(UNOFFICIAL TRANSLATION)

Readers should be aware that only the original Thai text has legal force, and that this English translation is strictly for reference.

Notification of Practice Guidelines

No. NorPor. 4/2559

Re: Practical Guidelines for Business Continuity Management

Reference is made to *the notification of the Capital Market Supervisory Board No. TorThor. 35/2556 Re: Standard Conduct of Business, Management Arrangement, Operating Systems, and Providing Services to Clients of Securities Companies and Derivatives Intermediaries dated 6 September 2013* ("***Notification No. TorThor. 35/2556***") and *the notification of the Office of Securities and Exchange Commission No. SorThor/Nor. 45/2559 Re: Rules in Detail on Regulations Concerning the Establishment of Risk Management System for Business Continuity of Intermediaries dated 21 October 2016* ("***Notification No. SorThor/Nor. 45/2559***") which specify on the rules for operation systems capable to support business continuity with suitability, reliability and effectiveness in order that the intermediaries are able to service with the best interest of customers and that the intermediary's personnel are able to work accurately as per their duties and create no risk which may render the intermediaries to infringe or not comply with laws, rules and standards relating to such business operations.

For benefits in compliance with the aforementioned provisions of the intermediaries, the SEC by virtue of Clause 5(1) in conjunction with Clause 12(3) of the ***Notification No. TorThor. 35/2556***, therefore, issues the practice guidelines as follows:

Clause 1 In case where the intermediaries have provided all operation systems for supporting business continuity under this practice guideline, the SEC shall deem that the intermediaries have already complied with the ***Notification No. TorThor. 35/2556***, in part of operation systems for supporting business continuity, and the ***Notification No. SorThor/Nor. 45/2559***. In this regard, if the intermediaries proceed differently from this practice guidelines, the intermediaries shall have an obligation in proving that such proceeding is still under the principles and provisions of the ***Notification No. TorThor. 35/2556***, in part of operation systems for supporting business continuity, and the ***Notification No. SorThor/Nor. 45/2559***.

Clause 2 The practical guidelines under Clause 2 have details as provided in appendix at the end of this Notification of Practice Guidelines, whereby such details are as the following matters:

(1) Division 1 Objectives of practice guidelines for business continuity management

(2) Division 2 Board of directors and senior management responsibility

(3) Division 3 Impacts of emergency incidents which may cause major operational disruptions

(4) Division 4 Companies should determine a recovery objective to restore normal operations

(5) Division 5 Companies shall arrange business continuity planning for supporting business continuity

(6) Division 6 Communications with relevant persons

(7) Division 7 Cross-border communication

(8) Division 8 Companies shall test and assess the BCP (Training, Exercising and Auditing)

(9) Division 9 Examples of emergency incidents which may cause major operational disruptions

Notified this 21st day of October 2016.

(Mr. Rapee Sucharitakul)

Secretary-General

Office of Securities and Exchange Commission

(UNOFFICIAL TRANSLATION)

Readers should be aware that only the original Thai text has legal force, and that this English translation is strictly for reference.

Appendix

Division 1 Objectives of practice guidelines for business continuity management

The SEC provides this practice guidelines for being a guideline in practice through which covers a critical matter of business continuity management that should be applied by each intermediary and for determining a clear detail of practical approaches suitable for size and complexity of business operation of companies. In addition, the intermediaries should study standards and practice guidelines for business continuity management from other related agencies, such as Business Continuity Institute (BCI)[1] or International Organization of Securities Commissions (IOSCO)[2].

Division 2 Board of directors and senior management responsibility

Board of directors ("***Board***") and senior management of the intermediaries shall be a responsible person for determining the company's strategies and policies on the business continuity management (BCM) and the business continuity plan (BCP), including allocation of resources and budgets to relevant units properly, and shall arrange following up and compliance with the said policies and plans. In this regard, the ***Board*** and the senior management may appoint a working group as a responsible person for operational works, but they shall keep monitoring such operations.

Division 3 Impacts from emergency incidents which may cause major operational disruptions to the critical functions

Companies shall arrange an assessment on risks and possibility of major operational disruptions due to a possible emergency incident, as well as analyse a business impact and assess damages from major operational disruptions, so that companies are able to set a priority of works and allocate its resources for business continuity management effectively. At least, companies should conduct a risk assessment and business impacts analysis once a year or when there is a significant change affecting the risks and impacts as such. In doing so, it shall be complied with the following approaches:

3.1 Defining Critical Business Function Companies should select a critical business function which it considers that if emergency incidents happen, it will disrupt and significantly affect customers, business operation, financial status or reputation of

---

[1] BCI Good practice guidelines http://www.thebci.org/

[2] High-level principles for business continuity and Market Intermediary Business Continuity and Recovery Planning document http://www.iosco.org/

companies, such as submission of securities trading order, clearing and settlement and delivery of securities and assets, sale and redemption of investment units, and NAV calculation.

3.2 Risk Assessment Companies shall conduct an assessment on risks and possibility of major operational disruptions by assessing on an emergency incident, which causes a disruption and business impacts in either short, medium or long term, such as damage on building or place of business or branches, a failure of information technology system, inaccessibility or unusability of building or personnel unable to come for work in both temporaty or permanently cases.

3.3 Business Impact Anaysis Companies shall analyse a business impact and assess on damage from major operational disruptions so that companies are able to set priority of works and allocate its resources for business continuity management effectively by taking into account of impacts, either financial or non-financial, on customers, personnel, subsidiary companies, equipments, assets and place of business of companies, financial status, customer's trust and company's reputation, as well as a compliance to governmental regulations. Also, it should consider to wide impacts as well. For example, for investment or encumbrance creation of mutual funds or private funds, it shall consider a process in settlement or delivery which may affect to an overall market system. For a failure of computer systems used for trading securities by companies which are members of the Stock Exchange of Thailand. If the incident results in no ability in recording an offer for trading come from variuos companies into a trading system at the same time and last longer than a period specified by the Stock Exchange of Thailand, it may be a part through which enables the Stock Exchange of Thailand suspending all trading temporality.

Division 4 Companies should determine a recovery objective to restore normal operations

4.1 Companies should determine a recovery time to restore normal operation (Recovery time objectives) and set a recovery order of every critical business function suitable for possible impacts.

4.2 Companies should consider to determine a data class and latest data set to recover (Recovery point objective), such as data on assets of customers and funds, securities or unit trading transactions or information on NAV, so that companies are able to operate consecutively and render no significant impact to customers, business operation and a compliance with regulations in case of emergency incidents happened. However, the latest data recoverable may be a data recovery as of the end of day of the day before or of 1 hour before the occurrence of emergency incidents, as the case may be. In addition, there should be provided an approach on provision or preparation of substitute data in replacement of lost important data.

4.3 If companies have used a service from a service provider, companies should cooperate with a service provider in determining a recovery time to restore normal operation and latest data set to recover in order to derive a suitable and practical objective.

In this regard, the determination of recovery time objectives and recovery point objective is a significant factor for determining a required resource. Therefore, it should be approved by senior management and the ***Board*** or the appointed working group.

Division 5 Companies shall provide business continuity planning for supporting business continuity

To operate a critical business function continually, companies shall arrange BCP in a written and obtain an approval from senior management and the ***Board*** or the appointed working group. The BCP as such should be kept at place of business, either inside or outside.

The BCP shall cover all critical business functions of companies, including a critical operational functions which companies use via a service provider. Also, companies should specify in detail of practical approach into the BCP to be suitable for size and complexity of business operation of companies and to cover a disruption possibly occured in every incident and a case where an occurrence of emergency incidents lasts a long time or results in damage covering wide areas, such as epidamics or a failure of electricity or communication in many areas, by allowing every units to participate in arranging the BCP for their own critical business functions. The BCP shall contain, at least, the following details:

5.1 Operational procedures and resposible persons In order that companies are able to restore its critical operational function within a specified period after operational disruption, companies shall determine duties and responsibilities for each operational staffs clearly and arrange a communication and rehearsal of understanding on duties to perform, as well as specify in details of operational approach understandable and practicable on what, when and where to work.

5.2 Methods and channels to communicate among relevant persons either inside or outside companies Companies shall determine methods and channels for communication, a list of relevant persons either inside or outside companies, responsible persons and communication, including clear detailed information for disclosure to relevant persons. Companies should arrange a call tree[3] and a name list of customers, the main service providers and other relevant persons, including contact information, such as an office phone number, home phone number, mobile phone number or e-mail of which companies shall update a name list and contact information regularly. Additionally,

[3] List of contact persons, including employee list, telephone number and contact chart, whereby each employee shall contact an employee as scheduled.

companies should specify additional communication channels, such as SMS, call center or other distribution via various media.

5.3 Required resources for operation Companies should prepare or procure required resources for operation, such as procurement or determination of substitute personnel at operational level and management level, financing source, office equipments and information technology systems, as well as, should evaluate on a usage of finance and accesibility to finance during an occurrence of emergency incidents.

5.4 Establishment of alternative site In order to prevent impacts from emergency incidents occurring wide areas, companies may arrange an alternative site for supporting continuity of operation. Such alternative site should not use the same source of infrastructure as the main office, should have a location distant from the main office sufficient for not suffering from the same impacts and it should be able to support a large amount of critical business functions or a long-lasting emergengy incidents. In addition, the alternative site should be ready to use immediately when emergengy incidents happened or within a specified period (recovery time objectives). In case where companies do not arrange the alternative site, companies should provide other practice guidelines to support continuity of operation.

Division 6 Communications with relevant persons

6.1 To prevent and lessen anxiety of relevant persons and the public as well as to be able to notify the incidents to the regulatory agencies in time, the intermediaries shall design a plan for communication with relevent persons either inside or outside companies in accordance with possible impacts. If the impacts as such significantly affect customers or relevant persons, such as, a close or postponement of opening in any business locations, a failure to securities trading systems or securities operational systems, a failure in receiving subscription and redemption order, or NAV calculation; companies shall inform or publicize thoroughly and swiftly to customers or relavant persons to acknowledge the occurrence of emergency incidents, the impacts happened, the communication channels for customers of relevant persons to contact for using services or to communicate with companies throughout a period of emengency incidents happened for checking asset balance and doing transactions, and action measures of companies. Also, companies shall periodically communicate a progress of operation in case of long-lasting emergency incidents.

6.2 In case where there is a suspension in serving of critical business funcions or there is an occurrence of emergency incidents significantly affecting customers of companies, companies shall inform the SEC shortly, not exceeding the next business day, together with a detailed report of incidents happened, operational procedures and a period of time used or expected to use in solving problems, on which companies shall inform its responsible officers. Also, when critical business functions have been restored to normal, companies shall notify the SEC to acknowlege as well.

Division 7 Cross-border communication

In case where a intermediary has a transaction or a service usage from a foreign service provider, a intermediary should have an effective plan for communication with a foreign regulatory agency, foreign authorities and foreign service providers in order to support in case of the occurrence of emergency incidents causing cross-border impact. In contacting with foreign regulatory agencies, a intermediary is able to contact through its foreign counterparties or the SEC.

Division 8 Companies shall test and assess the BCP (Training, Exercising and Auditing)

8.1 Companies should arrange a training and communication on the BCP to relevant persons, either inside or outside, regularly, as well as shall test the BCP to be in line with an actual situation nowadays, whereby the responsible staff in every level shall participate in the test. The BCP of critical business functions shall be arranged at least once a year or when there is a significant change[4]. Companies shall determine a sufficient scope of testing to ensure that companies are able to operate according to the BCP correctly and efficiently as expected.

8.2 In testing and assessing the BCP, companies should determine a simulation incident which may be different in each testing, such as, flood, earth quake, bombing, march in protest, bird flu epidemics or cyber attack[5], in order to testing of the BCP for supporting continuity of operation in various incidents. In doing so, companies may consider on current situations, past testing results or possible impacts. The test and assessment shall, at least, cover the following issues:

8.2.1 Procedures for communicating with relevant persons, correctness and modern of name list and contact data.

8.2.2 Procedures for evacuating employees or moving personnel to a specified location.

8.2.3 Procedures for normal operation ranging from the beginning until the ending process of critical business functions, such as, submission of securities trading orders, settlement and delivery of securities and assets, recording asset account of customers and funds, sale and redemption of investment units, NAV calculation or investment management.

---

[4] A significant change, such as, acquirement of additional business license, merger and acquisition or change of used technology.

[5] To focus on protecting information and privacy of customers[1] in angle of the BCP on cyber security

8.2.4 Readiness of computer systems, network, equipments and backing up and recovery of important data, whereby it is able to recover the latest data as specified from equipments or storing locations.

8.2.5 Readiness of alternative site (if any), whereby the alternative site is able to support an operation immediately or within a specified period.

Addtionally, companies should test the BCP by cooperating with relevent agencies, such as, the Stock Exchange of Thailand, the financial institutions, the main service providers and the selling and redemption agents.

8.3 In order that relevant persons are able to comply with the BCP practically and completely when emergency incidents happened, companies shall provide a qualified and independent evaluator to evaluate the effectiveness of auditing plan and the BCP testing results that the tests as such have achieved goals set by companies in aspect of either a time used or recoverable data and that relevant persons have complied with the plan completely and correctly. Also, the report of evaluation shall be reported to the ***Board*** or the assigned working group periodically as deemed appropriate. The evaluator as such may be insiders or outsiders of companies.

8.4 In order to adjust the BCP to be appropriate and in accordace with a current situation, companies shall review the BCP, both at unit level and organisation level, according to reciept of the evaluation results and when there is any significant change, such as, acquirement of additional business license, merger and acquisition or change of used technology.

8.5 Companies shall keep documents in relation to the test to be complete and up-to-date, as follows:

(1) Plans which have been used in the test;

(2) Testing result summary;

(3) Plan revision summary.

8.6 Companies should follow up and assess the BCP of the main service providers, by which companies may participate in the test, mutually observe or let the main service providers notify the BCP test to companies.

Division 9 Examples of emergency incidents which may cause major operational disruptions

Examples of emergency incidents are classified into a group for clearness and being a guideline for intermediaries for analysing possible impacts of various crises in order to specify more extensive measures. The intermediaries shall assess risks and impacts of various crises and shall arrange a reasonable measure to support. The crises can be classified into 5 aspects, as follows:

9.1 Economic/physical aspect, such as, strike of employees or inaccessibility to building or facilities in areas.

9.2 Human resource aspect, such as, loss of executives or a key personnel or lack of personnel in large number.

9.3 Reputation aspect, such as, being prosecuted in serious lawsuit or having various rumours in the way that being derogatory to an organisation.

9.4 Natural disaster aspect, such as, flood, conflagration, storm or epidemics.

9.5 Human-caused disaster, such as, terrorist, being caught as hostage or cyber attack.