutions' financial status, legal status, reputation and others.

As for preparing emergency plan for information technology (IT), which should be considered as part of the BCM and BCP, financial institutions shall comply with the Notification of the Bank of Thailand Re: Permission for Commercial Banks to Operate Electronic Banking Services or as later amended.

The essence of this Notification has not been changed from the original one.

2. Scope of Application

This Policy Statement shall apply to all commercial banks established in accordance with Financial Institutions Businesses Law.

3. Repealed Circulars

The Circular of the Bank of Thailand No. ThorPorTor. ForNorSor. (21) Wor.118/2007 dated 23 January 2007 Re: Submission of Business Continuity Management (BCM) and Business Continuity Plan (BCP) of Financial Institutions shall be repealed.

4. Contents

4.1 In this Policy Statement

"Board" means the board of directors of the financial institutions or authorized senior management in case of foreign bank branch.

"Key Outsourcer" means natural or juristic person, either domestic or international, who provides service pertaining critical business functions for the financial institutions

"Business Continuity Management (BCM)" means guideline for establishing policy, standards and procedures for the entire organization to ensure that in case where there is an incidence that brings the operation to a halt, the critical business functions may continue and resume within an appropriate timeframe.

"Business Continuity Plan (BCP)" means written plan with specific steps and procedures for resuming operation back to normal so that business may continue when the operation is put to a halt.

"Critical Business Function" means a function once disrupted may cause significantly impact to the operation, business, reputation, status and performance of financial institutions

"Business Impact Analysis (BIA)" means a process of analysis and assessment of impact or business loss, both qualitative and quantitative, caused by operational disruptions.

"Recovery Objective" means a setting up of a goal for operational recovery which consists of recovery time objectives and recovery strategies.

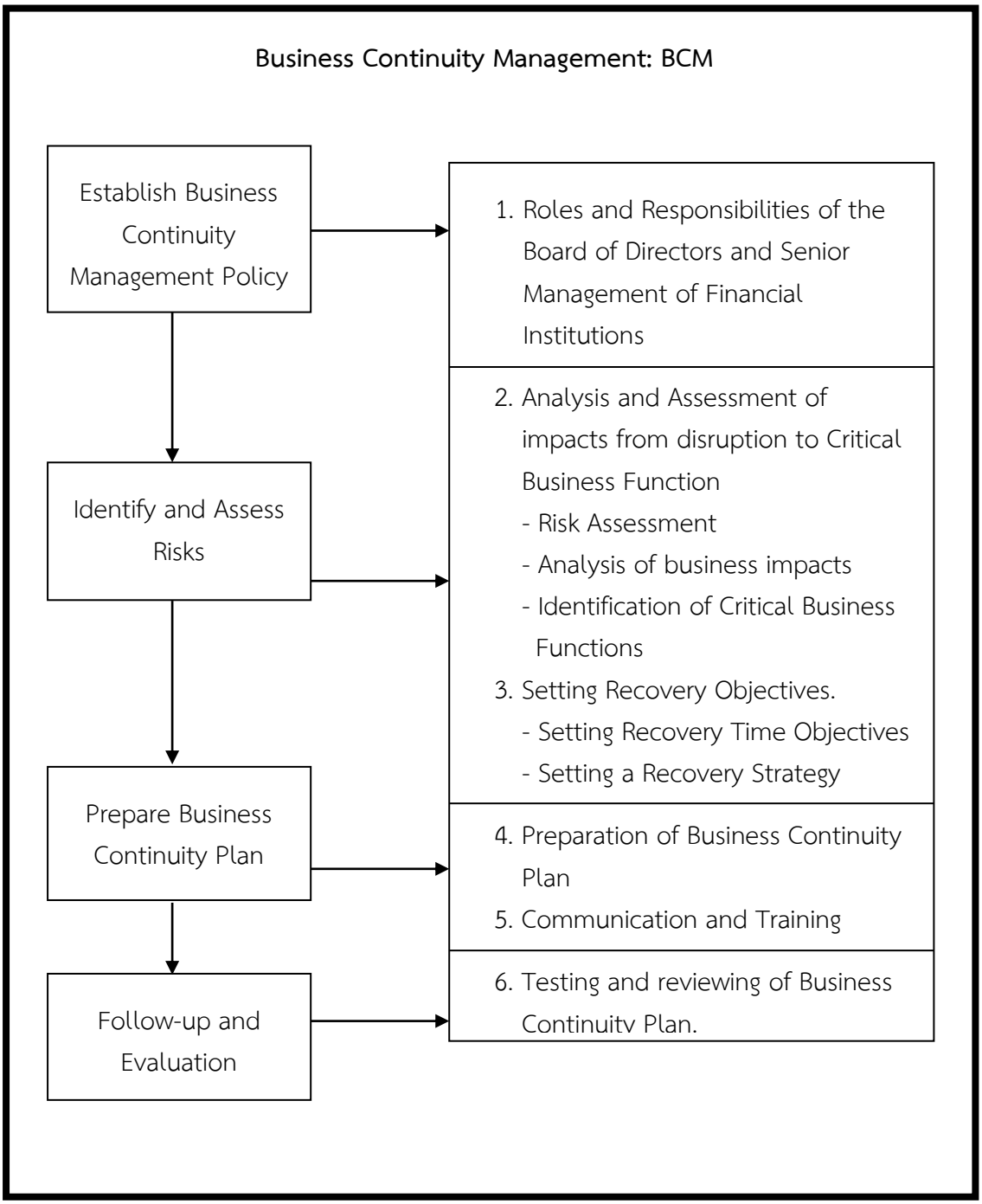
"Recovery Strategy" means a guideline to cope with the major operational disruptions.

"Recovery Time Objective (RTO)" means an acceptable period for operational disruption.

"Alternate Site" means a substitute place for operation and running business in case the main operational site is not available for operation as normal.

4.2 Scope of this Policy Statement

This Policy Statement addresses guidelines and major aspects for BCM and BCP of financial institutions. Each financial institution shall consider adopting such guidelines and set out appropriate details according to type and complexity of its business as follows:



4.3 Details of the Policy Statement

4.3.1 Roles and responsibilities of the Board and Senior Management

The Board and senior management shall be responsible for imposing strategies and policy concerning BCM and allocate adequate resources to support the operation. The Board may delegate operational authority to a working group or senior management; however, such delegation shall be done in writing. Senior management shall be responsible for setting out a clear structure, line of command and responsibilities of related parties in accordance with the approved BCM policy. In addition, the Board and senior management shall take into consideration the business continuity risks and control of compliance with BCP which should be considered as a part of the enterprise risk management. For large financial institutions with complex operation, the financial institutions may set up a specific department to oversee the BCM for the financial institutions.

4.3.2 Analysis and impact assessment on major operation disruptions

Financial institutions shall analyze and assess impacts from major operation disruptions in order to prioritize the operations and resources allocated for effective operational recovery. The analysis and assessment shall cover the following aspects:

(1) Risk Assessment

(1.1) Financial institutions shall conduct assessment on risk that may cause disruptions to critical business function at least once a year. The assessment shall include incidences that may cause disruption to the financial institutions' operation in a short, medium and long term as well as assessment on opportunity that such incidences may incur or upon significant changes either from internal or external factors which may potentially impact financial institutions (Example of possible disruption incidences are prescribed on attachment 1).

(1.2) Financial institutions shall analyze existing risk control processes and enhance processes and resources necessary for controlling risk that may cause disruption as well as conduct assessment and control on such processes.

(2) Business Impact Analysis (BIA)

Financial institutions shall analyze business impact on any possible incidence associated to the critical business functions (CBFs) in order to understand the relationship between the CBFs and impacts from disruption of such function. The analysis will allow financial institutions to prioritize the operations and resources allocated for effective operational recovery. In conducting BIA, financial institutions should take into account the impacts to all financial institutions' stakeholders, both quantitative and qualitative, such as potential loss of revenue, incurred expense, reputation and creditability of financial institutions, etc. Financial institutions should also prioritize resources, internal and external, necessary for each critical business function.

(3) Analysis and Identifying Critical Business Functions

Financial institutions shall analyze and identify CBFs, which once disrupted may cause significantly impact to the operation, reputation, and performance of financial institutions. Financial institutions shall set out a clear guideline on identifying CBFs.

4.3.3 Setting Recovery Objectives

(1) Setting up recovery time objectives (RTO)

Financial institutions shall develop recovery time objectives of each CBF. Moreover, financial institutions shall prioritize CBFs and set up recovery timeframe. Such recovery time objectives require approval by the Board and senior management of financial institutions.

(2) Setting up recovery strategy

Financial institutions shall take the outcomes of the BIA into consideration in setting appropriate recovery strategy in order to achieve specified goal by allocating sufficient resources and budgets for each relevant work unit to carry out such strategy. Financial institutions may also consider obtaining an insurance to reduce the loss from business disruptions. However, such insurance does not counted as a substitute for BCM since the main objective of insurance is not for business recovery.

4.3.4 Preparing business continuity planning

BCP is a written plan which determines procedures to support or resume business to normal operation so that business may continue. BCP may include repair, rebuild of damaged work system, facilities or utilities so that they may resume their normal operation. All relevant work units should continuously participate in preparing BCPs and all BCPs related documents should be kept with the responsible person, at least one copy, and should be kept outside of the workplace, at least one copy as well.

BCP shall cover all CBFs of the organization, including relevant key outsourcers and shall be kept up to date so that it will achieve the goal as needed. BCP should cover, at least, the following matters:

(1) Detailed operation procedure during CBF's disruption so that the CBF will be recovered within a specified timeframe;

(2) Necessary resources for operation such as staff, computer equipment, telephone, facsimile, office equipment, contracts, insurance policy, etc.;

(3) Communication plan for all financial institutions' relevant parties, both internal and external;

(4) Plan for setting up an alternate site when necessary. The alternate site should be located in a distance from the primary site which will not be impacted by the same incidences and should not utilize the same sources of utilities to prevent large scale impact. The alternate site shall be ready at all time for operation and should be able to support long-term consequence. However, in case of foreign bank branch, the bank may use other branches in other countries to oversee the alternative site issue or in case where the business transactions is not as much, financial institutions might not have to set up an alternative site, nevertheless, a proper substitute procedures is required.

(5) In case where financial institutions obtain services from key outsourcers, financial institutions shall ensure that BCP of the key outsourcer is complied with BCP of financial institutions.

4.3.5 Communications and Trainings

(1) Communication

Financial institutions shall established ways of communication, internal and external, to relevant parties as well as taking into consideration impacts to relevant parties oversea in case the disruption is incurred so that financial institutions can inform public of such incidences on a timely basis and prevent any public panic. The communication plan shall specify responsible persons, scope of authorities, communication procedures and channels, disclosure level, names and phone numbers of staff and external relevant parties which may be prepare in a form of a Call Tree. The communication plan shall provide instruction on how to contact relevant parties, internal or external, domestic or overseas in case the disruption may impact international financial system.

(2) Trainings and Public Relations (PR)

Financial institutions shall provide regular BCP trainings for staff and relevant parties. The BCP training program should include trainings on every CBF and on organizational level to ensure that staff and relevant parties understand their roles and responsibilities when such operational disruptions occur.

Financial institutions shall disseminate BCP by clearly specify PR procedures and methods so that FI's staff and relevant parties are informed. In addition, financial institutions shall specify PR procedures and method to customers when operational disruptions occur in order to ensure that financial institutions are capable to continue their operation.

4.3.6 Testing and Reviewing

(1) Financial institutions shall establish clear test plan for BCP which is in accordance with the financial institutions' current situation, policy and strategy. In addition, financial institutions shall conduct BCP testing for CBFs at least

once a year or whenever there is a material changes on factors which may trigger operational disruptions in order to ensure that BCP is effective and practical. Nevertheless, financial institutions may choose the test that is suitable for the functions and the frequency of the test may be set according to the various factors such as importance of the business function, financial institutions' role as financial center, major changes on situation and/or internal or external factors that may impact financial institutions, etc. Financial institutions shall allow all level of relevant parties to involve in testing of BCP.

(2) Testing and reviewing of BCP shall, at least, cover the following items:

(2.1) Objective and scope of testing

(2.2) Simulation for testing

(2.3) Test Period

(2.4) Employee evacuation procedure

(2.5) Communication plan

(2.6) Critical data back-up and retrieval

(2.7) Readiness of building/facility and resource necessary for business operation

(2.8) Readiness of alternate sites to be operated within specific timeframe

(2.9) Recovery of CBF

(3) Financial institutions shall collect the test results for conduction gap analysis so that financial institutions may continuously evaluate the testing and improve the efficiency of BCP and report the result to the Board.

(4) Financial institutions shall conduct an assessment and review of BCP by external experts or by independent and knowledgeable team internally. Financial institutions shall report the assessment and review results to the Board. In addition, financial institutions shall update BCP at least once a year or whenever there is a change that may impact the BCP such as violence, epidemic, turnover of employees who responsible for carrying out the BCP, etc. Information and documents distributed to employees and external parties should be updated accordingly.

(5) If financial institutions rely on key outsourcers or major utility providers such as electricity, water or telecommunication companies, etc., financial institutions shall conduct a BCP test with key outsourcers or such utility companies. If the key outsourcers or such companies are not able to participate on the test, financial institutions must ensure that the key outsourcers and aforementioned companies are able to carry out their services during the operational disruption. Otherwise, financial institutions shall establish a back-up plan.

4.3.7 Reporting to the Bank of Thailand

When there is a disruption to CBF which may significantly impact the financial institutions' depositors or clients, financial institutions shall inform the Bank of Thailand as soon as possible and should be within 24 hours from the instant of such disruption. Financial institutions shall inform the Central Point of Contact of each financial institution and relevant departments, as well as, report details on the incidence such as departments where the incidence incurred, time of incidence, details on how the incidence occurred, problem solving procedure and expected timeframe to resolve the problem, etc. Once the CBF is resumed to normal, financial institutions shall also notify the Bank of Thailand of such recovery.

In addition, financial institutions shall study a guideline for setting up an information technology contingency plan and BCM related guideline issued by other relevant organizations such as Basel Committee on Banking Supervision (BCBS), Federal Financial Institutions Examination Council (FFIEC) and Business Continuity Institute (BCI), etc.

5. Effective Date

This Policy Statement shall come into force with effect from 4 August 2008 onwards.

Attachment 1

Examples of Disruptive Events

Economics/Physical	Human Resource	Reputation	Natural Disaster	Human-made Disaster
■ Labor unrest ■ Inability to access operational site and utilities. ■ Damage to IT system and facilities preventing employees to operate normally.	■ Loss of key management and personnel. ■ Key management and personnel were not available. ■ Massive absence of employees.	■ Facing severe litigation ■ Negative rumor and adverse publicity for the organization.	■ Flood ■ Fire ■ Storm ■ Tsunami ■ Volcanic eruption ■ Severe epidemic such as avian flu.	■ Acts of terrorism such as bombing or arson, etc. ■ Hostage taking.