Unofficial Translation

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

Please refer to Thai text for the official version

Notification of the Bank of Thailand

No. FPG. 26/2551

Re: Permission for Commercial Banks to Operate E-Banking Services

---

1. Rationale

Currently, commercial banks, a financial service provider, have been utilizing information technology to further develop their capabilities to enhance the banking operations in order to respond efficiently and speedily to ever-changing customer demands. Therefore, the Bank of Thailand establishes a policy to support banking services by leveraging latest technologies within the scope applicable to the country's standing and economic status. Additionally, cost-effectiveness of technologies is also one of the considerations. Suitable choices of technology can help banks reduce cost, increase operating efficiency, and enhance reliability. Towards this end, banks can protect the interest of general customers.

Commercial bank that intends to utilize any system and equipment relating to new technologies in service provision requires approval in principle from the Bank of Thailand in advance. Otherwise, the Bank of Thailand shall not consider an application for service provision with such system or equipment. Regarding service provision with new technologies outside bank premise and/or beyond business hours, the bank shall adhere to the guidelines and the scope of out-of-premise operations.

Even though information technology could actually help reduce service cost, enhance efficiency, expedite service delivery, and improve convenience for customers, IT utilization also poses inherent risks. Hence, security control is critical because if such technological system was impaired, the bank might face immeasurable financial and reputational losses. In addition, there are also unconventional fraudulent practices which, after the moment it occurs, could spread quickly and cause heavy losses and widespread impacts on the country's banking system.

As the Bank of Thailand recognizes the magnitude of these issues, it thereby prescribes practical guidelines for the provision of e-banking services that shall be complied by commercial banks, a user of information technology.

The issuance of this Notification mandates pertinent statutory power in compliance with the Financial Institution business Act B.E. 2551 (2008) and constitutes a

compilation of relevant notifications of the Bank of Thailand relating to e-banking services. Notably, the essence of these regulations still remains the same as that of the previous regulations.

2. Statutory power

By virtue of Section 36 of the Financial Institution Business Act B.E. 2551 (2008), the Bank of Thailand hereby prescribes regulations for the provision of e-banking services as stipulated under this Notification.

3. Scope of application

This Notification shall apply to all commercial banks according to the law on financial institution business.

4. Repealed/Amended Notification and Circulars: See Attachment 1

5. Contents

5.1 Forms of e-banking transaction

When new technologies are utilized in the provision of banking services, commercial bank shall seek approval in principle from the Bank of Thailand prior to the introduction of such service. The extent of new technologies is inclusive of a totally new technology and further development of existing technology to enhance delivery capabilities of banking services. Presently, the forms of e-banking transaction permitted by the Bank of Thailand include:

5.1.1 For service provision of an electronic branch, establishment and service regulations shall adhere to the Notification of the Bank of Thailand Re: Regulations for Operations of Commercial Bank Branch.

5.1.2 To accommodate transactional requirements of internet-based services offered by commercial bank, the Bank of Thailand hereby prescribes regulations for such provision in Attachment 2. However, the commercial bank shall seek approval from the Bank of Thailand in advance. It is noted that commercial banks that have obtained the permission from the Bank of Thailand may continue to operate in accordance with such operating license.

5.1.3 Currently, there is an advent of e-banking services which allows customers to use electronic money to purchase goods and services. The Bank of Thailand has recognized the merits of electronic money business, such as technological development, enhanced efficiency and convenience of banking services for general public, and so forth.

Thus, the Bank of Thailand prescribes supervisory regulations for e-banking services that may be adopted by banks as guidelines for development of e-banking services which conform to stable development of the banking system, financial institution system, and payment system as described in Attachment 3. Accordingly, the commercial bank shall seek approval from the Bank of Thailand in advance. It is noted that commercial banks that have obtained the permission from the Bank of Thailand may continue to operate in accordance with such operating license.

5.2 Electronic fund transfer service

Commercial banks have offered electronic fund transfer service to general customers. With greater convenience and service speed, this service has grown in popularity among general public. However, inherent risks associated with the application of new electronic devices and technology in the service delivery may result in damages which often induce problems and disputes between banks, concerned parties, and general customers. Partly, such problem stems from the fact that customers may lack documentary evidence to attest actual transactions and may not be aware of correct procedures and cautions. In addition, presently there are no provisions, methods, or laws to protect and avert potential losses from electronic fund transfer transaction.

Therefore, it deems advisable to prescribe regulations for electronic fund transfer that may be adopted by commercial banks in their guidelines and practices. Consequently, all concerned parties will be treated fairly and public confidence will grow. Both elements form a solid foundation for and constitute a key factor in further development of an efficient and advanced payment system as stated in Attachment 4.

5.3 Security control

5.3.1 The provision of banking services via electronic media poses a major risk, that is, security risk of data, system, and service network. Thus, banks require an effective security policy and procedures in order to protect the service system from threats, unauthorized access, and thefts of bank and customer data which could result in financial and reputational losses which may lead to loss of confidence in banking services as a whole.

It deems advisable that commercial banks have practical guidelines for establishment of security control policy and procedures for the provision of e-banking services, thus ensuring that service delivery is secure and reliable and customer's interest will be protected. Therefore, it deems advisable to prescribe guidelines for commercial bank's security control practices of e-banking services as stated in Attachment 5.

5.3.2 The development of IT contingency plan is required so that banks can use this as a guideline for policy formulation and efficient planning process of

IT contingency plan. The objective is to prepare contingency responses for various scenarios and mitigate any potential impact as well as normalize the bank's IT system within a suitable period of time as stated in Attachment 6. Consequently, the bank can maintain business continuity or minimize adverse impacts after the services were disrupted by an incident, thus boosting confidence among customers and stakeholders in its service provision.

Nevertheless, such contingency plan is considered only a part of the practical guidelines of business continuity management (BCM) and development of business continuity plan (BCP) which constitutes an operational plan that maintains uninterrupted business operations or normalizes business operations after an emergency situation.

Besides, it is required that commercial bank operates a backup computer system outside the premise where the main computer center is located. Moreover, the backup system should be located quite far from the main computer center. The suspension of service provision to depositors and customers caused by computer system's failure or damage may not exceed one business day.

5.4 Internal control

To persuade commercial banks using computers to process data in various systems to recognize how critical data storage in ever-changing data recording media is, it deems advisable to prescribe minimum data standards of work systems as stated in Attachment 7 which banks may use as guidelines when considering a recording format. However, such data must conform to minimum data standards as prescribed by the Bank of Thailand.

5.5 Other business conducts

Since commercial banks leverage IT outsourcing to a greater extent in order to reduce cost, enhance operational capabilities, and upgrade services to keep pace with rapid technological development, the Bank of Thailand urges banks to adhere to the Notification of the Bank of Thailand Re: Regulations on IT Outsourcing for Business Operations of Financial Institutions. Hence, banks can utilize IT services rendered by other vendors in an efficient and reliable manner to safeguard the interest of customers.

5.6 Forms of banking fraud and prevention

To keep customers abreast of various incidents, enhance security in service delivery, mitigate impacts and damages on bank's businesses as well as to maintain customers' confidence in e-banking services, it is worth learning about various forms of banking fraud.

5.6.1 Using a scanning device (skimmer) to copy information in magnetic strip of customer's ATM card and create a fake card. Banks ought to recognize fraud issues,

be wary of service delivery, and implement fraud prevention measures, thus ensuring that customers can use ATM services securely as stated in Attachment 8.

5.6.2 Regarding internet fraud via phishing, banks that offer internet-based banking services should be wary of service delivery, implement preventive measures, and warn customers about potential frauds as stated in Attachment 9.

5.7 E-banking laws

There are other regulations regarding risk management of e-banking services that commercial banks should further explore to implement risk management enhance security of e-banking services, and ensure that their operations meet international standards, for example, Electronic Transactions Act B.E. 2544 (2001) (See Attachment 10) and the Bank for International Settlement (BIS) by Basel Committee on Banking Supervision which prepared and distributed the Risk Management Principles for E-banking (See Attachment 11).

6. Effective date

This Notification shall come into force as from the day following the dates of its publication in the Government Gazette.

Announced on the 3rd August 2008

(Mrs. Tarisa Watanagase)
Governor
Bank of Thailand

Attachment 1

Repealed/Amended Notification and Circulars

Item	Date of Notification/ Circular	Type	No.	Subject
1	28 May 1985	Circular	BOT. Nor.Wor. (C.) 678/2528	Service Provision of Commercial Bank Using New Technologies
2	23 June 1988	Circular	BOT. Nor.Sor. (C.) 969/2531	Establishment of Contingency Plan and Backup Computer System
3	13 September 1991	Circular	BOT. Nor.Khor. (C.) 1492/2534	Prescription of Minimum Data Standards for Commercial Bank's Operating Systems Using Computer Data Processing
4	5 July 1994	Circular	BOT. Ngor.Kor. (C.) 1230/2537	Guidelines for Electronic Fund Transfer
5	9 November 2000	Notifica-tion		Utilization of Internet Network in Commercial Bank's Business Operations (Circular No. BOT. FPG. (01) C. 3097/2534 Lor.Wor. 15 Nov'00)
6	5 March 2005	Circular	BOT. FPG. (11) C. 525/2545	Submission of the Electronic Transactions Act B.E. 2544 (2001)
7	8 March 2002	Circular	BOT. FPG. (11) C. 559/2545	Submission of Risk Management Principles for Electronic Banking, written by the Bank for International Settlement (BIS)

Item	Date of Notification/ Circular	Type	No.	Subject
8	19 November 2003	Circular	BOT. (C.) 2484/2546	Guidelines for Security Control of E-banking Services
9	10 February 2004	Circular	BOT. Nor.Kor. (C.) 378/2547	Policy Guidelines for the Supervision of E-banking services
10	26 February 2004	Circular	BOT. Ngor.Kor. (C.) 471/2547	Guidelines for Prevention of Banking Frauds by Using Skimmer to Copy Data in Magnetic Strip of Customer's ATM Card to Make a Fake Card
11	12 April 2005	Circular	FSD. (11) C. 695/2548	Guidelines for the Prevention of Internet Fraud via Phishing
12	12 October 2005	Circular	BOT. FPG. (11) C. 1953/2548	Guidelines for Development of IT Contingency Plan

Attachment 2

Using Internet-based Services in Banking Businesses

The Bank of Thailand hereby stipulates guidelines concerning permission for commercial banks to utilize internet-based services in banking businesses as follows:

1. Using internet-based services to disseminate information about banking businesses in a manner similar to advertising or about various services such as loan request procedures, loan application form, documentary evidences, and interest rates. These activities may be conducted to serve general customers or specifically cater to an individual customer. Commercial banks can perform such deeds without having to obtain prior approval from the Bank of Thailand.

2. Utilization of internet-based services in banking business and related businesses or any conducts indispensable for banking operations shall require prior approval from the Bank of Thailand.

Commercial banks that have been permitted by the Bank of Thailand to utilize internet-based services in banking businesses could use internet-based services for approved transactions.

3. To obtain permission, commercial bank shall submit an application as prescribed by the Bank of Thailand (Appendix 1 – Attachment to Annex 2) together with the followings:

3.1 Operational plan for internet-based transactions: At least such plan should contain information on system and data security measures, risk assessment and contingency plan, development of system technologies and security facilities, staff training and development, internal control system, solutions for potential legal issues that appreciate the right and interest of customers.

Accordingly, the bank shall be prepared to elaborate or provide additional explanation and comply with the Bank of Thailand's directives.

3.2 Provide documentary evidences for each transaction executed by customer that can be used as a legal evidence and retain copies of required documents for inspection by the Bank of Thailand.

4. After a period of 60 days following the filing of the application and support information stated in Item 3, if the Bank of Thailand has no objection or requests for additional written explanation, the permission shall be deemed effective and the bank shall be officially permitted after receiving a notice from the Bank of Thailand.

5. After the permission in Item 4 is obtained, the bank shall be able to provide internet-based services in banking businesses under the following scopes:

5.1 The bank can use internet-based services for additional transactions which are an extension of approved transactions without having to re-apply for approval of internet-based services. However, it is required that the bank modify the operational plan in support of such transactions.

5.2 The bank may display trademarks/logos or messages pertaining to other businesses on its website to accommodate the needs of end users who can learn about other businesses of which financial transactions can be made through the bank or to open up a channel for access to other businesses in the website by end users, with an exception of home page, the main website's screen, which displays only banking services.

Nevertheless, the bank shall not be allowed to generate revenue from display of logos or messages of other businesses similar to advertisement of other businesses or perform any action which may be considered advertisement or solicitation to persuade end users to obtain any service in the website of other businesses associated with the bank.

5.3 The bank shall not allow customers to follow steps to buy and sell products or services of other businesses on its website.

6. Regarding imposition of service fees for internet-based services and other businesses on end users, the bank shall adhere to market mechanism to stimulate competition and consider impartiality for all customers.

Where there are contractual terms imposed on the bank and customers or the bank and other businesses that oblige the bank to fulfill certain obligations, the bank shall perform such obligations. However, the bank has certain disclaimer, such disclaimer shall not constitute limited liability on fraud or gross negligence and violation of laws.

Appendix 1 of Attachment 2

Application for Utilization of Internet-based Services in Banking Businesses

Written at .....

Date .....

Governor, Bank of Thailand

Dear Sir/Madam:

.....desires to request for permission to use internet-based services in banking businesses in accordance with the internet-based transaction operational plan and documentary evidences used for the transactions listed below:

(1) .....

(2) .....

(3) .....

(4) .....

(5) .....

If the Bank of Thailand requests for additional support information or other details, I shall verbally present the required information and/or deliver additional details to the Bank of Thailand as requested. Aside from that, if the Bank of Thailand stipulates any condition before and after the granting of the permission, requiring that I perform or omit any act, I shall strictly abide by such condition.

For your consideration and approval.

Signature .....

(.....)

Authorized person

List of documentary evidences attached to the Application for Utilization of Internet-based Services in Banking Businesses

Required information that must be submitted along with the filing of an application includes at least the followings:

1. **Internet-based transaction operational plan**

    1.1 System and data security measures

    (Please specify applicable technology)

    1.2 Risk assessment

    1.3 Contingency plan

    1.4 Development of system technologies and security facilities

    1.5 Staff training and development

    1.6 Internal control system

    1.7 Solutions for potential legal issues that appreciate the right and interest of customers

2. **Documentary evidences for internet-based transactions**

Attachment 3

Supervisory Guidelines for E-banking services

Commercial banks intending to provide e-banking services shall request for permission from the Bank of Thailand in accordance with Section 36 of the Financial Institution Act B.E. 2551 (2008). In such approval, the Bank of Thailand shall consider potential impacts and risks on banking system, payment system and so forth as well as capabilities and credibility of participating vendors. In addition, the Bank of Thailand shall not impede technological and business developments which might adversely affect the country's competitiveness.

Contents

1. Features of electronic money

Electronic money or so-called multipurpose stored value card, e-purse, e-wallet, or smart card has three main features as follows:

1.1 Consumer pays money to an issuer of electronic money in advance (pre-paid).

1.2 Pre-paid money is recorded in electronic media (stored value), such as plastic card or other computer media.

1.3 Consumer can use electronic money to purchase products and services from retail outlets as specified by an issuer of electronic money.

2. Risks and impacts of electronic money

Usage of electronic money in an economic system may pose inherent risks and impacts on banking system, financial institution system, and payment system. To cope with such risks and impacts, the Bank of Thailand may prescribe supervisory guidelines to control potential risks and impacts as follows:

2.1 Impacts on banking system

Impacts

Usage of electronic money as a substitute for currency issued by the government sector impacts on abilities to control inflation and maintain economic stability of the central bank in two ways, that is,

(1) Money multiplier that may increase due to reduced necessity of bank notes used as a medium of payment.

(2) Monetary volume that may increase due to of the inclusion of electronic money used as a medium of payment in the definition of monetary volume and due to the fact that service providers can use pre-paid money (float) to further engage in other transactions.

Supervisory approaches

(1) Closely monitor and control electronic money volume in the system

(2) Prescribe cash reserve to electronic money ratio (where necessary)

2.2 Impacts on financial institution system and payment system

2.2.1 Liquidity risk stemming from the fact that issuer of electronic money may not be able to repay the money because of unscrupulous fund use and inefficient financial management and so on.

Impacts

(1) Revenue and payment abilities of other concerned parties, such as other participating financial institution or retail outlet

(2) Loss of consumer's money that has been paid to the issuer of electronic money in advance

(3) Consumer confidence in the system

Supervisory approaches

(1) As a service provider, banks must have suitable risk management system.

(2) The Bank of Thailand may prescribe requirements for float management, where necessary.

2.2.2 Operational risks stemming from deficiency in the system's security measures and frauds committed by the service provider or participating vendors

Impacts

(1) Data accuracy and confidentiality

(2) Uninterrupted services

(3) Reliability of payment system and financial institution system

Supervisory approaches

(1) Banks shall adhere to the guidelines prescribed in this notification and the Notification of the Bank of Thailand Re: IT Outsourcing and so forth.

(2) Encourage service providers to select only technologies that meet international standards.

(3) Require banks to adhere to good governance principles.

2.3 Other impacts

2.3.1 Consumer protection

Since electronic money services require consumers to pay cash in advance to exchange for electronic money, consumer protection is thus very important. In such service provision, key considerations include

(1) Scope of responsibilities of issuer of electronic money, retail outlet, and consumer in case of losses incurred from fraud, mistake, lost card (where monetary value is recorded on the card)

(2) Service fee

(3) Refund terms

Supervisory approaches

(1) Banks offering e-banking services must adhere to good governance principles.

(2) Educate and inform consumers and concerned parties about service provision and potential risks in explicit and transparent manners.

2.3.2 Since some form of e-banking services may facilitate money laundering, for example, the system whereby one customer can transfer money to another customer by bypassing the system of service provider.

Supervisory approaches

(1) Prohibit direct money transfer without passing through the information system of service provider.

(2) Service system must be able to trace back past transactions.

(3) Set maximum amount of electronic money to be used.

(4) Issued electronic money must be in Thai baht and used only in Thailand.

Attachment 4

Guidelines for Electronic Fund Transfer

These guidelines for electronic fund transfer were developed to protect the interest and ensure fairness of the service agreement executed between bank and customer. In addition, concerned parties and the bank's service staff would recognize the obligations and take necessary actions within the scope of prescribed rights, duties, and responsibilities. Furthermore, commercial banks are obliged to modify relevant procedures and terms of the service agreement in accordance with the prescribed minimum standards. Accordingly, banks shall notify or announce to general customers to ensure that users are aware of modified service procedures and terms. The guidelines and procedures are described below:

1. Contents

In these guidelines,

1.1 "Electronic fund transfer" is referred to money transfer through terminals, electronic communication devices, computers, or recording media of computer data that orders bank to transfer money in or out of a bank account, for example, services through automated teller machine (ATM) and point of sale (POS) fund transfer as well as office banking services, internet banking, and tele-banking services.

Money transfer will be completed only when a transferee or beneficiary receives cash or credited amount in the transferee's bank account is equal to the transferred amount transmitted from transferor bank or the transferee bank already receives the transferred amount. In the end, the transferee can use that money.

1.2 "Illegitimate electronic fund transfer" is referred to money transfer made by a third party without consent from a customer. In the end, the customer does not gain any benefit from such transfer. The cases other than the ones below are considered legitimate electronic fund transfer.

1.2.1 The customer voluntarily gives fund transfer tool to other person.

1.2.2 The customer commits an unscrupulous act alone or with other person.

1.2.3 The transfer was caused by the bank's failure and the bank later made a correction.

1.2.4 Fund transfer transaction whereby evidence indicates that the transfer was facilitated by the customer's "fund transfer tool" that was given to the customer by the bank.

1.3 "Fund transfer with pre-authorization" is referred to electronic fund transfer pertaining to a contract executed beforehand for agreed transfer transaction, such as bank debit for utility payment and payment of goods and services.

1.4 "Fund transfer tool" is referred to ATM card, debit or credit card, password, magnetic disk with embedded program or other tools given to a customer by the bank so that the customer can use it as a tool to transfer money in or out of bank account.

1.5 "Customer" is referred to a customer that opened a bank deposit account and entered into a service agreement for electronic fund transfer or transfer transaction with the bank.

1.6 "Fund transfer evidence" is referred to documentary evidence such as transaction slip, transfer notice, bank statement, and other evidences which are generated by computer and data recording media such as magnetic tape, magnetic disk, or other data recording media used for storing information.

Each type of fund transfer evidence shall contain transactional details of fund transfer in or out of customer's bank account.

2. Details

2.1 Commercial banks shall prepare at least two duplicates of a written service agreement for electronic fund transfer entered with a customer. One copy of the agreement is given to the customer as evidence. Beside essential contents of the contract pertaining to the obligations of contractual parties, the bank shall specify or stipulate the following contents and instructions as follows:

2.1.1 Title and description or type of service

2.1.2 Statement that underscores the importance and safekeeping of fund transfer tools and provides instructions to customer in case fund transfer tools are damaged, lost, or stolen or in case any fund transfer tool will be replaced upon its expiry date.

2.1.3 Service terms that at least cover details like date and time of service availability, maximum number of daily transactions and maximum amount of daily transfer, and estimated timing for completion of fund transfer.

2.1.4 Service fee or other expense (if any) imposed on customers

2.1.5 The right of customer pertaining to receipt of documentary evidence whenever a transfer is made or service is obtained through all types of bank account, such as transaction slip, transfer notice, and bank statement which may be used as evidence of transfer transaction.

2.1.6 Method and place where customer orders or notifies the bank to freeze or suspend fund transfer tool or fund transfer with pre-authorization and the period of time whereby the bank will fulfill the customer’s order or request.

2.1.7 Commercial bank may be liable to customer as follows:

(1) The bank performs or omits to perform fund transfer order, thereby causing failure in receiving money from electronic fund transfer within stipulated time as stated in 2.1.3, unless

(1.1) The customer has insufficient account balance.

(1.2) The customer does not have a credit line or the credit line granted by the bank has been suspended.

(1.3) Fund transfer renders account balance exceed the agreed credit line.

(1.4) Legal proceeding is ongoing.

(1.5) The bank informs the customer about fund transfer’s malfunction before or during the fund transfer's execution.

(1.6) The customer breaches terms of the agreement.

(1.7) Fortuitous event

(2) The bank does not pursue the order to freeze fund transfer with pre-authorization as stated in 2.1.6 or seize the customer's fund transfer tool as stated in 2.6 and later electronic fund transfer occurs.

(3) The bank does not provide a fund transfer tool to the customer and an illegitimate fund transfer occurs.

(4) Illegitimate fund transfer occurs and the customer is not at fault.

2.1.8 Liabilities of customer

Where electronic fund transfer is transacted after fund transfer tool was lost or stolen, the customer shall be liable for the transferred amount that was executed before the bank completed the seizure or freezing of the fund transfer tool or fund transfer with pre-authorization within a stipulated time frame described in the agreement as stated in 2.1.6.

2.1.9 In the event the customer discovers any transactional error in fund transfer and reports such error to the bank, the customer shall report the following information:

(1) Date and time of transaction

(2) Terminal location

(3) Account number of the customer and the concerned party

(4) Type of transaction

(5) Amount of transferred money

2.1.10 Guidelines and procedures for commercial bank's investigation and rectification of such error

2.1.11 Method for termination of service agreement for electronic fund transfer by contractual parties

2.2 Commercial bank may provide fund transfer tool to a customer under the following conditions:

2.2.1 Upon request by the customer

2.2.2 As a replacement for fund transfer tool that is damaged, lost, or stolen or fund transfer tool needs to be replaced when it lapses.

2.3 Commercial bank shall prepare a manual or document to clearly explain detailed steps or procedures of service provision to all customers.

2.4 Commercial bank shall store evidential information in the following formats that can be recalled and easily understood.

2.4.1 Magnetic tape

2.4.2 Magnetic disk

2.4.3 Other data recording media used for data storage

2.4.4 Document or computer report printout

2.4.5 Documentary evidence provided to customers by the bank as stated in 2.1.5

2.5 Where commercial bank designates other party to execute or jointly execute electronic fund transfer or perform other duties associated with or to facilitate electronic fund transfer, the bank shall be held accountable for any action as if the service is rendered solely by the bank. In addition, such designated party shall be instructed to store required information in a format as stated in 2.4.

2.6 Commercial bank shall promptly freeze or suspend fund transfer tool or fund transfer with pre-authorization and prepare an evidence of such notice after customer requests suspension of such tool. In this case, the customer shall not be liable for any loss incurred after instructing the bank to freeze such fund transfer tool.

2.7 Commercial bank shall promptly produce and provide the customer with transaction slip for each transaction after completing each step and the transaction. In addition, this also include transaction whereby money is not paid to the customer or other reasons relating to failure or incompletion of fund transfer, except the case whereby the bank already informed the customer in advance or an incidence is considered a fortuitous event. A transaction slip should at least contain the following information:

2.7.1 Terminal site code

2.7.2 Transaction date and time

2.7.3 Type of transaction

2.7.4 Account numbers of transferor and transferee

2.7.5 Transferred amount and outstanding balance

2.7.6 Code or text displayed to indicate whether transfer transaction fails or is uncompleted.

2.8 Require commercial bank to prepare bank statement that shows all transactional details or account movements for each customer. Such details shall at least include the followings:

2.8.1 Each transfer-in (credit) or transfer-out (debit) transaction; pertinent details include transaction date, type of transaction, and transferred amount

2.8.2 Service fee or any expense imposed on customers by the bank

2.8.3 Daily closing balance of the account and carried-over and carried- forward amount

2.8.4 Location and telephone number of bank office or branch where customers can contact conveniently

2.9 In case of fund transfer with pre-authorization, commercial bank shall deliver transfer notice that indicates debit amount to the customer within one month from the transfer date. The transfer notice shall include at the least the followings:

2.9.1 Transfer date

2.9.2 Transferor and transferee account numbers

2.9.3 Transferred amount and account balance before and after each transfer

2.9.4 Names of transferor and transferee

2.10 Commercial bank shall investigate failure of fund transfer reported by customer as stated in 2.1.9 and make suitable adjustment within 30 days from the notification date. If it was found that the bank was held liable for such failure and a reimbursement was called for, the bank shall transfer the reimbursed amount to the customer's account. Accordingly, interest payment will be calculated retrospectively from the transfer date when the amount was debited from the customer's account.

When pursuing such investigation and corrective action, the bank shall deal with the matter methodically in accordance with the provision in 2.1.10. The bank that jointly engaged in electronic fund transfer or was designated to do so shall be responsible for the investigation in order to gather pertinent evidences and facts concerning possible causes relating to or failure of its tool or equipment. The participating

bank shall report the findings to the customer's bank within 15 days from the notification date of such failure by the customer or the bank, whichever case may happen first.

2.11 Commercial bank shall inform the customer or account owner of the findings of such investigation as stated in 2.10 within seven days from the date the bank learns about the findings.

2.12 Commercial bank shall ensure that the electronic fund transfer system be inspected by an external auditor at least once a year.

2.13 Where commercial bank intends to amend any requirement or terms of the service agreement of electronic fund transfer, customers shall be informed of such revision at least 15 days in advance. Where such revision imposes higher expense or additional obligations, evidence shall be provided to attest that customers give consent or do not object to such revision.

2.14 Other provisions or terms in the service agreement for electronic fund transfer shall not contradict with these guidelines.

2.15 Commercial bank shall post a notice of the provision or agreement as stated in 2.1 in a highly visible place in every office or inform all customers of such details. In addition, commercial bank shall also inform the Bank of Thailand of its guidelines and procedures as stated in 2.1.10.

Attachment 5

Guidelines for Security Control of Electronic Fund Transfer

---

1. Rationale

1.1 Commercial banks throughout the world competitively offer all kinds of service to customers. Banking services offered through electronic media signify a channel to which both banks and customers give much more attention because of its speed and convenience. In addition, customers can perform transactions anytime anywhere without having to come to bank office. Currently, several banks are offering internet-based banking services to customers after obtaining approval from the Bank of Thailand.

1.2 Nonetheless, commercial banks keen on offering banking services through electronic media must seriously consider strategic implications of such services. Due to rapid technological changes, banks require a high initial outlay and must consider technologies that can best serve customers. Board of directors of a bank must prudently assess strategic risks and should not resolve to offer such services only to catch up with other banks but should formulate a strategy befitting the organization.

1.3 Even though e-banking services enable banks to respond to customer needs faster and more efficiently, they increase various types of inherent risks, especially security risks of service information, system, and related networks.

1.4 Security risk is referred to potential risk in service system of financial institution which may be vulnerable to threats or various forms of illegitimate access, such as unauthorized access from both inside and outside the organization, theft of in-transit data, unauthorized transaction using false authentication, and hacking that renders system inoperative. Beside using computer skills to tamper with the system, the bank's service system may be vulnerable to other deceitful attempts that lure banks and customers to authorize access to the system or release vital information (social engineering).

1.5 In other countries, commercial banks have experienced intrusion into data systems by hackers and suffered losses. Such loss also poses considerable reputational risk for banks. Without operating processes designed to resolve problems

and inform customers quickly, such loss might be so severe that customers lost confidence, causing deposit run on the bank.

1.6 When e-banking services are offered, commercial banks shall be cognizant of security control of the service system, encompassing various elements ranging from the internal system to electronic media used by customers to perform transactions. In other countries, hackers successfully penetrated customer's system and changed data to perform transaction by using false authentication (cookie poisoning). By using this technique, if no security system is installed in electronic media used by customers, the system might be harmed. Moreover, customer advice on provision of suitable security system is also instrumental in enhancing the effectiveness of the security procedures of commercial banks.

2. Contents

2.1 In these guidelines,

"E-banking services" is referred to provision of banking services through electronic media whereby customers can perform transaction by themselves.

"Banking services" is referred financial transactions and related ones whereby banks are permitted to operate, such as fund transfer, payment of goods and services, and displaying information in customer's bank account as well as request for, examination, confirmation, change, and revision of customer data and transmitting order or exchanging information with customers so as to facilitate financial services and transactions.

"Electronic media" is referred to equipment or tool used by banks as a channel for e-banking services, such as data recording media, communication devices, computer, and various forms of network.

"Service system" is referred to information technology system and other technological systems involving in the provision of e-banking services, such as database system, applications, operating system, and network system.

"Security technology" is referred to technique, computer tool, or various electronic devices used by banks in implementation of security control for e-banking services.

2.2 Principles

2.2.1 These guidelines place emphasis on security of banking services through public network such as internet and wireless communication network which are interlinked with the bank's internal network. As a result, it is highly likely that banks may be harmed by various forms of threat from intruder.

2.2.2 Commercial bank that uses public network for dissemination of business information (informational website) should apply the principles of these guidelines in the development of suitable security measures in order to prevent unauthorized access that intends to amend or modify disseminated information which may undermine the bank's reputation and customer confidence in banking services in the future when the scope of e-banking services will be further broadened.

2.2.3 Commercial bank may apply these guidelines in the provision of e-banking services through other channels with lower risk profile, such as service provision through proprietary network.

2.3 The contents of these guidelines are divided into three parts:

2.3.1 Formulation of security policy

2.3.2 Principal system security procedures that comprise the following security technologies:

(1) Access control

(2) Authentication and non-repudiation

(3) System and data integrity

(4) Data Confidentiality

(5) System availability

(6) Monitoring of abnormalities and vulnerabilities in the service system (system detection)

(7) Incident response and report

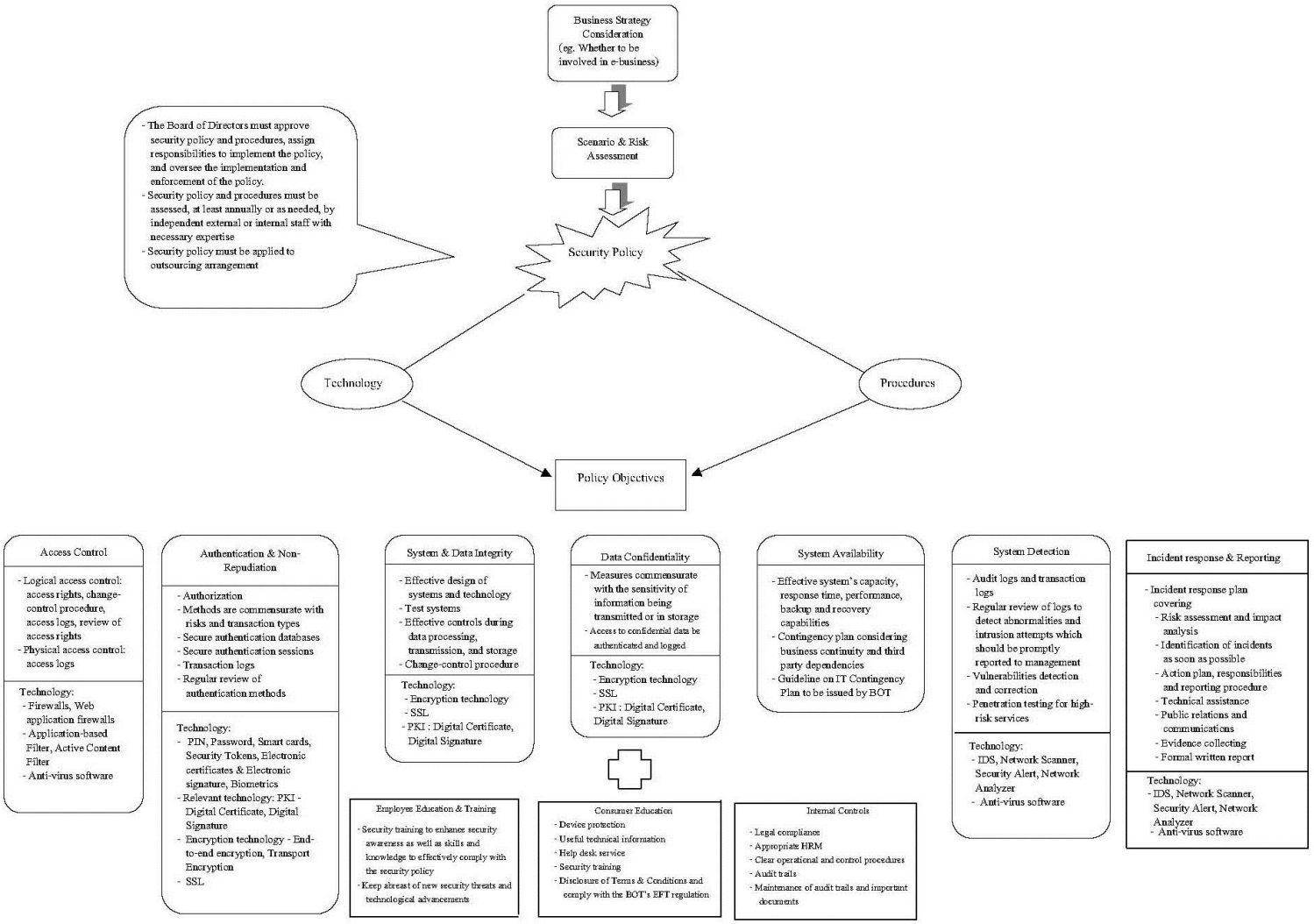
2.3.3 Security enhancement includes

(1) Staff training and orientation

(2) Dissemination of information and advice to customers

(3) Internal control

In the following page, overall contents of the guidelines are summed up in an easy-to-understand diagram.



BOT Notification No 26-2551 (6 September 2017)-check

3. Detailed guidelines

3.1 Security policy

3.1.1 The bank's board of directors shall be directly responsible for formulation of a written security policy for e-banking services and approval of security procedures which is proposed by the management. Accordingly, at least strategic applicability and insights into potential risks should be considered. The board may assign IT committee, risk management committee, executive board, or experienced external consultant to develop a security policy before presenting the proposed policy to the board for approval.

3.1.2 In the development of the security policy for e-banking services, critical factors that must be considered include the balance between security procedures and potential risks that may arise from related transactions and rapid technological changes.

3.1.3 After approving the security policy and security procedures, the board shall designate executives and employees to oversee the implementation of the approved policy and procedures, communicate to all employees, monitor to ensure that employees and parties associated with the system strictly adhere to the security policy and procedures, and review compliances where necessary. The effectiveness of security procedures depends on the existence of a coherent policy, effective communication, and suitable enforcement. Certainly, education and promotion of the awareness about security control and accountabilities among all levels of executive and employee will positively contribute to the implementation of the procedures.

3.1.4 The board shall conduct assessment of the effectiveness of the security policy and procedures at least once a year or every time there are changes that might affect security control, such as launching of new product and service, modification of existing technology, or hacking incident. Such assessment may be carried out by external or internal experts who are not a system developer or system administrator. Furthermore, the bank should closely monitor technological advancement which will be used as inputs for further development of a more efficient security policy and better security procedures.

3.1.5 Where the bank resorts to IT outsourcing for provision of e-banking services, wholly or partly, the board shall arrange for assessment of the efficiency

of security procedures of service providers in accordance with the stipulated security policy and the Notification of the Bank of Thailand Re: IT Outsourcing.

3.2 Principal security procedures

Since e-banking services through public network such as internet and wireless communication networks have open infrastructure, commercial bank must establish a link between public network and internal network. Consequently, the service system is prone to high risks and vulnerable to various forms of threat from hackers that can harm banks, for example, imitating IP address to gain unauthorized access to internal network linked with the internet network, harming the service system by overloading the website, hacking into the service system to forge information with spurious software, or infecting the service system with computer viruses.

Therefore, the bank must have good security control procedures and choose effective security technologies that meet pertinent standards in order to safeguard against threats. When the system becomes under threats, such technology can control damages and resolve problems. The principal security procedures for e-banking services include:

3.2.1 Access control

The procedures and technologies that control access to the service system must be able to prevent unauthorized access by internal and external entities and control access to the service system’s site and hardware (physical access control) and provide access control with computer techniques (logical access control). Such procedures should include

(1) Stipulation of access rights that conform to customer's service needs and service staff’s responsibilities and regular review of access rights

(2) Designation of authorized individual assigned to amend such access rights

(3) Keeping access logs, revision of access rights, and login and logout records of the service system’s site which will be used as evidence in case problem arises.

Examples of technologies that can safeguard against unauthorized access:

- Various types of firewall installed at network and application levels which are intended for detecting and filtering out deceitful data or codes from entering the service system

- Detection and filtering tools that detect and block out deceitful programs or data from entering service system

- Anti-virus software

3.2.2 Authentication and non-repudiation

Authentication and non-repudiation procedures and technologies are not only useful in verification of customer's identity before granting authorization to use the service, but they also benefit customer with respect to verification of customer's identity when he or she executes a transaction with the bank in case dispute arises. Such procedures should encompass the followings:

(1) Provision of authentication techniques and customer's right to use service before authorizing customer to access the service

(2) Provision of authentication techniques that are commensurate with risk level and transactional features and amount

(3) Provision of access control and alteration control of authentication database

(4) Customer identity authentication must be conducted safely on an ongoing basis. If any disruption occurs, authentication should commence again.

(5) Maintaining transaction logs as evidence for examination and keeping such logs in secure storage.

(6) Regularly review authentication techniques by considering risk level and ever-changing technological advancement.

Examples of authentication and non-repudiation technologies

- Password, PIN, tool or card used for storing personal data (tokens or smart card), biometrics

- Public Key Infrastructure (PKI) technology that facilitates creation of digital certificate and signature

- Encryption technology that facilitates customer identity authentication

- Use of highly secure channel for transmission and receipt of authentication data, e.g. Secure Sockets Layer (SSL)

3.2.3 Maintaining system and data integrity

The procedures that maintain the integrity of the service system and in-transit data, processed data, and stored data as well as ensure that the service system can operate effectively and satisfy customer needs efficiently should encompass the followings:

(1) Design of the service system and selection of efficient technology

(2) Conduct system testing to ensure system integrity before startup or whenever change occurs

(3) Provision of operational control of the service system, especially critical steps like procedures, processing, data transmission and storage so as to prevent unauthorized access

(4) Implementation of stringent change control procedures

3.2.4 Data confidentiality

Data confidentiality procedures and technologies, especially in-transit data, processed data, and stored data should encompass the followings:

(1) Provision of secure data transmission, processing, and storage that are commensurate with the degree of data criticality so as to avert exposure of confidential data and safeguard against illegitimate alteration.

(2) Provision of security control that allows only person with access right that passes authentication test to get access or change confidential data

(3) Maintaining access logs and revision records of confidential data which can be used as evidence in examination and keeping these evidences in secure location.

Examples of technology that maintains data integrity and confidentiality

- Encryption technology for confidential data, such as encryption for in-transit data (transport encryption), end-to-end encryption, and storage encryption

- Use of highly secure channel for transmission and receipt of confidential data, e.g. Secure Sockets Layer (SSL)

- Public Key Infrastructure (PKI) technology that facilitates creation of digital certificate and signature for authentication purpose before gaining access to confidential data

3.2.5 Maintaining system availability

The process that ensures system availability should encompass implementation that controls the service system's efficiency and system availability on an on-going basis. At least the service system should have capabilities to provide sufficient services during time period agreed with customers, accommodate transactions that meet customer needs adequately and speedily both during normal and peak hours. Moreover, the system should have proper data backup system so that system can be restored in a timely manner in case damage occurs.

With respect to contingency planning to cope with potential damage that may happen unexpectedly, the bank should develop a contingency plan to maintain system availability that deals with disruption stemming from the external system of third-party entities which the bank must depend on or have the system connected to. Accordingly, banks shall adhere to the guidelines in this Notification Re: Guidelines for Development of IT Contingency Plan (Annex 6)

3.2.6 Monitoring system abnormalities and vulnerability (system detection)

The procedures and technologies utilized to monitor system abnormalities and vulnerabilities should encompass the followings:

(1) Provision of audit logs for critical activities, such as system access, transaction log, access to authentication database, and service staff's conduct; such audit logs should be securely stored.

(2) Regular monitoring and review of audit logs, particularly transaction logs which may indicate abnormalities and likelihood of threat or intrusion attempt; any abnormality, whenever it is found, should be reported to management so that preventive plan can be developed before an incident actually happens.

(3) Continuous detection and rectification of system vulnerabilities, particularly network system, applications, and database; because intruder can capitalize on such defect to harm the system and gain unauthorized access. Most known vulnerabilities should be disclosed to general public in the website on an ongoing basis so that concerned parties can safeguard own system and upgrade their security system.

(4) Penetration test: The aim is to test the efficiency of security technology, especially high-risk service system like fund transfer

Examples of abnormalities and vulnerabilities detection technology include

- Intrusion Detection System (IDS)

- Technologies used for detection of spurious software or data in the system, such as network scanner, network analyzer, and security alert systems

- Anti-virus software

3.2.7 Incident response and report in case the system is harmed by threats

The procedures for incident response and report in case the system is harmed by threats or hacking incidents should encompass the followings:

(1) Assessing the likelihood of various threat and intrusion scenarios, including damage and impact assessment of such incident

(2) Prompt problem identification

(3) Action plan, designation of responsible personnel that should be trained to analyze and deal with potential problems; and reporting procedures

(4) Data preparation and procedures for requesting assistance from internal and external experts, particularly technical assistance

(5) Communication and public relations: These activities disseminate proper information and promote understanding among employees, mass media, and customers as soon as possible about the problem and how the problem is solved. The aim is also to preserve the bank's image and reputation and boost confidence of customers and concerned parties.

(6) Gathering evidence for prosecution of hacker, such as access logs that are an evidence of access to database and other parts of the service system, hacker's computer used as a communication device, hacker's bank account involved in fund transfer, information about source, destination, route, date, time, and so forth.

(7) Preparation of a written incident report that will be presented to the board of directors: However, the board may delegate the task of reviewing the report to IT committee, risk management committee, or audit committee. If the incident resulted in significant loss and impact on the bank's reputation and operation, the board might also instruct the designated committee to present such report to the board.

The written report should contain the followings:

(7.1) Date, time, and location where the system is damaged by the threat or hacking incident.

(7.2) Description of hacking incident, hacking technique, and hacker (if known)

(7.3) Description of cause and damage; identification of damaged data, work system, or electronic medium

(7.4) Damage assessment

(7.5) Actions already taken to solve the problem and next actions

(7.6) Details about responsible personnel at the location where the threat or hacking occurred, such as name, position, address, telephone number, and roles and responsibilities.

Banks should prepare information for the Bank of Thailand's inspection.

Examples of technology applications that deal with threat and hacking incident

- Intrusion Detection System (IDS)
- Technologies used for detection of spurious software or data in the system, such as network scanner designed to solve problems or abnormalities (Appendix 1 of Attachment 5: Examples of security technology for e-banking services)

3.3 Security enhancement procedures

3.3.1 Staff training and education

The bank should implement staff training and development programs on an ongoing basis for all levels of executive and employee involving in service provision. The aim is to raise awareness about service security and ensure that service provision complies with security policy and procedures to a full extent. Aside from that, concerned executives and employees should closely monitor latest technological development and threats and disseminate useful information to the rest of the organization.

3.3.2 Offering advice to customers

The bank should provide useful information and advice to customers, such as using the service securely, technical information or advice on how to keep computer system and hardware secured while executing a transaction, because intruder can hack into customer's system to steal information and use false identity to transact with the bank. Moreover, customers should also be advised to be wary of downloading software from unknown or suspecting sources and usage of such software because intruder might conceal malicious software in the downloaded one. (Appendix 2 of Attachment 5: Advice for e-banking customers)

Such information and advice should be described in layman's language in bank's website where customers can access readily. To further facilitate dissemination of customer advice, the bank may provide Help Desk service assigned to respond to queries and give advice on e-banking services. Furthermore, the bank may organize customer training program in order to provide knowledge and enhance understanding about security measures that may be relevant to customers and bank's security system that customers should know. Such training program is another mean to promote awareness and raise confidence in e-banking services.

The bank should disclose service agreement and terms to customers and solicit customers to accept the agreement and terms before deciding to subscribe to the services. For fund transfer service, banks shall adhere to this Notification Re: Guidelines for Electronic Fund Transfer (Annex 4)

3.3.3 Internal control

The bank should establish suitable internal control procedures for e-banking services, for example, ensuring that e-banking services do not

violate relevant legal provisions and regulations of concerned authorities, whether operational modes and applicable technologies, administration of concerned personnel adheres to a suitable principle of segregation of duties, having explicit operating procedures, suitable supervision of the operations, maintaining activity logs of service staff, safekeeping of service logs and important documents relating to service provision.

Appendix 1 of Attachment 5

Examples of security technology for e-banking services

A. Security technology for the service system

The security technologies for the service system interlinked between internal and external networks, especially internet and wireless communication networks, include

1. Firewall

Firewall is a technology that prevents intrusion into internal network by examining and authorizing access only to pertinent information that passes through the network. It also blocks data and codes sent from suspicious sources.

The effectiveness of firewall depends on design, installation, control, and maintenance. The design, installation, control, and maintenance procedures should be clearly described in a written document. To enhance firewall's effectiveness, continuous inspection and improvement procedures should also be established.

Applications of the firewall technology for the security of the service system should include

1.1 Installation of external firewall to control data transmission between external network and web server

1.2 Installation of internal firewall to control data transmission between web server and internal network

1.3 Using different types of firewall for each layer to make intrusion protection more formidable

1.4 Stipulation of clearly written operating procedures for firewall, such as installation, configuration setting, control, and maintenance for the benefit of monitoring and maintenance and so as to engage it promptly in case damage occurs.

2. Encryption technology

Encryption technology is a technique that can maintain data confidentiality and integrity by transforming data into an unrecognizable format. The

effectiveness of encryption technology depends on cryptographic algorithm, cryptographic key, and key management process.

When encryption technology is considered, selected technology should be commensurate with risk level, data criticality, and required degree of security. Key considerations include

2.1 Selected encryption algorithm should be tested to meet certain security standard, such as TripleDES, AES128/192/256, SSL/RC4/128, and RSA 1024+. Bank should also closely monitor the development of encryption algorithm.

2.2 Implementation of efficient key management process. Any operation relating to all types of key such as creation, storage, delivery, and alteration should be conducted carefully under proper control procedure.

2.3 Implementation of efficient control of data transmission: Data transmission between the bank and customer should pass through a highly secure channel like Secure Sockets Layer (SSL). Transmission of confidential or critical data like password should be subjected to encryption from the point where customer begins to enter data and along the route towards the server in the internal network where processing takes place (end-to-end encryption). Additionally, in-transit critical data should also be encrypted (transport encryption).

2.4 Establishment of security system for encryption and decryption hardware and software.

3. Intrusion detection system

The intrusion detection system is a technology that can detect abnormalities, hacking, or intrusion into internal network or database by analyzing data flown through the network and compare data features with those of data posing intrusion threat or by analyzing behavioral pattern of the network's operation that deviates from the normal pattern.

The intrusion detection system should be installed at critical server or internal network. Moreover, reporting procedures should be established where abnormalities or intrusion attempts are observed.

4. Other security technologies

4.1 Install active content filter or a tool that can detect and block malicious software, codes, files, or emails from entering into internal network.

4.2 Install web application firewall or scanner to detect and block malicious instructions or codes from entering into the web application layer of internal network

4.3 Install anti-virus software to safeguard the service system.

B. Authentication technology

Presently, there are authentication technologies as follows:

1. Password and personal identification number

This is the most common authentication technique because its usage is easy and convenient. Customer must enter user name and password that is a personal identification number (PIN) for verification by the system before accessing to the service. The efficiency of the service system that uses password as the authentication technique depends on safekeeping of password and requirement of password's format and length and other relevant control measures.

The service system that uses password as the authentication technique should conduct the followings:

- Give advice to customers and staff about requirements and safekeeping of password.
- Stipulate suitable format and length of password that is commensurate with risk level of each transaction. Generally, password should be at least eight characters long, whether numeric, alphabet, or alphanumeric.
- Name of person, place, or vocabularies found in Thai and English dictionaries may not be used in a password.
- Suspend service to user whose failed login attempts exceed designated quota.
- Stop service when the system has not been active for a certain period of time
- Determine a suitable usage life of password.
- Establish secure procedures for password creation, delivery and receipt as well as safekeeping of password. Password should be encrypted while it is being transmitted or received and stored.

- Segregate database where passwords are stored from other databases that is subjected to stringent security measures.

2. Electronic certificate and signature

Electronic certificate is electronic data or any other data record that attests linkage between signature owner and data used in creation of electronic signature.

Electronic signature constitutes alphabet, character, number, sound, or other symbol created in an electronic form which is used to supplement electronic data to validate relationship between an individual and electronic data. The objective is to identify a person who is the owner of electronic signature associated with such electronic data and indicate that that person accepts such electronic data.

Public Key Infrastructure (PKI) technology which is an effective authentication technology and a technology that can effectively maintain data confidentiality and integrity can be used to create electronic signature and certificate called digital signature and digital certificate.

PKI technology arises from the principles of public key and private key which are produced from algorithms tested and proven to be secured. Public key is kept by a proprietor that issues electronic certificate or so-called certificate authority. Private key is kept confidential in computer or smart card belonged to the owner of electronic signature. This private key is used to create digital signature when a customer sends data to the bank.

Digital signature is an electronic signature produced from the private key of a person and can be used to verify the identity of that person by having that person's public key authenticated. The certificate authority that keeps that person's public key will be responsible for sending the public key to a counter party that demands authentication and issuing digital certificate to attest that the public key belongs to that person.

The service system that uses PKI as an authentication technique should conduct the followings:

- Examination of received digital certificate before granting access to execute a transaction, such as cross-checking with up-to-date certificate revocation list

- Ensuring security of the work system and computer that accommodate authentication by PKI technology

- Provision of operational logs of the work system and computer that accommodate authentication by PKI technology

3. Token/smart card

This authentication technique uses an object belonged to a customer like a card with embedded chip (smart card) together with password or biometrics of the customer. This technique is more secure than the one that relies solely on password in the authentication.

The service system that uses token/smart card as an authentication technique should conduct the followings:

- Arrange for secure production and delivery of token/smart card

- Determine suitable usage life, replacement method, and termination method

- Suspend service to user whose failed login attempts exceed designated quota.

- Establish guidelines and agreement for usage of token/smart card and inform customers how to use token/smart card securely.

4. Biometrics

This authentication technique relies on customer's unique features such as voice and fingerprint as well as hand, eyeball, and facial features and so forth. Such unique features are stored for comparison purpose and customer's authentication before granting execution of a transaction.

The service system that uses biometrics as an authentication technique should conduct the followings:

- Arrange for secure procedures for recording of customer's biometrics.

- Arrange for encryption of in-transit biometrics and proper storage of biometrics.

- Suspend service to user whose failed login attempts exceed designated quota.

Appendix 2 of Attachment 5

Advice for E-banking Customers

Commercial banks should disseminate useful advice to customers to create better awareness so that customers recognize the importance of security while using the service. Such advice should include

1) Customer should not disclose own PIN and password to other person, not write or note password where it is highly visible, destroy PIN and password notification document, and be wary of scam or fraud that deceive customers to disclose PIN and password.

2) Advice customer on how to designate a secure password, frequent change of password, and channels where customer can promptly report any problem related to PIN and password.

3) Advice customer to verify bank's website address before starting to execute a transaction in order to avoid exposure to deceitful website.

4) Advice customer to check the accuracy of transactional details such as amount, transaction date, account number, and outstanding balance on regular basis in order to avoid potential irregularities in the transactional execution.

5) Advice customer on how to keep his/her own computer secured, for example:

- Install and use reliable anti-virus software that regularly updates virus information and also virus filtering software via internet.
- Control access to personal data.
- Log in and out the service system properly.
- Do not leave the computer or hardware while executing a transaction and log out the service system properly after completion of a transaction.
- Use computer and hardware that are compatible with the bank’s security system.
- Avoid using sub-standard computer and hardware or hardware that comes from unreliable sources.

- Avoid using public computer to perform e-banking transaction.
- Avoid accessing to suspicious website.
- Avoid disclosure of PIN, banking information, or credit card information to any unknown or unreliable website.
- Avoid opening unknown or suspicious emails (junk email).
- Avoid downloading or using software from unknown sources or sources where existence cannot be verified because customer's system may receive virus software or other attached software that allows intruder to gain unauthorized access.

6) Ensuring that customer understands the scope of responsibilities on the part of the bank and customer.

Attachment 6

Guidelines for Development of IT Contingency Plan

Commercial banks utilize IT system in service provision, supported with network links with internal network and those of other domestic and international entities. Therefore, if there was occurrence of an incident that causes any disruption or damage to IT system, whether it be natural disaster, accident, or malicious intent against banking system, such as fire, flood, sabotage, and computer virus, banking businesses would be affected immediately and customer service would be disrupted, causing widespread impacts on other entities interlinked with the network. Accordingly, if a bank does not have suitable procedures to deal with such occurrence, customers, end users, and stakeholders may lose confidence in the bank itself and the banking system as a whole.

The procedure that deals with such woeful incident is critical and it must be used when banks face such problem. If banks were well prepared, impacts would be mitigated, thus ensuring that its IT system would be restored within a reasonable period of time and the confidence of customers and stakeholders on the business and banking services would be maintained. It is imperative that banks have an efficient IT contingency plan that can be implemented when facing with a real harmful incident. Thus, the aim is to maintain business and service continuity or at least something close to the status quo.

Contents

1. In these guidelines,

"Management committee" is referred to a bank's committee or executive body incumbent on relevant responsibilities (in case of foreign bank branch).

2. Principles

2.1 In the development of IT contingency plan, commercial bank shall consider its feasibility, ensuring that IT contingency plan can be applied in a real harmful incident. IT contingency plan shall be viewed as a normal part of business operation and must be in accord with the guidelines of the Bank of Thailand Re: Business Continuity

Management (BCM) and Development of Business Continuity Plan (BCP). Furthermore, it is required that the bank hold emergency response drill at both operational and organizational levels at least once a year to assure that the contingency plan can be used effectively in real situation. Where operating systems are linked with external network or services are provided by external entities, the bank and external entities should jointly exercise such drill.

2.2 In the development of IT contingency plan, commercial bank should consider pertinent elements so that the plan's format can be tailor-made to suit the complexity of business operations, such as security system and internal control system, type and level of potential risks faced by the bank, customers, and stakeholders as well as overall banking and money market systems.

2.3 Commercial bank shall consider management of potential risks stemming from various harmful incidents. Beside general types of risk like operational risk and reputation risk, the bank should also consider other pertinent risks, including

2.3.1 System risk: For example, disruption at one bank may cause disruption to banking and money market systems as a whole.

2.3.2 Independency risk: For example, telecommunication or IT services provided by other service providers. If such service provider could not serve the bank, banking operations might be disrupted.

2.3.3 Concentration risk of critical operating systems or resources: For example, where clustering of telecommunication or utility system is located nearby bank office, if any damage occurred, these systems might suffer from losses at the same time. Another example is clustering of external service providers whereby many banks are served by the same service provider.

2.4 Where commercial bank resorts to IT outsourcing to support banking operations, its management committee shall arrange appraisal of the efficiency of IT contingency planning procedure to ensure that IT contingency plan conforms to IT contingency planning policy as formulated by the bank. IT outsourcing shall adhere to the Notification of the Bank of Thailand Re: IT Outsourcing.

3. The essence of these guidelines include

3.1 Roles and responsibilities of management committee

3.2 Policy and guidelines for development of IT contingency plan

3.3 Main processes in development IT contingency plan

3.3.1 Business impact analysis

3.3.2 Risk analysis and control

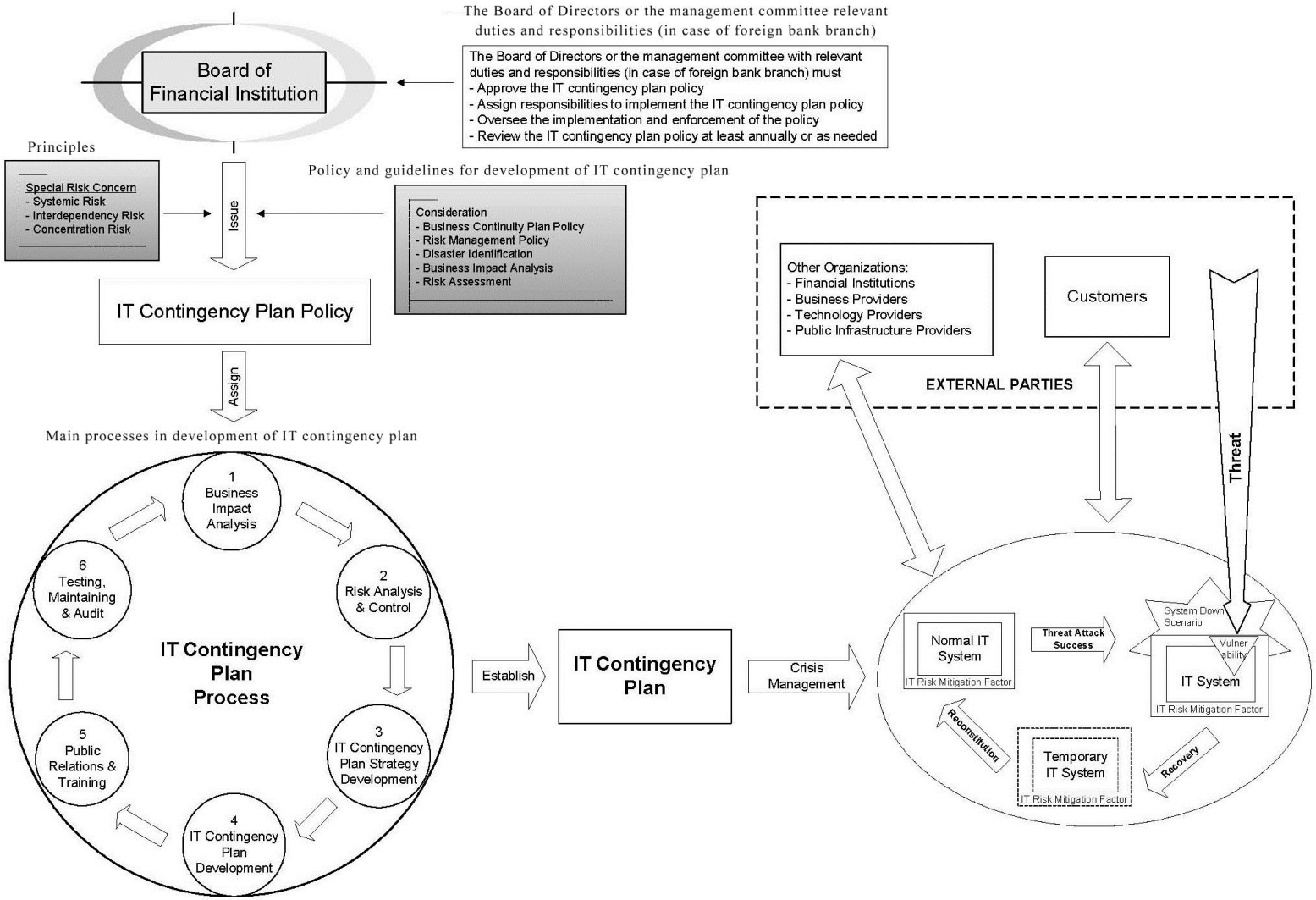
3.3.3 IT contingency plan and strategic development

3.3.4 IT contingency plan development

3.3.5 Public relations and training

3.3.6 Testing, improvement, and verification

To readily comprehend the contents, overall contents of the guidelines are summed up in the diagram in the following page.



BOT Notification No 26-2551 (6 September 2017)-check

4. Detailed guidelines

4.1 Roles and responsibilities of the management committee

The management committee is incumbent on the followings:

4.1.1 Establish policy and guidelines for development of a written IT contingency plan. The management committee may designate IT committee, risk management committee, or an executive body to establish such policy and guidelines and have them presented to the management committee for approval.

4.1.2 Appoint a working group that is responsible for development of IT contingency plan in accordance with prescribed policy and guidelines. After the working group finishes drafting IT contingency plan, a contingency plan shall be proposed to the management committee for review and approval before its implementation.

4.1.3 Ensure that staff and concerned parties properly implement IT contingency plan in both simulated incident and real harmful incident.

4.1.4 Arrange evaluation of the effectiveness of the policy and guidelines in the development of IT contingency plan at least once a year. Whenever there is any change that impacts on the contingency plan, such as changes in business strategy, overall risk management policy, business environment, or key IT resources, the management committee shall promptly arrange evaluation of the effectiveness of such policy and guidelines.

4.2 Policy and guidelines in the development of IT contingency plan

4.2.1 The management committee shall prescribe the policy and guidelines for the development of IT contingency plan by considering the conformity with business continuity plan policy and risk management policy as well as business complexities, rapidly changing technological advancement, banking environment, and organizational roles in the stabilization of banking and money market systems.

4.2.2 In the development of IT contingency plan, the management committee should consider the followings:

(1) Disaster identification: Identify potential harmful incidents that impact on IT system utilized in banking operations.

(2) Business impact analysis: Analyze impacts on IT-dependent businesses in case of system disruption.

(3) Risk assessment and risk management: Assess and manage potential risks stemming from harmful incident as well as determine acceptable risk level and maximum allowable disruption time in business operations and IT resources system in each operating system.

For instance, details in the policy and guidelines for the development of IT contingency plan may include overall objectives, outline of the plan, scope of the plan, plan development steps and time frame, and designation of those responsible for plan development as well as roles and responsibilities, identification of potential harmful incident, determination of acceptable risk level, risk management criteria, emergency response approaches, public relations approaches, and so forth.

4.2.3 Policy and guidelines for development of IT contingency plan should encompass four key aspects of planning process as follows:

(1) Disaster preparedness: The aim is to prevent and reduce potential occurrence of harmful incident that impacts on banking operations and services, for example, determination of risk prevention measures and ensuring that employees understand their roles and responsibilities.

(2) Emergency response: The aim is to control and limit the extent of damage and potential impacts on the bank, customers, concerned parties, and overall banking system, for example, determination of measures for control and rectification of emergency situation.

(3) Business continuity: Ensuring that the business can continue to operate, such as critical data and equipment backup, system and data recovery, and arrangement of the opening of backup center and staff transfer whenever disaster struck.

(4) Business restoration: Ensuring that banking business and services return to normalcy quickly, for example, determination of business restoration approaches, stipulation of control procedures for installation, configuration setting, and testing of recovered or substituted IT resources, and determination of damage assessment techniques.

4.2.4 Commercial bank shall appoint a distinctive working group to develop IT contingency plan. Working group members should be nominated from relevant IT and business departments and each department's responsibilities should be

defined explicitly and appropriately. Accordingly, executives of each relevant department should take part in the development of IT contingency plan.

4.3 Principal procedures of the development of IT contingency plan

Commercial bank shall establish a process for the development of efficient IT contingency plan whereby such contingency plan can be practically implemented in real situation, thus ensuring that the bank can continue to operate IT-dependent businesses. The principal procedures of the development of IT contingency plan include

4.3.1 Business impact analysis: Commercial bank shall assess and analyze business impacts in order to learn about the relationship between business operations and IT system and business impacts stemming from disruption of the IT system. Consequently, the bank can effectively prioritize business operations and IT resources expended in recovery efforts. The approaches are as follows:

(1) Analyze and identify business operations that are dependent on internal and external IT systems, vulnerable areas which are prone to system failure, financial and non-financial impacts from disruption, and allowable maximum disruption time in business operation.

(2) Prioritize business operation that requires system recovery and stipulate timing for system recovery and the goals of operating systems and data that should be recovered following any disruption.

(3) Stipulate the level of business continuity in each business operation. For instance, deposit/withdrawal services at bank branches should be assigned with a high level of business continuity. Thus, these services should be able to operate continuously during business hours.

(4) Analyze and identify internal and external IT resources required for business operations identified in 3.3.1 (1) as well as potential impacts following disruption of IT resources and allowable maximum disruption time of IT resources.

(5) Prioritize IT resources identified in 3.3.1 (4) that are required for system recovery, stipulate recovery timing, the goals of operating systems and data that should be recovered following any disruption, and minimum IT resources required for system recovery.

4.3.2 Risk analysis and control: Commercial bank shall identify factors that may induce risks and impacts on IT system on which business operations must dependent and improve control procedures to mitigate or avert potential impacts. The control procedures are as follows:

(1) Assess risks that may disrupt IT resources utilized in business operations by identifying incidents that might cause disruption, internal and external causes or sources of threat, vulnerable areas, severity and possibility of business disruption and acceptable risk level.

(2) Analyze risk control procedures and improve the procedures and resources required for controlling risks that might cause disruption as well as conducting assessment and control of such procedures.

4.3.3 Strategic development of IT contingency plan

Commercial bank shall formulate a strategy for development of IT contingency plan that is suitable with disruptive incident and its business environment and resources. Accordingly, the plan will encompass identified risks and business impacts. Such strategy should conform to the bank's business continuity plan. When strategic options of IT contingency plan are determined, commercial bank should consider the followings:

(1) Achievement of stipulated goals, such as system recovery timing, goals of operating systems and data that should be recovered following any disruption, and minimum IT resources required for system recovery.

(2) Key factors that influence selection of strategic options so that the bank can have a clear direction on the development of IT contingency plan that will achieve stipulated goals, such as managing critical information, acquiring backup technology, roles and responsibilities of operating staff. (Appendix 1 of Attachment 6: Examples of influential factors in the selection of strategic options of IT contingency plan)

(3) Allocate adequate budget for each strategy and ensure that the budget is sufficient for all required activities. Moreover, the bank may conduct cost and benefit analysis for each alternative for comparison and deliberation on suitable strategies.

Examples of strategic formulation, for instance, in the selection of alternative system recovery approaches, one IT system may present two

alternatives, that is, implementation of system recovery by procuring backup equipment or migrating IT operations to backup IT system.

4.3.4 Development of IT Contingency plan

IT contingency plan should have explicit form and content so that actions can be taken quickly and easily and should have flexibility when dealing with potential situation. In detail, IT contingency plan should include the following key elements: (Appendix 2 of Attachment 6): Examples of the structure of IT contingency plan)

(1) Operational support data

Operational support data helps ease understanding, implementation, and improvement of IT contingency plan. Such support data should include the title of the plan, objectives, scope, relationship with other operational plans, details of IT system, organizational chart showing line of command under the contingency plan, assignment of staff on duty and their responsibilities, and standby person in case assigned person is unable to perform duties as well as record of plan revision.

(2) Emergency response

Commercial bank should have emergency response procedures as follows:

(2.1) Detection of incident that may cause disruption or disaster and prompt notification to concerned groups or personnel

(2.2) Prompt and accurate assessment of the magnitude and aspects of the damage that impacts on the system and notification of the assessment to system recovery group or concerned personnel

(2.3) Stipulation of precise command and decision-making procedures, deliberation on the setup of command center, designation of an individual or a group of individuals responsible for directing and decision-making as well as approaches and criteria for initial system recovery based on consideration of various factors such as magnitude of damage on IT system, personnel safety, IT system's criticality to banking operations.

(3) Implementation of system recovery

Commercial bank should consider procedures that can operate IT system temporarily, repair damages on the existing system, in-situ restoration

or relocation to a new site. System recovery procedures should have the following aspects:

(3.1) Stipulation of explicit operational steps for system recovery and attention on communication and coordination within a group and between various operating groups. In addition, the bank should have a system or documentation of operational details and any consequential mistake or problem following failure of system recovery, for example, checklist of actions taken. The aim is to control that the operation follows required steps. Subsequently, operating results and defined targets can be compared and evaluated, thus resulting in further improvement of the efficiency of IT contingency plan.

(3.2) Have detailed steps for system recovery operation that conform to system recovery priorities identified by business impact analysis and defined recovery timing.

(3.3) Have alternative steps for system recovery operation in case the operation cannot follow the steps of the stipulated plan. For instance, while system recovery of one operating system was being carried out, the server of that operating system could not function normally because some server equipment malfunctioned. In such case, the bank should prepare an alternative operation, for example, replacing defective equipment or server. However, the bank should consider an alternative that is not dependent on IT system but also have to establish prevention procedures to avert potential risks.

(3.4) While implementing system recovery, the bank should be careful not to skip or neglect required steps and avoid introducing new procedures, unless additional steps are approved by authoritative person.

(4) Business restoration

Commercial bank should consider procedures that attest system operability after the system is restored. Such operation may require existing or new IT resources, for example, control procedures for installation, configuration setting, testing of recovered or substituted IT resources or procedures for migration from backup IT system to the main IT system.

(5) Documentation of planned implementation

Commercial bank shall arrange documentation of planned implementation of IT contingency plan and store these documents at a secure

location which is not affected by disruptive incident. At least one copy of the documents should be kept at the authoritative person and another copy should be kept at the backup location, thus allowing relevant personnel to access to and use documents for planned implementation.

4.3.5 Public relations and training

(1) Public relations

Commercial bank shall arrange public relations program for IT contingency plan by stipulating explicit public relations activities and action steps so that all concerned staff are aware of the details regarding plan development, plan implementation steps, concerned staff, and any change.

Aside from that, the bank shall stipulate public relations activities and action steps in dealing with emergency situation in order to convince customers that banking services can continue without any disruption, such as publicizing how to communicate to the bank in case normal communication channel fails or inform customers when services will resume after disruptive incident.

(2) Training

Commercial bank shall organize training for concerned employees that are involved in plan implementation at least once a year. Training topics should at least cover objectives of the plan, action steps, coordination and communication among different groups, reporting procedures, security system, internal procedures of each operating group, and individual responsibility. The employees that attend the training course should understand and be able to implement the plan even without plan implementation documents.

4.3.6 Testing, improvement, and review

(1) Plan testing

Commercial bank shall regularly conduct testing of the plan at operational and organizational levels at least once a year or whenever the plan is revised, especially operating systems that impact on service provision of the whole banking system in the event of disruption, such as deposit system and interbank fund transfer and payment systems. If such operating systems are linked to external network or served by external entities, the bank should jointly test the contingency plan with concerned external entities. In system testing, the bank should exercise caution to avoid

repercussions on normal banking operations and maintain record of test results for comparison with defined targets. Furthermore, test results will be reported to the management committee so that they will be used as criteria for evaluation of test results and improvement of the efficiency of IT contingency plan.

The details of system testing that are stipulated in IT contingency plan of each operating system by the bank include test objectives, scope of the test, test scenarios, test duration and steps, required resources, and evaluation criteria. Moreover, considerations should also encompass actual operations and specified scenarios. In system testing, the bank may conduct partial or full testing. However, it is suggested that the bank conduct a full test at least once a year. In each test, only a single scenario may be chosen.

(2) Improvement

The bank shall clearly define action plan, guidelines, and duration of the review and improvement of IT contingency plan, thus ensuring that IT contingency plan is practical and in accord with technological development, current situation, and the bank's policy and strategies. Accordingly, the bank should arrange plan review and improvement at least once a year or whenever there is any change that impacts on the contingency plan, such as transfer of staff responsible for plan implementation and changes in IT system environment. Moreover, the bank should also consider updating information and documents distributed to staff or external entities in accordance with such improvement.

(3) Review

The bank should arrange a review of IT contingency plan to validate procedures for plan development, thus ensuring viability of the plan. Moreover, reviewer may be chosen from external or internal entities within the organization but must be able to work independently.

Appendix 1 of Attachment 6

Examples of influential factors in the selection of strategic options of IT contingency plan

1. Management of critical data

Commercial bank should develop critical data management procedure to attest their existence, integrity, security, and accessibility. When there is occurrence of a disruptive incident, the bank should have the following procedures:

1. Identify data or groups of data that are critical to banking operations such as financial transactions of each customer and the bank's asset management data as well as information required for installation of operating systems. Aside from that, the bank should also take into account critical data of each operating unit or bank staff stored in personal computer which may not be backed up properly.

2. Regarding data backup and retrieval, the bank should stipulate precise and suitable methods that are commensurate with assigned criticality of information. Aside from that, the bank should also determine frequency of data backup and external storage sites as well as conduct testing to confirm readiness and suitability of the facilities.

3. Regarding the setup of external backup sources, the bank should consider pertinent factors such as location and environment, security protocol, accessibility, and stored data.

2. Provision of backup IT system

Commercial bank shall procure backup IT system that can be used as a substitute for the main IT system in case of harmful incident in order to maintain business and service continuity. The backup IT system may be a backup site and/or backup IT system for certain portion of the system, such as data, applications, computer, and network equipment. Key considerations include

1. Main and backup IT systems should be located quite far from each other and should not share same utility sources. Moreover, risk distribution principles should be adopted to avert widespread disruption.

2. Backup IT system must be overseen or tested to ensure that it can process data in accordance with planned system recovery procedures and guidelines.

Moreover, data backup methods, frequency, and type of data must be stipulated to commensurate with necessity, priority, and impact on operating system in case of harmful incident.

3. Backup IT system should be available and readily accessible at all time or should at least be able to substitute the main IT system in case of disruption. In addition, the backup IT system should have security system that conforms to the bank's security policy and can deal with potential harmful incident with long-term consequences.

Examples of backup IT system include

- Active/backup model is an IT system configuration whereby a main computer system serves the operation and another system works as a backup system. The backup system will start operating whenever the main computer system cannot function normally or encounters disruption. The backup system is installed with computer hardware compatible with the main computer system. In most cases, the backup system can operate for many hours. Moreover, the backup system may be served by external entities.

- Split operation model or active/active model is an IT system configuration that maintains more than two separate IT system sites. Each site operates interdependently as backup system and each site is capable of taking over some part or the whole operation of another site for a certain period of time. When a disruption occurs at one site, another site will restore the operation promptly or almost instantly. However, this model may have a rather high maintenance cost because maintenance and improvement must be carried out at several main IT system sites.

When determining backup IT system configurations, the bank should review the suitability in terms of size, complexity, and the bank’s operations as well as potential risks, risk management approaches, and the bank’s operating cost.

Appendix 2 of Attachment 6

Examples of the structure of IT contingency plan

Examples of the structure of IT contingency plan are presented so that commercial bank can use these examples as guidelines for plan implementation whereby the examples may be applied in accordance with the bank's policy and guidelines on development of IT contingency plan and risk management policy, business continuity policy, and other relevant policies. Moreover, the bank should also consider modifications that are suitable with the current situation.

Generally, examples of the structure of IT contingency plan should encompass the followings:

Operational support data: To ease understanding, implementation, and improvement of the plan:

1. Title of contingency plan: Specify title of the plan

2. Objectives of contingency plan development: Identify plan objectives; potential risk-based impacts on the bank, customers, and other relevant external entities; and expected outcome resulted from plan implementation.

3. Scope of contingency plan: Identify scope of operating system, detailed operating procedures, and part of operating system where the plan will be enforced as well as detailed work flow.

4. Details of IT system: Identify title and structure of IT system, security system, and communication system.

5. Designation of authoritative person: Identify persons empowered to make decision and put the plan into action (authoritative and responsible persons), roles and duties, and scope of responsibilities as well as designation of a person who will take over the responsibilities in the event the first authoritative person is unable to perform his/her duties.

6. Alternative site: Identify an alternative site that can take over the operation of the main site in the event of a sabotage that may incapacitate the main site.

7. Record of changes: Indicate preparation and revision date and names of those who prepare, revise, and review the plan. Additionally, a short description of revision should be stated.

Action plan: The elaboration of scenarios, conditions for the implementation of action plan, relevant details and steps, required resources, and detailed scope and limitation encompasses four areas of planning as follows:

1. Pre-incident preparedness: Stipulate prevention and risk control procedures to prevent and reduce opportunities for occurrence of harmful incident.

2. Emergency response: To control and limit the scope of damage and other repercussions in the event of harmful incident. The emergency response procedure include

a) Conditions for plan implementation: Determine or identify conditions or situations.

b) Identify basic action steps: Preliminary assessment of the situation, location, cause, and scope of damage; specify actions that put an end to harmful incident; relevant operational approaches; approaches for data and document storage; staff safety and evacuation; and required IT resources.

c) Determine communication action plan: Stipulate methods of communication to operating units or other relevant persons, both internal and external, to inform them of the situation and operational approaches or contingency contact site; develop directories of various units or those responsible for assistance; and cease internal and external damages arising from the incident.

d) Identify resource requirements: Clearly specify the needs for resources, number of personnel, location, equipment and tools, and telecommunication and public utility systems

3. Business continuity plan: This is an action plan mentioned in Clause 2 that ensures the continuity of IT system which supports banking business or the recovery of IT system within stipulated period of time without other persistent impacts. Details are as follows:

a) Conditions for plan implementation: Determine or identify conditions or situations.

b) Identify basic action steps: Identify steps, priorities, and timing of system recovery. Specify operational methods and how to start backup data system to ensure uninterrupted operation.

c) Determine communication action plan: Stipulate communication methods and coordination with operating units or other relevant persons, both internal and external, to keep them informed of the facts and operational approaches or temporary site.

d) Identify resource requirements: Clearly identify resource needs in case the recovery might take a long time, the number of personnel, backup site, equipment and tools, and telecommunication and public utility systems

4. Resumption of the operation: To restore operating systems and put them in order again as well as assess damages and future preventive approaches. Details are as follows:

a) Identify action steps: Specify operational methods to restore the situation; control procedures for installation, configuration setting, and testing of recovered or substituted system. Also, submit damage report to the superior.

b) Identify relevant persons: Prepare directories of operating units or persons, both internal and external that are responsible for lending assistance to restore the situation.

Public relations and training: Designate public relations steps and schemes that deal with bank staff and customers. Hold training for operating units and relevant staff so that all concerned parties are aware of the objectives, operating procedures, coordination, communication between different groups, reporting procedures, security system, and own duties and responsibilities in accordance with the contingency plan.

Testing, improvement, and review of the contingency plan

1. Testing

a) Determine testing period: Specify coherent testing frequency and duration of testing from the beginning until the end of testing procedure

b) Identify tested scenarios and relevant details: When describing scenario details, objectives, scope of operating system, or operating procedures relating to the whole test of contingency plan as well as detailed steps of the test should be elaborated.

c) Resources required for testing of the plan: Designate persons responsible for controlling, coordination, and management of testing of the contingency plan, including site, equipment and tools, and budget.

d) Evaluation criteria: Designate persons responsible for evaluation, defining evaluation criteria that may differ depending on the aspects of operating systems, operating procedures, and the objectives of each test.

2. Plan improvement and review

a) Duration of the review: Clearly stipulate action plan, approaches, duration of the review and improvement, ensuring that the plan is most up-to-date and suitable with current situation.

b) Designate person responsible for the review: Designate reviewer to attest applicability of various procedures for the development of IT contingency plan.

Additional information

Other details that should be included in IT contingency plan are as follows:

1. Names, addresses, and phone numbers of bank staff responsible for plan implementation

2. Names of operating units, locations, and phone numbers of concerned external entities

3. Checklist

4. Required report formats

Attachment 7

Minimum data standards of operating systems of commercial bank that uses computer data processing

---

To standardize data storage of commercial bank that uses computer for data processing purposes in order to accommodate reference needs of the bank itself and facilitate supervision of the Bank of Thailand, it deems advisable by the Bank of Thailand to prescribe minimum data standards of operating systems of commercial bank that uses computer data processing. To this end, at least the bank must record and store data in accordance with these standards within the scope and details of data used in operating systems. Data record may be in a form of report or other forms of recording medium which facilitate speedy data retrieval. Moreover, storage duration of such reports and recording media must conform to the necessity and integrity as prescribed under the accounting laws.

Scope

The Bank of Thailand considers establishing minimum data standards for five operating systems as follows:

1. Deposit and overdraft system - Call deposit and overdraft, saving deposit, and term deposit

2. Credit system - Loan, draft, etc.

3. Foreign business system - Foreign exchange system (spot or forward contract), money market system (lending or investment in money market), lending and obligations pertaining to imported and exported goods (opening letter of credit, cashing out bill of exchange, export loan, export guarantee)

4. Matching transaction and future obligation systems – Bill for collection, endorsement, bank aval, guarantee, etc.

5. Accounting system

Detailed information about various operating systems

The customer data that all operating systems should have are described under the first topic and specific information of each operating system is described under the following topics:

1. Customer information in all operating systems

ID number/ account number

Name

Address

Type of customer (in case of deposit or overdraft, customer type is indicated as required in Thor.Phor. report, Table 31; in case of foreign business, customer type is indicated as required in relevant Thor.Phor. report)

Type of business (for credit granting, business type is indicated as required in Thor.Phor. report, Table 33)

Details of credit line, future obligations, and credit line for forward contract

- Type of credit line, future obligation, credit line for forward contract
- Credit line (baht)
- Date credit line is first granted
- Due date
- Interest/ discount rate
- Type of collateral
- Appraised value of collateral (if deposit is put up as collateral, indicate account number and amount)
- Collateral appraisal date
- Credit line for mortgage/ pledge/ guarantee

Credit rating (bad debt/ doubtful debt/ below standard)

2. Deposit and overdraft systems

Account number

Type of account (saving deposit, call deposit, term deposit; these may be summed under an account number)

Account status (movement, no movement, frozen)

Account opening date

ATM/ POS/ credit card password

Cheque number of cheque paid to customer

Currency (foreign currency)

Account balance (available for withdrawal)

Frozen amount

Account freezing reason

Frozen amount due to cheque deposit for collection

Frozen amount due to collection of cheque deposit on the previous business day

Interest rate

Accrued interest receivable/ payable

Date of the last interest calculation

Date of the last account movement

Date of the last overdraft

Details of account balance of term deposit

- Date of transaction that effects interest calculation
- Sequence of deposit transaction/ deposit slip of customer account
- Amount
- Duration of deposit
- Interest rate

Details of account movement

- Date of transaction

- Date of transaction that effects interest calculation
- Description/ type of transaction
- Cheque number (in case of cheque collection from call deposit and cheque withdrawal)
- Previous outstanding balance
- Amount of deposit/ withdrawal
- Carried-over outstanding balance
- Branch where transaction takes place
- Code of staff who executes transaction
- Code of staff who approves transaction

3. Credit system

Contract/bill number

Loan date/ bill issuance date/ bill discount date

Loan objective

Due date/ discount period

Payment term (number of installations and payment in each installation)

Bill issuer

Bill/ bill amount

Outstanding balance (accrual)

Interest/ discount rate

Accrued interest

Date of the last interest calculation

Details of movement

- Date of transaction
- Date of transaction that effects interest calculation
- Description/ type of transaction
- Previous outstanding balance
- Transaction amount
- Carried-over outstanding balance

Details of movement

- Date of transaction
- Date of transaction that effects interest calculation
- Description/ type of transaction
- Previous outstanding balance
- Transaction amount
- Carried-over outstanding balance

4. Foreign business system

4.1 Foreign exchange system

Name and code of financial institution or client

Document reference number

Transaction date

Remittance date

Transaction type

Traded currency

Traded amount

Exchange rate

Conversion to baht

Relevant deposit account number opened in foreign bank

Receipt/ remittance fee (option, collar)

4.2 Money market system

Name and code of financial institution

Document reference number

Transaction type (loan or investment)

Transaction date/ posting date

Maturity date/or loan or investment period

Currency code

Bill

Exchange rate

Conversion to baht

Interest rate

Accrued interest receivable/payable or prepaid interest receipt/expense

Relevant deposit account number opened in foreign bank

Lending/ investment objective

4.3 Credit and future obligations relating to imported and exported goods system

Name and account number of client

Document reference number

Transaction date

Document date (draft, L/C etc.)

Due date of document (draft, L/C etc.)

Currency code

Amount

Exchange rate

Interest/ discount rate

Accrued debt and each type of obligation

Deposit for L/C opening

Accrued interest receivable/payable

Name of partner bank

Name of recipient bank/remittance bank of partner bank

Relevant deposit account number that is opened in a foreign bank

5. Matching transactions and other future obligation system

Draft number/ contract number/ document number

Name of bank that endorses/ guarantees/ issues bank aval/ etc.

Holder of a right stipulated in endorsement/ guarantee/ aval contract among others

Type of obligation

Contractual date

Maturity date

Account transfer date (only bill for collection)

Amount

Deposit payment for endorsement/ guarantee/ bank aval etc.

Fee

6. Accounting system

Account number

Account name

Transaction date

Description of transaction/ relevant document number

Previous outstanding balance

Transaction amount (debit/ credit)

Carried-over outstanding balance

Attachment 8

Prevention of fraud with skimmer to steal customer data from automated teller machine (ATM) so as to make a fake card

---

The aim is to raise awareness among commercial banks offering automated teller machine (ATM) services about fraud issues so that they will be more wary of service delivery and develop safeguard measures to prevent potential frauds, thus ensuring the security of ATM services for customers, reducing adverse impacts and business damages, and maintaining customer confidence in e-banking services.

Contents

1. Fraud issues

ATM-related frauds have been growing in number and the severity of the problem seems to be on the rise because this type of fraud can be done easily by using low-cost devices and preying on customer's naivety. Such fraud incurs not only financial losses to customers and banks but also erodes customer confidence in ATM services.

A widely popular fraud scheme is the use of a small data recording device or skimmer that stores data in magnetic strip. Such device is installed at the card inlet of ATM machine before customer executes a transaction. After a customer inserts a card, the data recording device will record customer data stored in the card's magnetic strip, enabling the swindler to use recorded data to make a fake card. To steal password, normally the swindler will glance at the password behind the customer's back while the customer is entering the password. The swindler may ask for help from customer or lend assistance in order to persuade customer to demonstrate how to use ATM. When the customer demonstrates and keys in his/her password, the swindler will take note and memorize the password so he/she will be able to use it with a fake card. Subsequently, the swindler can transfer or withdraw money from the customer's account via ATM.

Beside the above unscrupulous scheme, there are also other schemes, for example, installing a small camera on ATM to sneak a look at customer's password, using a fake keyboard that can record while customer is entering the password, and tampering with ATM or network system linked with ATMs.

2. Preventive measures

2.1 Be more wary

Commercial bank should be more wary of the problems and reinforce security measures for the provision of banking services through ATMs by considering risk level and areas where ATMs are located. The security measures should encompass the followings:

2.1.1 Assign personnel to inspect ATMs regularly, especially ATMs located in fraud-prone area in order to prevent tampering or installation of swindling device on ATM.

2.1.2 Establish continuous monitoring procedure of functional performance of ATMs and network system. With such information, the bank can quickly find out about unusual transactions and swindling opportunities.

2.1.3 Consider installing closed-circuit televisions at ATMs, especially in fraud-prone area. Such CCTVs will help the bank realize any problem and irregularity quickly and can record fraud incident that may be used as evidence in prosecution against swindler.

2.1.4 Develop problem-solving procedure, designate a team of specially trained personnel to quickly deal with problem analysis and resolve the problem. Also, report such incident to management.

2.1.5 Maintain transaction logs and store such logs securely so they can be used as evidence in examination.

2.1.6 Constantly monitor technological advancement relating to ATM and various cards used in e-banking transaction as well as the latest fraud schemes so that security measures can be upgraded appropriately and effective technology for fraud prevention can be selected.

2.2 Customer advice

Commercial bank should provide customers useful information and advice either in writing or via notification so that customers can safely use banking services via ATMs, thereby reducing potential losses to customers and the bank. Customer advice should include

2.2.1 Keep ATM card and password securely; do not reveal password to other person; do not write password on ATM card whatsoever; do not expose password while writing or not keeping password in disclosed place. The best way is that customer should memorize password.

2.2.2 Advise customer in high-risk target group to change password immediately after receiving a new ATM card, destroy password notification document, and change password regularly at least every three months.

2.2.3 Use different passwords for various types of banking service, for example, ATM password should not be the same as that of tele-banking.

2.2.4 Be careful not to reveal password to other person while entering the password at ATM. Customer should not lend assistance or get help from stranger, especially in situation where stranger can observe while customer is entering password.

2.2.5 Examine ATM before performing a transaction to see if there is an unusual device installed on ATM, especially at the card inlet. If any irregularity is found and there is any doubt, customer should avoid using the service there and promptly inform the bank that owns the ATM. Commercial bank may consider affixing a sign prominently to show standard procedure and usage instruction as well as advice or warning to suggest customers to observe irregularities before performing a transaction.

2.2.6 Advise customer to check account balance regularly. If any unusual transaction is found, the bank must be notified immediately to probe the matter and avert a greater loss.

2.2.7 Advise customer to keep transaction slips so they can be used as evidence.

2.3 Complaint handling procedure

Commercial bank should provide a channel for complaint handling and inform customers of the existence of such channel. The bank should at least post a contact phone number on ATMs and clearly display a contact phone number on the back of ATM card. Accordingly, customers can notify the bank owning ATMs or the issuing bank of ATM card when ATM card is seized or lost or irregular transaction is observed.

2.4 Bank responsibilities

When commercial bank offers deposit and withdrawal services and other types of service to general customers through its ATMs, it is duty of the bank to ensure that general customers be protected from any loss incurred by a third party or swindler. Hence, in the course of service delivery through ATMs and investigation of relevant error, the bank shall adhere to the Notification Re: Guidelines for Electronic Fund Transfer (Annex 4). In case of illegitimate electronic fund transfer and flawed service delivery where customer is not at fault, the bank shall be liable for any damage suffered by the customer. In addition, based on good governance principles, if customer followed normal procedure and lost some money to a swindling third party that used skimmer installed on ATM and stole data stored in magnetic strip or subsequently committed other deceitful act that caused damage to customer, the bank shall be liable for incurred loss to that customer.

2.5 Other non-ATM cards

Since such deceitful method may be used to commit fraud by using other types of card that store data in magnetic strip, such as credit and debit cards, the bank should implement the above safeguard measures with other types of electronic fund transfer services that are prone to similar deceitful act.

Attachment 9

Guidelines for prevention of an internet fraud called phishing

To raise awareness of potential fraud issues among commercial banks and to be more wary of security in service provision as well as to develop preventive measures and to keep customers abreast of potential frauds, to ensure security in service delivery to customers, to mitigate business impacts and losses, and to maintain customer confidence in banking services.

Contents

"Phishing" is an attack in a form of fake email address (email spoofing) and fabrication of a fake website to lure victims or email recipients to reveal banking or personal data, such as credit card number, username, password, citizen ID number, or other personal data.

1. Fraud issues

Presently, fraud issues relating to phishing scheme are widespread in many countries and begin to spread among e-mail users in Thailand. Such incident seems to be on the rise because this scam can be done easily and often preys on customer's gullibility, resulting in financial losses of customers and banks and affecting customer confidence in e-banking services.

Reportedly, present fraud schemes include sending deceitful e-mail to customer and pretending to be e-mail sent from bank by using credible heading and message, for example, requesting customer to confirm banking data so as to comply with security measure that oversees customer accounts; or notifying that customer data need to be updated; or notifying that customer account is being temporarily frozen and requesting customer to confirm personal data so customer can continue to perform banking transaction. At the same time, a link to fake website (hyperlink) of the bank may be included by stealing or illegally copying the bank's mark, symbol, or other aspects of a well-known bank. Moreover, a questionnaire may be attached to fake e-mail and customer may be asked to fill out personal data such as credit card number, saving

account number, username, and password. After customer filled out personal data in fake website or questionnaire, the swindler can use such data in many illegitimate ways, such as transferring money; or making payment to a third party via internet banking, tele-banking, mobile banking; or making online purchase of goods and services with credit card.

2. Preventive measures

2.1 Be more wary

Banks should be more watchful and develop security measures as follows:

2.1.1 If the bank sends email to customers, it must not provide hyperlink to its website or questionnaire that requires customer's personal data.

2.1.2 Risk analysis procedure must be implemented to review high-risk services and implement prevention measures to avert potential risks. For instance, the bank offers fund transfer service that transfers money from customer account to a third party via internet network and such service does not require customers to notify the bank in writing before using the service. The bank should stipulate a suitable maximum transfer amount or consider using two-factor authentication[1] for high-risk service via the internet.

2.1.3 Provision of monitoring procedure to regularly monitor transactions performed by customers through various electronic media. This procedure will enable banks to quickly learn about irregular transactions and fraud opportunities.

2.1.4 Keeping abreast of technological advancement pertaining to service provision and the latest fraud techniques via internet network[2] and other electronic media so that the information can be exploited to improve security measure and select effective technology to prevent fraud.

---

[1] This authentication technique provides greater security for internet-based services. It comprises two-stage authentication, including

1. Username and password
2. Using additional tool to supplement authentication, such as using token to create new password every time the user accesses to the service, or using private key stored in smart card or other tools owned by customers.

[2] Learn more information from

- Thai Computer Emergency Response Team (ThaiCERT) http://www.thaicert.nectec.or.th
- U.S. Anti-Phishing Working Group http://www.antiphishing.org

2.1.5 Send warning to customers about unscrupulous conduct via phishing by showing warning statement on website's home page and sending notification letter to customers. Moreover, banks should also have procedure to inform new customers.

2.1.6 Developing problem-solving procedure by designating a team of responsible staff trained to analyze and resolve problems quickly. Also, reporting procedure must be developed to keep the management informed of the situation.

2.2 Customer advice

Commercial bank should provide useful information and advice to customers in writing and ensure that customers are informed so that customers can use e-banking services securely, thus reducing opportunities for damage to customers and the bank. Customer advice should include

2.2.1 Informing customers that the bank does not have the following service policies:

(1) Sending e-mail to customers with hyperlink to bank website.

(2) Inquiring personal and financial data, such as username, password, and credit card number, via e-mail and other channels like telephone and letter.

2.2.2 Advise customers to type website address (URL) by themselves when accessing to the bank's internet network. Never use hyperlink in e-mail to link to the website.

2.2.3 Advise customers to review accuracy of transactional details, such as amount, transaction date, and account number, and check account balance regularly to prevent abnormal transaction.

2.2.4 Advise customers not to submit personal data or key banking data to e-mail with suspicious message, pretending it is sent from the bank. Also advise customers to report such incident to the bank immediately.

3. Complaint handling procedure

Banks should provide channels for complaint handling and inform customers of the existence of such channel. Banks should at least provide a contact phone number where customers can contact in case abnormal incident or transactions are observed. Banks should organize training for staff dealing with complaint handling and ensure that they have adequate knowledge to advise customers how to use e-banking services properly and securely.

Attachment 10

Electronic Transaction Act B.E. 2544 (2001)

Electronic Transaction Act

B.E. 2544

BHUMIBOL ADULYADEJ, REX.

Conferred on the 2nd day of December 2001
During the 56th year of the present reign

His Majesty King Bhumibol Adulyadej graciously decrees to proclaim that

Whereas it is expedient to establish a law governing electronic transaction, this Act contains some provisions concerning restriction on individual rights and liberty whereby Section 29, an adjunct to Section 50 of the Constitution of the Kingdom of Thailand, prescribes that people are conferred such rights by virtue of the statutory provision.

Hence, His Majesty assents to the enactment of this act under advice and consent of the parliament as follows:

SECTION 1: This Act shall be referred to as "Electronic Transaction Act B.E.2544."

SECTION 2: This Act shall come into force within 120 days after its publication date in the Government Gazette.

SECTION 3: This Act shall be enforced upon civil and commercial transactions conducted with electronic data, except transactions that the Royal Decree precludes the enforcement of this Act, in whole or in part.

The substance under Paragraph 1 shall not have any repercussion on any law or regulation prescribed for consumer protection.

This Act shall be enforced on transactions involved in state conducts as stipulated under Chapter 4.

SECTION 4: In this Act,

“Transaction” is referred to any undertaking pertaining to civil and commercial activities or state conducts as stipulated under Chapter. 4.

“Electronic” is referred to applications of electronic, electrical, electro-magnetic wave, or any other similar techniques. Such application encompasses optical or magnetic means or devices that are involved in such application.

“Electronic transaction" is referred to transaction that is carried out with electronic means, in whole or in part.

“Content” is referred to an account or a fact, whether it be alphabet, numeric, sound, or visual form or any other form that conveys meaning by itself or any means.

“Electronic data” is referred to content that is created, transmitted, received, stored, or processed with electronic means, such as electronic data exchange, electronic mail, telegram, teletype, or facsimile.

“Electronic signature” is referred to alphabets, characters, numeric, voice, or any symbols in an electronic form that is used to supplement electronic data to validate relationship between individual and electronic data. The aim is to identify certain individual as the owner of electronic signature that is related to such electronic data and to confirm that such individual accepts the content in such electronic data.

“Data system” is referred to data processing performed by electronic device so as to create, transmit, receive, store, or process electronic data.

“Electronic data exchange” is referred to transmission or receipt of contents with electronic means between computers based on pre-determined standards.

“Data sender” is referred to a person who sends or creates electronic data before saving such data for further delivery with a method determined by that person. In this regard, such person may send or create electronic data by himself/herself or send or create electronic data for himself/herself or on behalf of somebody else. However, this does not include intermediary of such electronic data.

“Data receiver” is referred to a person to whom electronic data are sent by a sender and intended for and who receives such electronic data. However, this does not include intermediary of such electronic data.

“Intermediary” is referred to a person that sends, receives, or store specific electronic data as well as performs other services pertaining to such electronic data on behalf of others.

“Certificate” is referred to electronic data or any other records which validate connection between signature owner and data used in the creation of electronic signature.

“Signature owner” is referred to a person who owns data used in the creation of electronic signature and creates such electronic signature for himself/herself or on behalf of other person.

“Related party” is referred to a party that may pursue any action relating to electronic certificate or signature.

“State agency” is referred to ministry, bureau, department, government office under other title that has the stature of department, regional administration, local administration, and state enterprise established under an act or a Royal Decree. In addition, it is also referred to juristic person, a group of persons, or individual empowered to perform any state conduct.

“Committee” is referred to an electronic transaction committee.

“Minister” is referred to an acting minister pursuant to this Act.

SECTION 5: The provisions under Section 13-24 and Section 26-31 may be agreed in some other ways.

SECTION 6: The prime minister shall act to serve this Act.

Chapter 1
Electronic transaction

SECTION 7: Do not refuse obligations and statutory enforcement of any content only because that content is in a form of electronic data.

SECTION 8: Under the provision of Section 9, where the law prescribes that any conduct be done in written form, supported with documentary evidence or has document that may be shown, if such content is created in a form of electronic data that can be accessed and retrieved without having discrepancy of the meaning, it shall be deemed such content is prepared in written form or supported with documentary evidence, or has document that may be shown.

SECTION 9: Where a person signs a document, it shall be deemed electronic data is signed if

(1) A method is used whereby signature owner can be identified and it can be demonstrated that signature owner attests that the content in electronic data belongs to him/her; and

(2) Such method is a reliable one that befits the aim of creation or delivery of electronic data, considering circumstantial conduct or agreement between contractual parties.

SECTION 10: Where the law requires presentation or storage of any content in original condition as an original copy, if data presentation or storage is in a form of electronic data and meets the following criteria, it shall be deemed presentation and storage of original document is executed as required by the law:

(1) Electronic data resort to a reliable method to preserve the integrity of such content after the creation of such content was finished; and

(2) Such content may be shown later.

Regarding the integrity of the content according to (1), considerations shall be given to completeness and the fact that the content has not be modified, except additional endorsement or note or any change that may occur in the normal course of communication, storage, or where presentation of the content does not have any bearing on the integrity of the content.

When scrutinizing the reliability of the method used to preserve the content's integrity according to (1), all relevant circumstances and objectives pertaining to the creation of such content must be considered.

SECTION 11: Do not refuse to accept electronic data as evidence in legal proceeding only because they are electronic data.

When weighing evidences to determine whether or how much electronic data are trustworthy, considerations shall be given to the reliability of the way or the method used in creation, storage, or communication of electronic data; storage features or means, completeness and integrity of the content; and the way or the method used to identify or demonstrate who data sender is as well as all relevant circumstances.

SECTION 12: Under the provision of Section 10, where the law prescribes storage of document or content, if any document or content is stored in a form of electronic data according to the following criteria, it shall be deemed the document or content is stored as required by the law:

(1) Such electronic data can be accessed and retrieved without having meaning altered;

(2) Such electronic data are stored in the same format as when they are created, transmitted, or received; or stored in a form that can correctly display the created, transmitted, or received content; and

(3) Storage of the contents that indicate source, upstream, and downstream of electronic data as well as its delivery and receipt date and time.

The substance under Paragraph 1 shall not be applicable to the content that only serves delivery and receipt of electronic data.

State agencies responsible for storage of any document or data may stipulate detailed guidelines relating to storage of such document or data as long as they do not contradict or are inconsistent with the provision under this Section.

SECTION 13: Proposal or response in an agreement may be in a form of electronic data. Do not refuse statutory enforcement of an agreement only because proposal or response in the agreement is in a form of electronic data.

SECTION 14: Between data sender and receiver, state of intent or remark may be expressed in a form of electronic data.

SECTION 15: Where data are sent by any method, it shall be deemed electronic data belong to the person who sends the data.

Between data sender and receiver, it shall be deemed electronic data belong to data sender if electronic data are sent by

(1) An authorized person designated to deal with electronic data on behalf of the sender; or

(2) A data system programmed by data sender or authorized person to operate automatically on pre-determined conditions.

SECTION 16: Data receiver may consider that electronic data belong to data sender and proceed accordingly if

(1) Data receiver reasonably examines the data and observes that electronic data belong to data sender by using the method agreed with data sender;

(2) Electronic data received by data receiver are created by an action of a person who uses a method used by data sender to demonstrate that such electronic data belong to data sender. Accordingly, the person knows that from the relationship between that person and data sender or authorized person.

The substance under Paragraph 1 shall not be applied if

(1) At that time data receiver is informed by data sender that electronic data received by data receiver are not data transmitted by data sender, and at the same time, data receiver has enough time to examine facts as informed; or

(2) According to Paragraph 2, when data receiver knows or should know that electronic data do not belong to data sender, if data receiver exercises reasonable caution or follows the agreed method.

SECTION 17: According to Section 15 and Section 16, Paragraph 1, between data sender and data receiver, data receiver has the right to consider that received electronic data are accurate in accordance with the intent of data sender and shall proceed accordingly, unless data receiver knows or should know that received electronic data have some discrepancy caused by transmission, provided that data receiver exercises reasonable caution or follows the agreed method.

SECTION 18: Data receiver may duly consider that each set of received electronic data are disparate data and may proceed based on the information in each set of electronic data, unless that set of electronic data is a duplicate of another set and data receiver knows or should know that electronic data are duplicates, if data receiver exercises reasonable caution or follows the agreed method.

SECTION 19: Where acknowledgment of the receipt of electronic data is required, whether data sender previously requested or agreed with data receiver or the request is notified when electronic data are being transmitted or shown in electronic data, the following criteria shall be applied:

(1) Where data sender does not agree on the acknowledgment of the receipt of electronic data with any specific format or method, receipt confirmation may be done via communication from data receiver, whether it be done with automatic data system or other method or any action undertaken by data receiver, in order to adequately inform data sender that data receiver already received such electronic data.

(2) Where data sender stipulates conditions that transmission of electronic data shall be recognized only when data sender receives acknowledgment from data receiver, it shall be deemed electronic data have not been delivered until data sender received a reply message.

(3) Where data sender does not stipulate conditions as in (2) and data sender does not receive acknowledgment within stipulated or agreed or sufficient period of time in the event time constraint is not stipulated or agreed.

(a) Data sender may send a message to inform data receiver, stating he/she still does not receive receipt acknowledgment, and stipulate a reasonable time period allowed for data receiver’s acknowledgment; and

(b) If data sender does not receive acknowledgment within the stipulated period as stated in (a), when data sender informs data receiver, data sender shall consider electronic data have not been sent or data sender may exercise other rights that he/she may have.

SECTION 20: Where data sender receives acknowledgment from data receiver, it shall be assumed that data receiver already received relevant electronic data. However, such presumption does not mean electronic data received by data receiver are accurate, compared to electronic data sent by data sender.

SECTION 21: In acknowledgment of the receipt of electronic data, where it appears that electronic data received by data receiver conform to technical specification as agreed by data sender and receiver or stipulated in applicable standards, it shall be assumed that transmitted electronic data conform to technical specifications entirely.

SECTION 22: Regarding transmission of electronic data, it shall be deemed electronic data have been transmitted once electronic data entered into the data system that is not under control of data sender.

SECTION 23: Regarding receipt of electronic data, it shall be deemed electronic data have been received when electronic data entered into the data system of data receiver.

Where data receiver specifies information intended to be received in electronic data, it shall be deemed electronic data have been received after such electronic data entered into the data system as required by data receiver. However, if such electronic data was sent to other unspecified data system of data receiver, it shall be deemed electronic data have been received after electronic data were viewed from that data system.

The substance in this Section shall be applied even though data system of data receiver is located in another location which is separate from the location where data receiver receives electronic data pursuant to Section 24.

SECTION 24: It shall be deemed transmission or receipt of electronic data takes place at the office of data sender or data receiver, whatever the case may be.

Where data sender or receiver has several offices, the office where data sender or receiver is mostly involved in respect to such transaction shall be considered the office used for the benefits as stated in Paragraph 1. However, if it cannot be defined which office data sender or receiver is mostly involved in respect to such transaction, head office shall be considered the place where such electronic data are received or sent.

Where the office of data sender or data receiver is not known, normal resident shall be considered the place where such electronic data are received or sent.

The substance in this Section is not applicable to delivery and receipt of electronic data via telegram and teletype or other communication methods as stipulated in the Royal Decree.

SECTION 25: It shall be assumed that any electronic transaction executed with a secure method as stipulated in the Royal Decree is deemed a reliable method.

Chapter 2
Electronic signature

SECTION 26: Electronic signature that meets the following criteria shall be considered a trustworthy electronic signature.

(1) Under application circumstance, information used in the creation of electronic signature is linked to signature owner, without any connection to other person.

(2) While electronic signature is being created, information used in the creation of electronic signature is under control of signature owner, without any control by other person.

(3) Any change in electronic signature from the time of its creation can be examined.

(4) Where the law stipulates that electronic signature certifies completeness and integrity of the content. Any change to the message can be examined from the time electronic signature is applied.

The provision under Paragraph 1 does not constitute limitation that there is no other method to demonstrate whether electronic signature is trustworthy or there is no other evidence concerning trustworthiness of electronic signature.

SECTION 27: Where information is used in creation of electronic signature that is legally binding, signature owner shall take the following actions:

(1) Exercise reasonable caution to prevent unauthorized usage of the information in creation of electronic signature.

(2) Inform without delay the person who is believed, on reasonable ground, to perform any act that depends on electronic signature or provide service relating to electronic signature when:

(a) Signature owner knows or should know that information required for the creation of electronic signature is lost, ruined, tampered, disclosed illegitimately, or known, not in accord with the objectives.

(b) Based on known circumstance, signature owner is aware that the circumstance poses a high risk, indicating that information required for creation of electronic signature is lost, ruined, tampered, disclosed illegitimately, or known, not in accord with the objectives.

(3) Where a certificate is issued to supplement electronic signature, reasonable caution shall be exercised to ensure correctness and completeness of all substances which are performed by signature owner throughout the effective period of the certificate or pursuant to prescription in the certificate.

SECTION 28: Where a service provider issues a certificate to supplement electronic signature, the certificate shall be legally binding as if the signature is written. The service provider that issues the certificate shall perform the followings:

(1) Adhere to its policies and guidelines that have been declared.

(2) Exercise reasonable caution to ensure correctness and completeness of all substances which are performed by the service provider throughout the effective period of the certificate or pursuant to prescription in the certificate.

(3) Provide reasonable access methods to allow concerned counterparties to examine the facts of all substances shown in the certificate, including

(a) Indication of the service provider that issues the certificate;

(b) Signature owner indicated in the certificate exercises control of the usage of information used in creation of electronic signature when the certificate is issued;

(c) Information used in creation of electronic signature is effective during or before issuance of the certificate.

(4) Provide reasonable access methods to concerned counterparties so that they can examine the followings in the certificate or by other means.

(a) Method used to identify signature owner;

(b) Limitations relating to objectives and values of the utilization of information in creation of electronic signature or certificate.

(c) Information used in creation of electronic signature is valid and is not lost, ruined, amended, disclosed illegitimately or known, not in accord with the objectives;

(d) Limitations on the scope of liabilities as indicated by the service provider that issues the certificate;

(e) Having methods where signature owner can send notification when there are incidents pursuant to Section 27 (2);

(f) Providing service for timely revocation of the certificate.

(5) Where services under (4) (e) are provided, notification methods shall be provided to signature owner who can notify pursuant to the criteria under Section 27 (2). Also, where service under (4) (f) is provided, such service must be able to revoke the certificate in timely manner.

(6) Deploy reliable system, method, personnel in service provision.

SECTION 29: When considering the reliability of system, method, and personnel pursuant to Section 28 (6), the following aspects shall be considered:

(1) Financial standing, personnel, and existing assets;

(2) Quality of hardware and software;

(3) Issuance method of certificate, certificate application, and storage of service data;

(4) Disclose information concerning signature owner indicated in the certificate and persons expected to be counterparties;

(5) Frequency and scope of the audit which shall be conducted by independent auditor;

(6) Certifying body or service provider that issues the certificate relating to the practices or the existence of the elements under (1) to (5);

(7) Any other cases which may be stipulated by the committee.

SECTION 30: Relevant counterparties shall perform the followings:

(1) Reasonably examine trustworthiness of electronic signature;

(2) Where electronic signature has a certificate, the following actions shall be duly performed:

(a) Check for completeness, suspension, and revocation of the certificate;

(b) Adhere to any limitation pertaining to the certificate.

SECTION 31: The certificate or electronic signature is deemed legally binding without having to consider:

(1) Place where the certificate was issued or place where electronic signature was created or used; or

(2) Office of certificate issuer or owner of electronic signature.

Certificate issued in other country shall be legally binding pursuant to local laws similar to certificate issued in the country, provided that the issuance of such certificate utilizes a reliable system that is not less reliable than the stipulation under this Act.

Electronic signature created or used in other country shall be legally binding pursuant to local laws, similar to electronic signature created or used in the country, provided that creation or usage of such electronic signature utilizes a reliable system that is not less reliable than the stipulation under this Act.

When determining which certificate or electronic signature is reliable according to Paragraph 2 and 3, international standards and other relevant factors shall be considered.

Chapter 3
Service business relating to electronic transaction

SECTION 32: An individual has the right to operate service business relating to electronic transaction only for undertakings that preserve financial and commercial securities, or for the benefits in enhancing credibility and acceptance of electronic data system, or for safeguarding against damages on general public. Hence, enacted Royal Decree shall stipulate which service business relating to electronic transaction is required to notify the authority before obtaining business registration or required to obtain operating license beforehand.

Accordingly, when stipulating which case must be notified, registered, or obtain license beforehand according to Paragraph 1, prevention of damages in accordance with the level of severity of potential impacts on such business operation shall be considered where appropriate.

In this regard, a state agency may be designated as a supervisory body under the Royal Decree.

Before proposing enactment of the Royal Decree according to Paragraph 1, public hearing shall be organized where appropriate and deliberation should be based on the findings of such public hearing.

SECTION 33: Where the Royal Decree stipulates which service business relating to electronic transaction is the business that must notify the authority or obtain registration, the person who intends to operate such business shall notify or have the

business registered with the official stipulated under the Royal Decree prior to business start-up.

The guidelines and methods used for notification or registration according to Paragraph 1 shall comply with the provisions of the Royal Decree. When the official performing duties under the mandate of the Royal Decree is notified or receives the filing of registration application, receipt of notification or registration shall be issued as evidence on the notification or registration filing date. Then, the notifier or registrant shall be allowed to operate such business from the notification or registration filing date. However, if the official performing duties under the mandate of the Royal Decree later finds that notification or registration filing is incorrect or incomplete, he/she is authorized to instruct the notifer or registrant to make correction or make it complete within seven days from the issuance date of such instruction.

In the course of business operation, the notifer or registrant under Paragraph 1 shall comply with the guidelines prescribed in the Royal Decree and in accordance with the stipulation of the committee.

If the notifer or registrant under Paragraph 1 does not make correction or make the notification or registration complete as stipulated in Paragraph 2 or commits a breach or fails to comply with the business operation guidelines according to Paragraph 3, the committee shall deliberate over punishment and impose administrative fine not exceeding one million baht by judging on severity of the offence. Where appropriate, the committee may order that person to take necessary action to make such correction or suitable amendment.

The criteria for deliberation on administrative fine shall comply with the stipulation of the committee. If the offender who is ordered to pay administrative fine refuses to pay such fine, statutory enforcement of administrative punishment governing public administration practices shall be applied mutatis mutandis. Moreover, if there is no official to oversee the execution of the order, the committee shall be authorized to file charge at an administrative court to execute the payment of the fine. In this regard, if the administrative court discerns that the imposition of the fine is legitimate, the court is authorized to pass a judgment and execute confiscation or freezing of properties that will be sold in the market to raise fund for fine payment.

In the event the offender under Paragraph 4 does not make correction pursuant to the committee's order or commits the same offence again, the committee shall be authorized to issue an order to bar that person from engaging in such notified or registered business.

SECTION34: Where the Royal Decree stipulates that business operation relating to electronic transaction is considered a business that requires an operating license, any person intending to operate such business shall file a license application with the official stipulated under the Royal Decree.

Qualifications of the applicant, criteria and filing of license application, issuance of the license, and renewal and return of the license as well as suspension or revocation of the license shall adhere to the guidelines stipulated under the Royal Decree.

In the course of business operation, the licensee under Paragraph 1 shall comply with the guidelines prescribed in the Royal Decree, the committee's notification, or the license's conditions.

Where the licensee commits a breach or fails to comply with the guidelines of business operations relating to electronic transaction pursuant to Paragraph 3, the committee shall deliberate over punishment to impose administrative fine not exceeding two million baht by judging on the severity of such offence. Where appropriate, the committee may order that person to undertake any action to make correction or make suitable modification. In this regard, the substance under Section 33, Paragraph 5 shall be applied mutatis mutandis.

If the offender under Paragraph 4 fails to make correction in accordance with the committee's order or commits the same offence again, the committee shall be authorized to issue an order to revoke the license.

Chapter 4
Electronic transaction in the state sector

SECTION 35: If application, approval, registration, administrative order, payment, and any notification or legal undertaking imposed on state agency or by state agency is executed in a form of electronic data pursuant to the guidelines and methods prescribed by the Royal Decree, the Royal Decree shall be enforced and legally binding, similar to any undertaking pursuant to the guidelines and methods prescribed under relevant laws. However, the Royal Decree may mandate that concerned person take certain action or refrain from any action or that state agency issue regulation to stipulate minor details in some cases.

When enacting the Royal Decree under Paragraph 1, the Royal Decree may stipulate that operator of service business relating to electronic transaction notify the authority, obtain registration, or acquire the license, whatever the case may be, before

business start-up. In this case, the provision under Chapter 3 and relevant penal provision shall be applied mutatis mutandis.

Chapter 5
Electronic transaction committee

SECTION 36: An electronic transaction committee shall be established and chaired by the minister of the Ministry of Science, Technology, and Environment and comprise 12 cabinet-appointed committee members that shall be selected from a group of qualified persons through nomination process. Among them, two qualified persons must be keen in each of the following disciplines:

(1) Finance

(2) E-commerce

(3) Law

(4) Computer technology

(5) Science or engineering

(6) Social sciences

Each qualified person from each discipline shall come from the private sector. Moreover, the director of the National Electronics and Computer Technology Center, the Office of the National Science and Technology Development Agency shall also be appointed as committee member and secretary.

The criteria and nomination method and appointment of suitable persons by the cabinet to form a committee under Paragraph 1 shall comply with the regulation as prescribed by the minister.

The secretary can appoint no more than two assistant secretaries.

SECTION 37: The electronic transaction committee is incumbent on the following duties:

(1) Recommend the cabinet on policies to promote and develop electronic transaction as well as resolution on problems and pertinent obstacles.

(2) Monitor the conduct of business operation relating to electronic transaction.

(3) Offer advice or consultation to the minister on enactment of the Royal Decree under this Act.

(4) Issue regulation or notification governing electronic signature pursuant to this Act or Royal Decree under this Act.

(5) Pursue actions in compliance with this Act or other laws.

To pursue actions pursuant to this Act, the committee shall be designated as the official as stipulated under the Criminal Code.

SECTION 38: Competent committee member shall have three-year tenure. Committee member who vacates the office may be re-appointed, but he/she may not hold the office for two consecutive terms.

SECTION 39: Apart from the vacation of the office upon the expiry of his/her term pursuant to Section 38, competent committee member shall vacate the office upon

(1) Death;

(2) Resignation;

(3) The cabinet relieves committee member of the duties because misconduct, deficiency, dishonesty, or inefficiency;

(4) Being incompetent or quasi-incompetent;

(5) Being imprisoned by a final judgment, except punishment for negligence or misdemeanor.

SECTION 40: Where competent committee member vacates the office pursuant to Section 39, it shall be deemed the committee comprises the remaining number of members and the committee shall proceed with the appointment of a new committee member within 60 days from the date the committee member vacates the office.

In this regard, the new committee member who takes over the vacated office shall serve the remaining term of the substituted member.

SECTION 41: At committee meeting, no less than half of the total number of committee members shall constitute a quorum.

If the chairman does not attend meeting or is unable to perform duties, the committee shall select a committee member to act as a chairman.

Resolution of the committee shall be decided with a majority of vote. Each member has one vote. In case of a tie, the chairman shall cast an extra vote as a deciding vote.

SECTION 42: The committee shall be authorized to appoint sub-committee to deliberate or perform any task as assigned by the committee.

The substance under Section 41 shall be applied to meeting of sub-committee mutatis mutandis.

SECTION 43: The National Electronics and Computer Technology Center, the Office of National Science and Technology Agency shall be responsible for the administrative functions of the committee.

Chapter 6
Penal provision

SECTION 44: Any person who operates service business relating to electronic transaction and fails to notify or register the business with the official as stipulated under the Royal Decree pursuant to Section 33, Paragraph 1; or violates the business operation restriction order of the committee pursuant to Section 33, Paragraph 6 shall be punished with imprisonment for a term not exceeding one year or a fine not exceeding 100,000 baht or both.

SECTION 45: Any person who operates service business relating to electronic transaction without an operating license pursuant to Section 34 shall be punished with imprisonment for a term not exceeding two year or a fine not exceeding 200,000 baht or both.

SECTION 46: Regarding offence pursuant to this Act which is committed by a juristic person, manager, representative of the juristic person, or any person participating in business operation of the juristic person shall be punished likewise, unless it is proven that he/she is unaware or does not collude in such offence.

Countersigned by
Pol.Lt.Col. Thaksin Shinawatra
Prime Minister

Note:- The reason for the promulgation of this Act is as follows: Presently, when transactions are executed, there is a trend towards the adoption of communication modes which depend on development of electronic technologies which are convenient, speedy, and efficient. However, since such electronic transactions are vastly different from traditional transactions which are under the realm of the existing laws. Consequently, it is necessary to recognize the legal status of electronic data similar to the

treatment of document or documentary evidence. In the course of acceptance of delivery and receipt modes of electronic data, usage of electronic signature, and acceptance of electronic data as admissible evidence so as to promote electronic transaction's trustworthiness and statutory enforcement, it is expedient to establish an electronic transaction committee that is mandated to formulate policies that stipulate guidelines on promotion of electronic transaction, monitoring of business operation relating to electronic transaction. Moreover, the committee is also incumbent on promotion of technological development to keep pace with dynamic technological advancement and constant development of potential technological capacity in order to establish credible standards. Furthermore, the committee is also designated to offer advice on how to resolve issues and overcome pertinent obstacles. To promote domestic and international electronic transactions, it is thereby expedient to promulgate an exclusive law that conforms to acceptable international standards and to enact this Act.