Unofficial translation

BANK INDONESIA REGULATION

NUMBER: 9/ 15 /PBI/2007

CONCERNING

IMPLEMENTATION OF RISK MANAGEMENT IN THE USE OF INFORMATION TECHNOLOGY BY COMMERCIAL BANKS

BY THE GRACE OF GOD ALMIGHTY

GOVERNOR OF BANK INDONESIA,

Considering

a. whereas the development of Information Technology enables Banks to make use of said technology to increase the efficiency of operational and the quality of the Bank's service to its customers;

b. whereas the use of Information Technology in a Bank's operational could also increase the risk towards the Bank;

c. whereas with the increase of the risks involved, Banks should implement effective risk management;

d. whereas Information Technology is a valuable asset for Banks and therefore its management should not only be the responsibility of Information Technology organizing working units but also all parties who partake in its use;

e. whereas the fact that for the implementation of *Basel II*, an adequate infrastructure of Information Technology is needed;

f. whereas in relation to considerations as mentioned in letter a, letter b, letter c, letter d, and letter e, regulations which control the implementation of risk management in the use of Information Technology by commercial banks is required as part of the Regulation of Bank Indonesia.

In view of

1. Act Number 7 year of 1992 regarding Banking (State Gazette year of 1992 Number 31; Additional State Gazette Number 3472) as amended with Act Number 10 year of 1998 (State gazette year of 1998 Number 182; Additional State Gazette Number 3790);

2. Act Number 23 year of 1999 regarding Bank Indonesia as amended with Act Number 3 year of 2004 (State

Gazette year of 1999 Number 66; Additional State Gazette Number 3843);

3. Act of Bank Indonesia Number 5/8/PBI/2003 regarding the Implementation of Risk Management for Commercial Banks (State Gazette year of 2003 Number 56; Additional State Gazette Number 4292);

HAS DECREED

To enact: THE REGULATION OF BANK INDONESIA REGARDING THE IMPLEMENTATION OF RISK MANAGEMENT IN THE USE OF INFORMATION TECHNOLOGY BY COMMERCIAL BANKS

CHAPTER I

GENERAL PROVISIONS

Article 1

In this Regulation of Bank Indonesia the following terms are used:

1. "Bank" is a Commercial Bank as mentioned in Act Number 7 year of 1992 regarding Banking as amended through Act Number 10 year of 1998, including branch offices of foreign banks.

2. "Information Technology" is technology related to computers, telecommunication and other electronic devices which are used in organizing monetary data and/or banking services.

3. "Banking Services delivered through Electronic means" or what will subsequently be referred to as Electronic Banking is a service which enables a Bank's customers to gain information, communicate, and carry out banking transactions by electronic means, amongst others by ATM, phone banking, electronic fund transfer, internet banking, mobile phone.

4. "Information Technology Strategic Plan" is a document which illustrates the visions and missions of the Bank's Information Technology, strategies that support said visions and missions, and the main principles that that form the guidelines for the use of Information Technology to fulfill business necessities and support long-term strategic planning.

5. "Data Centers" are the main facility of the Bank's data processing which consists of hardware and software to support the Bank's continual operational venture.

6. "Database" is a cluster of comprehensive data that is arranged systematically, and can be accessed by users according to their authorization, and is controlled by a database administrator.

7. "Disaster Recovery …..

7. “Disaster Recovery Centers (DRC)” are a reserve facilities for when a Data Center suffers problems or can not function because due to the computer room being cut off of its electricity supply, fire, explosion or damage to the computers, and is used temporarily during the recovery of the Bank Data Center to ensure business continuity.

8. “Business Continuity Plans (BCP)” are a policies and procedures which contain a series of planned and coordinated actions regarding steps to reduce risks, the handling of the effects of problems/disasters and recovery processes to ensure that the Bank’s operational venture and service to customers can still proceed.

9. “Technology-based Transaction Processing” are actions in the form of additions, alterations, deletions, and/or authorizations of data which are applied to the application system used to process transactions.

10. Board of Commissioner:

    a. to a Bank in the form of a limited holding, is the board of commissioner as mentioned in Article 1 number 6 Act Number 40 year of 2007 regarding limited holding.

    b. to a Bank in the form of a local company, is an observer as mentioned in Article 19 Act Number 5 year of 1962 regarding local companies.

    c. to a Bank in the form of a cooperative, is an observer as mentioned in Article 38 Act Number 25 year of 1992 regarding cooperatives.

    d. to a branch office of a foreign bank is an official selected by the head office of the foreign bank to act as an observer.

11. Board of Director:

    a. to a Bank in the form of a limited holding, are directors as mentioned in Article 1 number 5 Act Number 40 year of 2007 regarding limited holding.

    b. to a Bank in the form of a local company, are directors as mentioned in Article 11 Act Number 5 year of 1962 regarding local companies.

    c. to a Bank in the form of a cooperative, are managers as mentioned in Article 29 Act Number 25 year of 1992 regarding cooperatives.

    d. to a branch office of a foreign bank is the chief of the branch office of the foreign bank.

CHAPTER II

SCOPE OF INFORMATION TECHNOLOGY

RISK MANAGEMENT

Article 2

(1) Banks must implement effective risk management in the use of Information Technology.

(2) Implementation of risk management as mentioned in paragraph (1) must at least include:

a. active supervision by the board of Commissioner~~s~~ and Director~~s~~;

b. sufficient policies and procedures on the use of Information Technology;

c. sufficient processes of identification, measurement, monitoring and risk control on the use of Information Technology;

d. internal control systems for the use of Information Technology;

(3) Implementation of risk management must become an integral part during every stage of Information Technology use, from the process of planning, construction, development, operation, maintenance, up to the discontinuation and the disposal of Information Technology resources.

Article 3

The implementation of risk management in the use of Information Technology by Banks as mentioned in Article 2 must be in accordance with the goal, policies, size and complexity of the Bank's business.

CHAPTER III

IMPLEMENTATION OF RISK MANAGEMENT IN THE USE OF

INFORMATION TECHNOLOGY

First Section

Active supervision by the board of Commissioner~~s~~ and Directors

Article 4 …..

Article 4

Banks must determine exact levels of authorization and obligation for each position related to the use of Information Technology.

Article 5

Authorization and obligations as mentioned in Article 4 for the board of Commissioner at least includes:

a. directing, monitoring and evaluating Information Technology Strategic Plan and the policy of the Bank related to the use of Information Technology.

b. evaluating the directors' accountability on the implementation of risk management in the use of Information Technology.

Article 6

Authorization and obligations as mentioned in Article 4 for Directors at least includes:

a. determining Information Technology Strategic Plan and the Bank's policy related to the use of Information Technology.

b. ensuring that:

1. Information Technology used by the Bank can support business development, the accomplishment of the Bank's goals and the continuation of service to customers;

2. there are efforts to increase the competency of human resources related to the use of Information Technology;

3. the implementation of risk management in the use of Information Technology is done sufficiently and effectively;

4. there are adequate policies and procedures of Information Technology which are communicated and implemented effectively for both the organizing working units and the users of the Information Technology;

5. there exists a system to measure the performance of the carrying-out of Information Technology which at least could:

a) support monitoring of the implementation of strategies;

b) support the completion of project(s);

c) optimize the employment of human resources and investment in infrastructure.

d) increase performance of the carrying-out of Information Technology and the quality value delivery of the results to related users.

Article 7 …..

Article 7

(1) Banks must have an Information Technology Steering Committee.

(2) The Information Technology Steering Committee as mentioned in paragraph (1) is responsible to present recommendations to the Directors which at least is related with:

a. Information Technology Strategic Plan which is in accordance with the Bank's business strategic plan;

b. Conformity of approved Information Technology projects with the Information Technology Strategic Plan;

c. Conformity of the application of Information Technology projects with the project charter;

d. Conformity of Information Technology with the requirements of management information systems and of the Bank's business venture;

e. effectiveness of the steps taken to minimize the risks of the Bank's investment on the Information Technology sector so that such investment contributes to the accomplishment of the goals of the Bank;

f. surveillance on the performance of Information Technology and the efforts to enhance it.

g. efforts to solve problems related to Information Technology, which can not be solved by the either the organizing or user working units, effectively, efficiently and on time.

(3) The Information Technology Steering Committee as mentioned in paragraph (1) has members of at least:

a. A director who oversees the Information Technology working unit;

b. A director who oversees the Risk Management working unit;

c. The highest rank officer who oversees the Information Technology working unit;

d. The highest rank officer who oversees the Information Technology main user working unit.

Second Section

Sufficiency of Policy and Employment Procedures of

Information Technology in Banks

Article 8 .....

Article 8

(1) Banks must possess policies and employment procedures of Information Technology as mentioned in Article 2 paragraph (2) letter b.

(2) Policies and employment procedures of Information Technology includes at least the following aspects:

a. Management;

b. Development and Acquisition;

c. Operational Information Technology;

d. Communication network;

e. Information security;

f. Business Continuity Plan;

g. End user computing;

h. Electronic Banking, and

i. Information Technology service providers.

(3) Banks must determine a limit of tolerable risks to ensure that aspects related to Information Technology as mentioned in paragraph (2) will proceed optimally.

Article 9

(1) Banks must possess an Information Technology Strategic Plan which supports the Bank's business strategic plan.

(2) The Information Technology Strategic Plan as mentioned in paragraph (1) is illustrated in the Bank's Business Plan.

Third Section

The Process of Risk Management Related to

Information Technology

Article 10

(1) Banks must employ risk management processes which include identification, measurement, monitoring and control of risks related to the use of Information Technology.

(2) The process of risk management are employed towards Information Technology related aspects which include at least the development and establishment of Information Technology, Information Technology operations, communication network, information security, Business Continuity Plan, end

user computing, Electronic …..

user computing, Electronic Banking, and Information Technology service providers.

(3) In the event where a Bank utilizes the service of another party to organize Information Technology, the Bank must ensure that the parties involved also implement risk management that is at least in accordance with this Regulation of Bank Indonesia.

Article 11

In carrying out development and acquisition of Information Technology, Banks must employ controlling measures actions to ensure that systems and data are kept confidential and integrated as to support the accomplishment of the Bank's goals, including amongst others:

a. determine and implement procedures and methodologies of the development and acquisition of Information Technology consistently;

b. implement project management in system development;

c. employing sufficient testing during development and acquisition of a system, including tests with user working units, to ensure accuracy and conformity of the system and requirements of related users, as well as the compatibility of one system to another;

d. employing proper documentation of the developed system and its maintenance;

e. to have an application system change management;

Article 12

(1) Banks must identify and survey as well as control the risks of Information Technology operational activities, in communication networks and in end user computing to ensure the effectiveness, efficiency and security of such activities, amongst others by:

a. implementing physical and environmental control on Data Centers and Disaster Recovery Centers;

b. implementing sufficient access control in accordance with determined levels of authorization;

c. implementing control at the time of input, processing, and output of information;

d. evaluating possible risks originating from the Bank's reliance on communication networks;

e. ensuring that design …..

e. ensuring that design and operational aspects in the implementation of communication networks are in accordance with he bank's requirements;

f. employing surveillance of Information Technology operations, including audit trails;

g. employing surveillance on the use of applications developed or organized by working units other than the Information Technology working unit.

(2) Banks with business units based on the principle of sharia, must have a system that is able to provide separate reports for business activities based on the principle of sharia.

Article 13

(1) Banks must ensure that the Business Continuity Plan and Disaster Recovery Plans can be carried out during significant disruptions on the banks Information Technology facilities.

(2) Banks must employ tests on its Business Continuity Plans and Disaster Recovery Plans on every critical system/application and infrastructure in accordance to the result of the Business Impact Analysis, at least once in 1 (one) year involving end user (end to end).

(3) Banks must employ reassessment of its Business Continuity Plan and Disaster Recovery Plan.

Article 14

Banks must ensure effective information security with consideration to at least the following:

a. information security is aimed to effectively and efficiently maintain confidentiality, integrity, and availability, according to regulations;

b. information security is employed on aspects of technology, human resources and processing, in the use of Information Technology;

c. information security includes management of the Bank's assets related to information, human resources policies, physical security, access security, operational security, and other aspects of Information Technology use.

d. Availability of incident handling management for information security; and

e. information security is implemented based on the result of risk assessment on the information in possession of the Bank.

Fourth Section …..

Fourth Section

Control System and Internal Audit over the Carrying-out of Information Technology

Article 15

(1) Banks must implement an effective internal control system on all aspects of Information Technology use.

(2) An internal control system as mentioned in paragraph (1) includes at least:

a. Supervision by management and practice of control;

b. risks identification and assessment;

c. controlling actions and function separation;

d. information systems, accounting systems and communication systems;

e. surveillance and discrepancies correction, which are done by either operational working units, internal audit working units, or other parties.

(3) Information systems, accounting systems and communication systems as mentioned in paragraph (2) letter d has to be supported by technology, human resources and adequate organizational structures.

(4) Monitoring and discrepancies corrections as mentioned in paragraph (2) letter e include at least:

a. constant surveillance;

b. implementation of effective and comprehensive internal audit functions;

c. correction on discrepancies identified by either operational working units, internal audit working units, or other parties.

Article 16

(1) the implementation of internal audit functions of Information Technology as mentioned in Article 15 paragraph (4) letter b considers compliance to regulations.

(2) Due to limitations in the capabilities of a bank's internal Information Technology audit working unit of, the functions of internal audit as mentioned in paragraph (1) may be carried out by an external auditor.

(3) internal auditing must be carried out periodically.

Article 17 …..

Article 17

(1) a bank's internal audit guidelines must include internal audit on the use of Information Technology that is either managed by itself or by Information Technology service providers.

(2) Banks must submit the result of internal audit on Information Technology as part of a report on activities and key results of internal audit as determined in regulations regarding standard implementation of internal audit functions.

(3) Banks must review the internal audit functions on Information Technology use at least once every 3 (three) years.

(4) The review as mentioned in paragraph (3) must utilize an independent external party.

(5) The results of review with additional suggestions for improvement are reported to Bank Indonesia as a part of review report as determined in regulations regarding standard internal audit functions.

CHAPTER IV

THE CARRYING-OUT OF INFORMATION TECHNOLOGY BY INFORMATION TECHNOLOGY SERVICE PROVIDERS

First Section

General

Article 18

(1) Banks can organize its own Information Technology and/or utilize an Information Technology service provider.

(2) Utilizing an Information Technology service provider as mentioned in paragraph (1) is allowed on the condition that the Bank and the Technology service provider abide by the following requirements;

a. for the Bank:

1) the Bank remains responsible for the implementation of risk management;

2) the Bank is capable of carrying out supervision of the Bank's operational provided by the Information Technology service provider;

3) selection of the Information Technology service provider is made based on cost and benefit analysis and involves the Information Technology organizer working unit;

4) the Bank must monitor and evaluate the abilities of the service provider periodically, including its overall performance, reputation, and in the continuous availability of service;

5) the Bank must provide ……

5) the Bank must provide access to data and information for internal, external and Bank Indonesia's auditors when required;

6) the Bank must provide prompt access to its database, either for its latest or past data, to Bank Indonesia;

b. for the Information Technology service provider(s):

1) service providers must implement sufficient Information Technology Control principles, which are verified by audit results carried out by independent parties;

2) service providers must provide access to necessary data and information for the Bank's internal auditor, for external auditors appointed by the Bank, and the auditor of Bank promptly when required;

3) service providers must declare their acceptance to be audited by Bank Indonesia for given services;

4) as an affiliated party, the service provider must guarantee the security of all and every information including the Bank's secrecy and customer's personal information;

5) service providers may sub-contract part of their services only with a written agreement;

6) service providers must report on every critical occurrence with possible consequences of significant monetary loss and/or disturbance to the operational activities of the Bank;

7) service providers must periodically submit the result of Information Technology audit carried out by independent auditors on the carrying-out of Data Centers, Disaster Recovery Centers and/or Technology-based Transaction Processes, to Bank Indonesia through the related Bank;

8) service providers must provide adequate and properly tested Disaster Recovery Plan; and

9) service provider must be willing to accept the possibility of early termination;

(3) the use of Information Technology service providers by the Bank as mentioned in paragraph (1) must be based on a written agreement which contains at least the ability of said Information Technology service provider to render services and or as mentioned in paragraph (2) letter b.

(4) in the event where the Information Technology service provider is a party related to the Bank, the Bank must still conduct selection process and transaction with the service provider prudently according to risk management principles, and based on arm's length principle.

(5) in the event of the following conditions:

a. declining performance …..

a. declining performance in the carrying-out of Information Technology by the Information Technology service provider with possible significant consequences to the Bank's business venture;

b. Information Technology service provider becomes insolvent, or is in the process of liquidation, or is legally declared bankrupt;

c. Violations of the Bank's secrecy and obligation to maintain the confidentiality of the bank's customers personal information, by service providers; and/or

d. there are conditions which causes the Bank to be unable to provide data necessary for supervision by Bank Indonesia;

the Bank involved must employ the following:

a. report to Bank Indonesia within 3 (three) working days from the time of discovery by the Bank of the conditions mentioned above;

b. decide a course of action to solve the problem, including discontinuation of service if necessary;

c. report to Bank Indonesia immediately in case of the discontinuity of the services before the expiration of agreement;

(6) In the event of an employment of service provider or plans to employ a service provider causes or is indicated to cause disturbances on the observation by Bank Indonesia, Bank Indonesia is able to:

a. direct the Bank to discontinue the employment of related Information Technology service provider before the expiration of agreement;

b. reject plans issued by the Bank to employ a service provider;

Second Section

The Carrying-out of Data Centers and/or Disaster Recovery Centers

Article 19

(1) Data Centers and/or Disaster Recovery Centers are managed domestically.

(2) In the event where a Bank will run its Data Centers and/or Disaster Recovery Centers out of Indonesia, the Bank must have prior approval from Bank Indonesia by fulfilling certain requirements.

(3) Approval as mentioned in paragraph (2) will be granted if the Bank fulfils requirements as mentioned in Article 18 paragraphs (2) to (4) as well as the following additional requirements:

a. The Bank submits the results of a country risk analysis;

b. The Bank ensures
…..

b. The Bank ensures that the carrying-out of Data Centers and/or Disaster Recovery Centers out of Indonesia does not decrease the effectiveness of surveillance by Bank Indonesia;

c. The Bank ensures that information concerning the Bank's secrets are only disclosed in accordance to the Indonesian laws;

d. The Bank ensures that the written agreement with a service provider also contains choice of law clauses;

e. If the Bank is a branch office of a foreign bank or is in the ownership of a foreign financial institution, the Bank must submit:

1) Statement by the state's authority on financial audit that the service provider is within its scope of audit.

2) Statement by the state's authority on financial audit permitting Bank Indonesia to perform inspections on the service provider;

3) Statement that the Bank will periodically submit the results of evaluations carried out by the foreign bank office on the implementation of risk management on the service provider(s).

f. Request for approval submitted by the Bank must also contain the following:

1) Benefits to the Bank should exceed the costs paid.

2) The Bank's plans to increase human resources capacity, related to either to the carrying-out of Information Technology, business transactions or products offered.

Third Section

The Carrying-out of Transaction Processes by Service Providers

Article 20

(1) The carrying-out of transaction processes by service providers must be carried out with utmost caution.

(2) The operation of Information Technology-based Transaction Processing done by service providers in Indonesia must be in accordance with the requirements stated in Article 18 paragraph (2) until (4).

(3) The operation of Information Technology-based Transaction Processing done by service providers outside Indonesia must be approved by Bank Indonesia.

(4) The approval as mentioned in paragraph (3) will be granted if the Bank fulfills certain requirements as mentioned in Article 18 paragraphs (2) to (4) and in Article 19 paragraph (3) as well as the following additional requirements:

a. Safeguarding of customers;

b. Activities which process …..

b. Activities which process is handed over to service providers outside Indonesia are not inherent banking functions;

c. Documents supporting financial administration of transactions done in a Bank's office in Indonesia must be maintained in an office of said Bank in Indonesia;

d. The Bank's Business Plans show existing efforts to increase the role of Banks in the economic development of Indonesia;

Article 21

(1) The intention of using service providers in the carrying-out of Data Centers, Disaster Recovery Centers and/or the Information Technology-based transactions processing must be contained in the Information Technology Strategic Plan and the Bank's Business Plan.

(2) Banks must report the arrangements in the use of service providers for carrying out Data Centers, Disaster Recovery Centers and/or the Information Technology-based transactions in Indonesia to Bank Indonesia within 2 (two) months at the latest of said services being operated effectively.

(3) In the event of arrangements to hand over the carrying-out of Data Centers, Disaster Recovery Centers and/or Information Technology-based transactions processing to service providers out of Indonesia, the Bank must submit a request for approval within 4 (four) months at the latest before said services being operated effectively.

(4) Realizations of arrangements to carry out Data Centers, Disaster Recovery Centers and/or Information Technology-based Transactions Processing by service providers must be reported within 1 (one) month at the latest since said activity being effectively operated.

(5) Submission of arrangements and realizations of arrangements as mentioned in paragraph (2), paragraph (3) and paragraph (4) are employed using the Fundamental Alteration Report format.

(6) Approval or rejection of requests as mentioned in paragraph (3) is given within 3 (three) months at the latest after all necessary documents detailing the request are received.

CHAPTER V

ELECTRONIC BANKING

Article 22

(1) Banks providing Electronic Banking services must abide by the regulations of Bank Indonesia.

(2) Banks must continually …..

(2) Banks must continually educate customers regarding Electronic Banking products and its security.

Article 23

(1) Every plan to issue new Electronic Banking products must be contained in the Bank's Business Plan.

(2) Every plan to issue transactional Electronic Banking products must be reported to Bank Indonesia within 2 (two) months at the latest before said product is published.

(3) Reports of plans for products as mentioned in paragraph (2) are not valid for Electronic Banking products as long as there are regulations from Bank Indonesia that exclusively regulate the requirements for the approval of such products.

(4) Reports of plans to issue products as mentioned in paragraph (2) must be complemented with the following:

a. proof of readiness to manage Electronic Banking, that contains at least:

1) supporting organization structure, including surveillance from management;

2) policies, systems, procedures and authorization in the issuing of Electronic Banking products;

3) readiness of the Information Technology infrastructure to support Electronic Banking products;

4) results of analysis and identification of the inherent risks accompanying Electronic Banking;

5) readiness to implement risk management, especially in security control to ensure the fulfillment of the principles of confidentiality, integrity, authentication, non repudiation and availability;

6) legal analysis results;

7) delineation of accounting information system;

8) customer's safeguarding and education programs;

b. results of business analysis on projections of new product for 1 (one) year ahead.

(5) Submission of reports as mentioned in paragraph (2) must be complemented with audit results from independent parties, so as to provide opinions on the product's characteristics and the sufficiency of security on Information Technology systems related to the product, as well as compliance towards regulations and/or international best practices.

(6) In the event that the …..

(6) In the event that the use of Information Technology to carry out Electronic Banking is performed by service providers, bank must also comply the regulations as specified in Chapter IV regarding management of Information Technology by Information Technology service providers.

(7) Realizations of plans to publish Electronic banking products must be reported within 1 (one) month at the latest since said plans are deployed, using the Information Technology Fundamental Alteration Report format.

CHAPTER VI

REPORTING

First Section

Information Technology Usage Report

Article 24

(1) Banks must resubmit its Information Technology Usage Report within 6 (six) months at the latest since the enactment of this Regulation of Bank Indonesia.

(2) Banks must submit an Annual Information Technology Usage Report within 1 (one) month after the end of year report.

(3) The annual report as mentioned in paragraph (2) will be submitted for the first time on January 2009 for the year 2008 report.

Second Section

Fundamental Alteration Report

Article 25

(1) Banks must submit Fundamental Information Technology Alteration Plan Report within 2 (two) months at the latest before said alteration(s) being effectively operated.

(2) Banks must submit Realization of Fundamental Information Technology Alteration Plan Report within 1 (one) month at the latest since said alteration(s) being effectively operated.

(3) Products and/or new activities that have been reported in the Realization of Fundamental Information Technology Alteration Plan Report do not need to be reported in Products and New Activities Report as directed in the Regulations of Bank Indonesia regarding risk management of commercial banks.

Third Section …..

Third Section

Miscellaneous Report

Article 26

(1) Banks must submit results of the Information Technology audits conducted by independent parties on its Data Centers and/or Disaster Recovery Centers and/or Technology-based Transaction Processing of which are carried out by service providers as mentioned in Article 18 paragraph (2) letter b number 7, within 2 (two) months at the latest after said audit is completed.

(2) Banks must submit results of assessments on the implementation of risk management of service providers outside Indonesia as mentioned in Article 19 paragraph (3) letter e number 3, within 1 (one) month at the latest after the last period of risk assessment.

(3) Banks must report critical occurrences, abuses, and/or offenses in the management of Information Technology that are able to cause and/or have caused significant monetary loss and/or disturbances on the operational progress of the Bank.

(4) Reports as mentioned in paragraph (3) must be submitted as soon as possible by e-mail or telephone followed by a written report within 7 (seven) working days at the latest after said occurrences and/or abuses / offenses are identified.

(5) Written report as mentioned in paragraph (4) is part of a circumstantial Report with a potential of significant loss in a bank's financial situation as mentioned in the regulation regarding implementation of risk management for Commercial Banks.

Fourth Section

Report Format and Addresses for Submission

Article 27

The format and guidelines for formulation of reports as mentioned in Article 24, Article 25 and Article 26 are stipulated in a Circular Letter of Bank Indonesia.

Article 28

Requests of approval on the use of service providers outside Indonesia as mentioned in Article 19 and Article 20, as well as report submission as mentioned in Article 24, Article 25 and Article 26 are addressed to:

a. Directorate of Bank Supervision, Jl. MH Thamrin no.2, Jakarta 10350, for a Banks having its Head Office in the working area of Bank Indonesia's Head Office;

B. Bank Indonesia's …..

b. Bank Indonesia's local office, for Banks whose main office is outside the working area of Bank Indonesia's Head office;

CHAPTER VII

MISCELLANEOUS

Article 29

(1) Bank Indonesia is able to carry out inspections or to instruct Bank to carry out inspections on aspects related to the use of Information Technology.

(2) Banks must provide access to allow Bank Indonesia to carry out inspections on all aspects related to the management of Information Technology, both conducted by the bank itself or by other parties.

CHAPTER VIII

SANCTIONS

Article 30

Banks that do not carry out regulations as determined in this Regulation of Bank Indonesia and other related regulations can be penalized as mentioned in Article 52 Act Number 7 year of 1992 regarding Banking as having been changed through Act Number 10 year of 1998, amongst others in the form of:

a. written reprimands;

b. a decrease in management factor in ratings system;

c. freezing and/or closure of certain business activities;

d. mentioning of management personnel in listings of those who have failed in fit and proper tests.

Article 31

Banks that do not comply to the regulation of reporting as mentioned in Article 21 paragraph (2), paragraph (3) and paragraph (4), Article 23 paragraph (2) and paragraph (7), Article 24 and Article 25 of this Regulations of Bank Indonesia will be penalized according to Banking Law Article 52 Act Number 7 1992 as amended by Act Number 10 year of 1998, in the form of:

a. financial penalties of Rp 1.000.000,00 (one million rupiah) per day of lateness per report;

b. financial penalties of Rp 50.000.000,00 (fifty million rupiah) per report, for Banks that have not submitted a report after 1 (one) month has passed since the indicated deadline.

Article 32 …..

Article 32

To banks that submit reports not in accordance with the Bank's actual circumstance are imposed a penalty of Rp 50,000,000.00 (fifty million rupiah) after 2 (two) prior letters of reprimand by Bank Indonesia within a space of 7 (seven) working days for each reprimand, and if the Bank does not fix the report within 7 (seven) working days after the last letter of reprimand.

CHAPTER IX

TRANSITION PROVISION

Article 33

Banks with policies, procedures in the use of Information Technology and risk management guidelines in the use of Information Technology must adjust and refine said policies, procedures and guidelines within 12 (twelve) months at the latest since the enactment of this Bank Indonesia Regulation.

Article 34

Banks that utilize the service of Information Technology service providers before the enactment of this Bank Indonesia Regulation, must conform agreements made according to this Regulation of Bank Indonesia within 12 (twelve) months since the validation of this Regulation of Bank Indonesia.

Article 35

(1) Banks who have reassigned the management of Data Centers, Disaster Recovery Centers and/or Information Technology-based Transactions Processing to service providers outside Indonesia must submit a new request for approval to conform to the regulations of this Bank Indonesia Regulation within 12 (twelve) months at the latest since the enactment of this Bank Indonesia Regulation.

(2) In the event where a Bank does not obtain approval from Bank Indonesia as mentioned in paragraph (1), said Bank must submit an action plan report to Bank Indonesia.

(3) Action plans as mentioned in paragraph (2) should be submitted within 3 (three) months at the latest after the duration as mentioned in paragraph (1) ends, or after the rejection of said Bank's request.

Article 36 …..

Article 36

Banks that have not possess an Information Technology Steering Committee as mentioned in Article 7, must form or conform said committee to this Regulation of Bank Indonesia within 12 (twelve) months at the latest since the enactment of this Bank Indonesia Regulation.

CHAPTER X

CONCLUDING PROVISIONS

Article 37

Further regulations regarding Implementation of Risk Management in the Use of Information Technology by Commercial Banks Implementation are stipulated in a Circular Letter of Bank Indonesia.

Article 38

With the enactment of this Bank Indonesia Regulation:

a. Decree of Board of Directors of Bank Indonesia Number 27/164/KEP/DIR and Notification of Bank Indonesia Number 27/9/UPPB, dated 31st of March 1995 regarding The Use of Information System Technology by Banks;

b. Decree of Board of Directors of Bank Indonesia Number 31/175/KEP/DIR and Notification of Bank Indonesia Number 31/14/UPPB, dated 22nd of December 1998 regarding The Refinement of Bank's Information System Technology in dealing with the year 2000;

c. Regulation of Bank Indonesia Number 1/11/PBI/1999 dated 22nd of December 1999 regarding Special Facilities in the Event of Dealing with Short-term Financial Difficulties for Commercial Banks caused by Computer Problems in the year of 2000;

d. Notification of Bank Indonesia Number 6/18/DPNP dated 20th of April 2004 regarding The Implementation of Risk Management on Internet Banking Activities.

are no longer valid to Commercial Banks.

Article 39

This Bank Indonesia Regulation shall come into force on 31st of March 2008.

For the public to be informed, it is ordered that this Bank Indonesia Regulation be promulgated in the State Gazette of the Republic of Indonesia.

Enacted in Jakarta …..

Enacted in Jakarta

Dated November 30, 2007

on behalf of GOVERNOR OF BANK INDONESIA

MIRANDA S. GOELTOM
SENIOR GOVERNOR DEPUTY

STATE GAZETTE OF THE REPUBLIC OF INDONESIA YEAR OF 2007 NUMBER 144

DPNP

Unofficial translation

EXPLANATION

ON

REGULATION OF BANK INDONESIA

NUMBER: 9/ 15 /PBI/2007

REGARDING

IMPLEMENTATION OF RISK MANAGEMENT IN THE USE OF INFORMATION TECHNOLOGY BY COMMERCIAL BANKS

GENERAL

To increase operational efficiency and service quality, Banks are required to develop its business strategies by using further advances in Information Technology so as to increase the Bank's competitive edge.

The implementation of Information Technology have brought changes in operational and data management, resulting in increased efficiency and effectiveness, as well as providing information accurately and fast. Development of technology-based Bank products such as Electronic Banking help customers carry out a non cash transactions through electronic network with virtually no time constraints. Furthermore the use of third-party services to provide Banking systems and services are also increasing.

Apart from various benefits and advantages obtained from the use of Information Technology in the carrying-out of a Bank's operational, also present are risks harmful to Banks and customers, such as operational risks, legal risks, and risks to the Bank's reputation, aside from other banking risks such as liquidity risks and credit risks.

Considering that Information Technology is an important operational asset that can increase a Bank's value and competitive edge, but holds various risks in its implementation, Banks must implement IT Governance. The success of said implementation of IT Governance depends a great deal on the commitment of the Bank's entire work force, both organizers and users of Information Technology. The implementation of IT Governance is employed by conforming Information Technology Strategic Plan with the Bank's business strategies, optimization of resources management, utilizing Information Technology (IT value delivery), performance measurement, and effective implementation of risk management.

To be able to implement effective risk management, the following are required: involvement and supervision of the Board of Commissioners and Directors; the planning and implementation of policies and procedures related to Information Technology; as well as the process of risks identification, measurement, surveillance, and continuous control.

Aside from the aforementioned, Banks are required to anticipate the necessity of adequate Information Technology infrastructure in dealing with the implementation of *Basel II*.

With this regulation, Banks are expected to be able to manage the risks it faces effectively, in any and all operations supported by the use of Information Technology.

ARTICLE BY ARTICLE …..

ARTICLE BY ARTICLE

Article 1

Self-explanatory

Article 2

Paragraph (1)

Self-explanatory

Paragraph (2)

Self-explanatory

Paragraph (3)

Information Technology resources consist of, amongst others, hardware, software, networks, human resources, and data/information.

Article 3

Complexities of business consist of, amongst others, variations of transactions/products/services and office networks as well as supporting technologies used.

Article 4

In determining authorization and responsibilities, it necessary to consider, amongst others, segregation of duties, for example the party who inputs data is different from the one who validates data.

Article 5

Self-explanatory

Article 6

Letter a

Self-explanatory

Letter b

Number 1

Self-explanatory

Number 2

Efforts to increase competitiveness of human resources are done through, amongst others, the carrying-out of education or training.

Number 3

Self-explanatory

Number 4 …..

Number 4

Self-explanatory

Number 5

Self-explanatory

Article 7

Paragraph (1)

Self-explanatory

Paragraph (2)

Self-explanatory

Paragraph (3)

Structure of the committee is adjustable according to the Bank's magnitude and complexity as well as the Bank's structure of ownership/legal entity.

Letter a until letter d

Self-explanatory

Article 8

Paragraph (1)

Self-explanatory

Paragraph (2)

Depth of policies and procedures other than being adjusted to the purpose, business policy, magnitude, and complexity of the Bank, also takes the Bank's risk profile into consideration.

Letter a until letter i

Self-explanatory

Paragraph (3)

Limit of risks is the level of risks tolerable by the system (risk tolerance) or a security standard determined or agreed not to be exceeded. Said security standard are adjusted to the Bank's risk appetite.

Article 9

Paragraph (1)

Self-explanatory

Paragraph (2)

Self-explanatory

Article 10 …..

Article 10

Self-explanatory

Article 11

Self-explanatory

Article 12

Paragraph (1)

Information Technologies operational activities include activities at Data Centers, Disaster Recovery Centers, or Information Technology users.

Letter a until letter g

Self-explanatory

Paragraph (2)

A system capable of producing separate reports, is one capable of identifying inputs and processes as well as outputs from transactions based on the principle of sharia.

Article 13

Paragraph (1)

Business Continuity Plan and Disaster Recovery Plan are drafted to include recovery plan not only for total disasters, but also for various levels of disturbances and disasters, including minor disasters (with little or no effect and requiring little expenditure and time to be resolved), major disasters (with considerable effects that can worsen if not dealt with immediately), and catastrophic disasters (could cause permanent damage if not dealt immediately and therefore inflicting huge repair/relocation costs)

What is meant by being carried out effectively is when Information Technology operations can proceed immediately after the occurrence of disturbances so as to not hinder services to customers.

Paragraph (2)

Self-explanatory

Paragraph (3)

Self-explanatory

Article 14

Self-explanatory

Article 15

Paragraph (1)

In carrying out …..

In carrying out internal control systems of Information Technology, Banks refer to general principles as regulated in provisions regarding standard reference of internal control systems.

Paragraph (2)

Self-explanatory

Paragraph (3)

What is meant by adequate amongst others are technologies appropriate to a Bank's operations, competent human resources, and organization structures that do not present opportunities for anyone to create and to conceal errors in his/her duty.

Paragraph (4)

Self-explanatory

Article 16

Paragraph (1)

Existing regulations consist amongst others regulation regarding standards of carrying out internal audits.

Paragraph (2)

The employment of external auditors to carry out the function of internal audit on Information Technology does not result in fewer responsibilities for the chief of the Bank's Internal Audit working Unit. In addition, the use of external auditors must consider the magnitude and complexity of the Bank.

Paragraph (3)

Self-explanatory

Article 17

Self-explanatory

Article 18

Paragraph (1)

What is meant by using Information Technology service provider is the use of services provided by another party in the carrying-out of Information Technology in a continual manner and/or a certain period of time. What is meant by another party to branch offices of a foreign Bank includes both out-of-state main offices and other offices of the Bank, or the Bank's business group. What is meant by another party to foreign Banks includes main offices and a Bank's business group.

Paragraph (2)

Letter a

Number 1

What is meant by responsibilities of Banks in implementing risk management are, amongst others,

Ensuring that said service …..

ensuring that said service providers implement risk management adequately on Bank activities carried out by the Information Technology service providers, in accordance with the requirements in this Regulation of Bank Indonesia.

Number 2

Self-explanatory

Number 3

Self-explanatory

Number 4

Self-explanatory

Number 5

Access to data and information is intended to achieve effective inspections.

Number 6

Access to aforementioned databases includes, but is not limited to supplying terminals, user ids to conduct queries, and data downloading.

Letter b

Number 1

This requirement is meant to ensure that Data Centers, Disaster Recovery Centers and/or Technology-based Transaction Processing used by the Bank possess adequate Information Technology control which includes at least physical and logical security.

Number 2

Said access is needed to obtain data and information for auditing, either auditing of Information Technology or other objects.

Number 3

Said statement is confirmed by a Letter of Declaration which has to be made by service providers carrying out Data Centers, Disaster Recovery Centers, and/or Technology-based Transactions Processing.

Number 4

What is meant by information security is the accomplishment of confidentiality, integrity, and authentication.

Number 5

Self-explanatory

Number 6

Self-explanatory

Number 7

Audit by independent …..

Audit by independent auditors includes application systems used to process data.

Number 8

Self-explanatory

Number 9

Self-explanatory

Paragraph (3)

Self-explanatory

Paragraph (4)

What is meant by parties directly involved with Banks are involved parties as regulated in provisions of Bank Indonesia regarding The Legal Lending Limit for Commercial Banks

What is meant by arm's length principle is conditions where transactions among parties are carried out independently, as uninvolved parties, done on an equal basis according to regular market prices, so as to minimize conflicts of interest.

Paragraph (5)

Self-explanatory

Paragraph (6)

Indications of difficulties in the carrying out of inspections are, amongst others:

a. difficulties in accessing data and information by observing authorities

b. difficulties in carrying out inspections on service providers;

c. service providers are used as a media to manipulate the Bank's data or Bank's finances.

Article 19

Paragraph (1)

Self-explanatory

Paragraph (2)

The carrying-out of Data Centers and/or Disaster Recovery Centers out of state which requires the approval of Bank Indonesia, applies to the Bank's office, main office or out-of-state Bank's business groups.

Paragraph 2 does not apply to the carrying-out of Data Centers and/or Disaster Recovery Centers by a branch office of a Bank whose main office is in Indonesia but operates out of state.

Paragraph (3)

Letter a

Self-explanatory

Letter b

What is meant by “does not decrease the effectiveness of Bank Indonesia’s inspections” is not to cause difficulties for inspectors in obtaining data and information required, such as having access to databases and possessing database structures for all applications used.

Letter c

Provisions of valid regulations in Indonesia include, amongst others, the provision of Bank Indonesia regarding manners of directives or written orders to disclose a Bank’s secret.

Letter d

Self-explanatory

Letter e

Self-explanatory

Number 1)

Self-explanatory

Number 2)

Self-explanatory

Number 3)

What is meant by an out-of-state Bank office to a foreign Bank’s branch office, is a main office or other office. On the other hand, for a Bank owned by a foreign financial institution, an out-of-state Bank’s office means said Bank’s central office.

Letter f

Number 1)

Expected benefits are, amongst others, increase in the quality of service to customers.

Number 2)

Self-explanatory

Article 20

Paragraph (1)

What is meant by prudence in this case includes, amongst others, the management of risks on new products and activities, as regulated in the provision concerning risk management. What is meant by new products and activities are, amongst others, products and activities which add or increase risks to the Bank ,including service development such as credit marketing.

Paragraph (2)

Self-explanatory

Paragraph (3)

The carrying-out of Information Technology-based Transactions Processing out of state in this case includes those carried out at the

Main office or other …..

main office or other offices for a foreign Bank's branch office, or central office for Banks under foreign financial institution.

Paragraph (4)

Self-explanatory

Letter a

The relationship between a Banks with its customers is based on clear agreements and considers the provision regarding product information transparency and the use of customers' personal information, as well as the provision regarding customers' complaint resolution. Banks remain responsible for each and every transaction which process is handed over to service providers.

Letter b

What is meant by inherent banking functions activities are activities related to savings, direct deposits, time deposits, and credit excluding credit cards. Included as related activities are amongst others, the maintenance of the master file of customers' personal information.

Letter c

What is meant by documents supporting financial administration are data proving the existence of rights and obligations as well as business activities of a company, which is used to support the drafting of financial reports. For example: credit deeds and credit approval documents, deal slips and deal confirmations on treasury transactions, as well as documents of fund transfer orders through SWIFT.

Letter d

Efforts to increase the role of Banks for Indonesia's economic developments, is reflected, amongst others, through plans to increase credit funding, an increase in export import funding, etc.

Article 21

Paragraph (1)

Self-explanatory

Paragraph (2)

Self-explanatory

Paragraph (3)

Self-explanatory

Paragraph (4)

Such report includes post implementation review.

Paragraph (5)

Self-explanatory

Paragraph (6)

What is meant by all …..

What is meant by all necessary documents detailing the request are received, is that all the required documents are physically received, with additional data/information if necessary.

Article 22

Paragraph (1)

The valid Regulation of Bank Indonesia consists of provisions that regulate products, such as the provision regarding the Payment Using Cards, and other provisions such as the provision regarding the Implementation of Know Your Customer Principle, and the provision regarding the Implementation of Risk Management, as well as other provisions which regulate the principles of prudence in a Bank's business.

Paragraph (2)

Education given by Banks to customers is meant as an effort to increase the customers' understanding on the characteristics of Electronic Banking, including its benefits, risks, security, and possibilities of squander by other parties resulting in losses for customers.

Article 23

Paragraph (1)

Self-explanatory

Paragraph (2)

What is meant by Electronic Banking products are new products which characteristics are different from existing products, and/or add or increase risk exposure to the Bank.

Paragraph (3)

Self-explanatory

Paragraph (4)

Self-explanatory

Paragraph (5)

The result of examinations from an independent party outside the Bank is required for Electronic Banking products issued for the first time such as transactional internet banking, and sms banking.

On the other hand, to add existing Electronic Banking products' service features which could add or increase risk exposure, Banks can submit the result of examinations conducted internally, by a party uninvolved in the planning and development of application systems as well as decision making in the implementation of Electronic Banking.

Paragraph (6)

Self-explanatory

Paragraph (7)

Report of realization of the plan to publish Electronic Banking products includes post implementation review.

Article 24

Paragraph (1)

Self-explanatory

Paragraph (2)

The content of this report consists of alterations done over one report year on data submitted through the Report of Information Technology Use, outside alterations reported in the Fundamental Alteration Report. Items necessary to report are, amongst others, the change of deciding authorities in the Information Technology organization structure as well as long term plans alteration (IT Strategic Plan).

Paragraph (3)

Self-explanatory

Article 25

Paragraph (1)

Fundamental alterations reported are, amongst others, alterations on configurations, core banking applications, Electronic Banking products, the use of domestic service providers, and other fundamental alterations which could add or increase Bank's risks.

Paragraph (2)

Self-explanatory

Paragraph (3)

With the validation of provisions in this paragraph, the obligation to submit the report of new products and activities as regulated in the provision of risk management becomes invalid for the product reported in this report of realization form.

Article 26

Paragraph (1)

Self-explanatory

Paragraph (2)

Self-explanatory

Paragraph (3)

Included in critical occurrences are serious system failures, system down time, and performance degradation of systems affecting a Bank's performance in providing service to its customers.

Paragraph (4)

Reports through e-mail or telephone to auditors are based on initial information.

Paragraph (5) …..

Paragraph (5)

Self-explanatory

Article 27

Self-explanatory

Article 28

Self-explanatory

Article 29

Paragraph (1)

Self-explanatory

Paragraph (2)

Providing access to Bank Indonesia is meant to enable effective observation by Bank Indonesia, to ensure, amongst others, integrity, validity, availability, and authenticity of data on each and every transaction.

Said access includes :

a. access to databases, for recent and past data;

b. access to supporting infrastructure such as communication networks.

Article 30

Self-explanatory

Article 31

Self-explanatory

Article 32

Self-explanatory

Article 33

Self-explanatory

Article 34

Self-explanatory

Article 35

Paragraph (1)

Request of re-approval is submitted in the form of a Fundamental Alteration Plan Report, as regulated in the Notification of Bank Indonesia.

Paragraph (2)

The content of the action plan are, amongst others, plans on relocating Data Centers, Disaster Recovery Centers, and/or Technology-based Transaction Processing back to Indonesia, and the action plan's timetable.

Paragraph (3)

Self-explanatory

Article 36

Self-explanatory

Article 37

Self-explanatory

Article 38

Self-explanatory

Article 39

Self-explanatory

ADDITION TO STATE GAZETTE OF THE REPUBLIC OF INDONESIA NUMBER DPNP