BANK INDONESIA REGULATION
NUMBER 2 OF 2024
ON
INFORMATION SYSTEM SECURITY AND CYBER RESILIENCE FOR PAYMENT SYSTEM PROVIDERS, MONEY MARKET AND FOREIGN EXCHANGE MARKET PARTICIPANTS, AS WELL AS OTHER PARTIES REGULATED AND SUPERVISED BY BANK INDONESIA

BY THE BLESSINGS OF ALMIGHTY GOD

THE GOVERNOR OF BANK INDONESIA,

Considering : a. that in order to realize the objectives of Bank Indonesia to achieve stability of rupiah value, maintain payment system stability, and contribute to maintaining financial system stability in order to support sustainable economic growth, it is necessary to utilize information technology to encourage the acceleration of digital financial economic development;

b. that the utilization of information technology has the potential to increase cyber risk exposure which may cause financial losses and disrupt the stability of financial system, thus it is necessary to establish information system security and cyber resilience which refers to international standards and best practices;

c. that in order to establish information system security and cyber resilience, it is necessary to regulate information system security and cyber resilience for payment system providers, money market and foreign exchange market participants, as well as other parties regulated and supervised by Bank Indonesia;

d. that based on the considerations as referred to in point a, point b, and point c, it is necessary to issue the Bank Indonesia Regulation on Information System Security and Cyber Resilience for Payment System Providers, Money Market and Foreign Exchange Market Participants, as well as Other Parties Regulated and Supervised by Bank Indonesia;

Observing : 1. Law Number 23 of 1999 on Bank Indonesia (State Gazette of the Republic of Indonesia of 1999 Number 66, Supplement to the State Gazette of the Republic of Indonesia Number 3843) as amended several times and last by Law Number 4 of 2023 on the Development and Strengthening of the Financial Sector (State Gazette of the Republic of Indonesia of 2023 Number 4, Supplement to the State Gazette of the Republic of Indonesia Number 6845);

2. Law Number 4 of 2023 on the Development and Strengthening of the Financial Sector (State Gazette of the Republic of Indonesia of 2023 Number 4, Supplement to the State Gazette of the Republic of Indonesia Number 6845);

HAS DECIDED:

To enact : BANK INDONESIA REGULATION ON INFORMATION SYSTEM SECURITY AND CYBER RESILIENCE FOR PAYMENT SYSTEM PROVIDERS, MONEY MARKET AND FOREIGN EXCHANGE MARKET PARTICIPANTS, AND OTHER PARTIES REGULATED AND SUPERVISED BY BANK INDONESIA.

CHAPTER I
GENERAL PROVISIONS

Article 1

In this Bank Indonesia Regulation, the following definitions are employed:

1. Information System is an integration of components of data, information, apps system, information technology infrastructure, process and/or humans that interact with each other to achieve a goal.
2. Cyber is a virtual space formed from an Information System.
3. Payment System is a system that includes a set of rules, institutions, mechanisms, infrastructure, sources of funds for payments, and access to sources of funds for payments, which are used to carry out transfer of funds in order to fulfill an obligation that arises from an economic activity.
4. Financial System is an entity consisting of financial services institutions, financial markets and financial infrastructure, including the Payment System, which interact in facilitating the collection of public funds and their allocation to support the national economy activities, as well as corporations and households connected to financial services institutions.
5. Money Market is a part of the Financial System which is connected with:
   a. issuance and trading activities of financial instruments or debt securities with maturity of no more than 1 (one) year;
   b. money-lending transactions;
   c. interest rate derivative transactions; and
   d. other transactions that fulfil the characteristics of money market,

   in rupiah or foreign currencies.
6. Foreign Exchange Market is a part of the Financial System which relates to a transaction activity which involves the exchange of currencies from 2 (two) different countries and their derivatives, but does not include the exchange of banknotes organized by foreign exchange business activities.
7. Payment Service Provider (Penyedia Jasa Pembayaran), hereinafter referred to as PJP is as referred to in Bank Indonesia Regulation on Payment Service Provider.

8. Payment System Infrastructure Providers (Penyelenggara Infrastruktur Sistem Pembayaran), hereinafter referred to as PIP, is a party which organizes infrastructure as a facility which may be used to transfer funds for the interests of its members.
9. Business Actor in the Financial Sector Engaged in the Money Market and/or Foreign Exchange Market (Pelaku Usaha Sektor Keuangan yang Bergerak di Pasar Uang dan/atau Pasar Valuta Asing), hereinafter referred to as PUSK PUVA is a business actor in the Money Market and/or Foreign Exchange Market that obtains an institutional permit from Bank Indonesia.
10. Money Market Supporting Agency is a party that provides services relating to the issuance of Money Market instruments, intermediary for the implementation of Money Market instruments transactions, transaction settlements, administration of Money Market instruments and transactions, and other parties as stipulated by Bank Indonesia.
11. Foreign Exchange Market Supporting Agency is a party that may provide services in relation to intermediary for transaction implementation, transaction settlement, administration of transaction in Foreign Exchange Market, and other parties stipulated by Bank Indonesia.
12. Provider of Foreign Exchange Business Activities Other Than Banks is as referred to in Bank Indonesia Regulation on Foreign Exchange Business Activities Other Than Bank.
13. Provider is a party regulated and supervised by Bank Indonesia which is exposed to cyber risk, both systemic and non-systemic for the Financial System.
14. Cyber Vulnerability is weakness, vulnerability, or flaw in Cyber which has a negative impact on the business and/or operational services of a Provider.
15. Cyber Threat is a situation which has the potential to exploit Cyber Vulnerability.
16. Cyber Attack is an attempt to exploit Cyber Vulnerability.
17. Cyber Incident is a Cyber Attack which disrupts the expediency of business and/or operational services of a Provider which requires a response and/or recovery.
18. Cyber Risk is the possibility of a Cyber Incident and the resulting impact of a Cyber Incident.
19. Information System Security and Cyber Resilience (Keamanan Sistem Informasi dan Ketahanan Siber), from this point onwards, is referred to as KKS, is a condition of maintaining the confidentiality, integrity, and availability of information and/or Information System of a Provider from a Cyber Attack and maintaining the business continuity of a Provider through anticipatory, adaptive and proactive measures against a Cyber Threat, as well as the ability of a Provider to quickly respond and recover from a Cyber Incident.
20. Self-Regulatory Organization hereinafter referred to as SRO, is a forum or institution incorporated in an Indonesian legal entity designated by Bank Indonesia to support the organization of Payment System, Money Market and Foreign

Exchange Market, and/or other activities that are regulated and supervised by Bank Indonesia.

CHAPTER II
REGULATION AND SUPERVISION OF KKS

Article 2

Bank Indonesia shall regulate and supervise KKS with the aim of creating KKS at Providers in order to support the objectives of Bank Indonesia.

Article 3

Targets for regulation and supervision of KKS shall include:
a. improvement of KKS of Providers to prevent and handle the impacts of a Cyber Attack;
b. improvement of Cyber Risk management of Providers; and
c. strengthening the supervision and collaboration in the prevention of Cyber Incident and/or the handling of a Cyber Incident that occurs to Providers.

Article 4

The basic principles of KKS implementation shall include:
a. clarity of roles and responsibilities;
b. comprehensive strategy;
c. Cyber Risk management integrated with enterprise risk management;
d. integration with KKS culture; and
e. readiness to deal with Cyber Incident.

Article 5

Providers that become the object of KKS regulation and supervision shall include:
a. PJP;
b. PIP;
c. PUSK PUVA;
d. Money Market Supporting Agency;
e. Foreign Exchange Market Supporting Agency;
f. Provider of Foreign Exchange Business Activities Other Than Banks; and
g. other parties regulated and supervised by Bank Indonesia.

Article 6

The scope of regulation and supervision of KKS to include:
a. governance;
b. prevention;
c. handling;
d. supervision; and
e. collaboration.

CHAPTER III
GOVERNANCE

Part One
General

Article 7
Governance as referred to in Article 6 point a shall include:
a. KKS strategy and policy; and
b. KKS culture.

Part Two
KKS Strategy and Policy

Article 8
(1) The KKS strategy and policy as referred to in Article 7 point a shall include:
   a. KKS strategic plan
   b. KKS policies, standards and procedures; and
   c. KKS organizational function.
(2) The KKS strategy and policy as referred to in section (1) shall be prepared and implemented by Providers in order to strengthen KKS.

Paragraph 1
KKS Strategic Plan

Article 9
(1) The KKS strategic plan as referred to in Article 8 section (1) point a shall include:
   a. strategic direction for the strengthening of KKS;
   b. roadmap for the strengthening of KKS; and
   c. estimated resource requirements,
   which include human, process and technological aspects.
(2) Providers shall periodically evaluate the KKS strategic plan as referred to in section (1) in accordance with the development of Cyber Risk.
(3) Further provisions regarding the KKS strategic plan as referred to in section (1) shall be regulated in Regulation of the Members of the Board of Governors.

Paragraph 2
KKS Policies, Standards and Procedures

Article 10
(1) The KKS policies, standards and procedures as referred to in Article 8 section (1) point b shall encompass human, process and technological aspects which at least comprise:
   a. data security, apps system, and information technology infrastructure;
   b. third party security; and
   c. consumer protection and fraud management.
(2) Providers shall periodically evaluate the KKS policies, standards and procedures as referred to in section (1) in order to ensure the adequacy and effectiveness of KKS

policies, standards and procedures in accordance with the latest developments.

(3) Further provisions on the KKS policies, standards and procedures as referred to in section (1) shall be regulated in a Regulation of the Members of the Board of Governors.

Paragraph 3
KKS Organizational Function

Article 11

The KKS organizational function as referred to in Article 8 section (1) point c shall include:

a. KKS management;
b. Cyber Risk management; and
c. KKS audit.

Article 12

(1) In carrying out the KKS organizational function as referred to in Article 11, Providers shall pay attention to:
   a. effectiveness and efficiency;
   b. accountability; and
   c. capacity and capability of human resources.

(2) In carrying out the KKS organizational function as referred to in section (1), Providers may cooperate with other parties.

Article 13

(1) Providers shall implement the KKS management as referred to in Article 11 point a which includes:
   a. strategic planning of KKS;
   b. formulation of KKS policies, standards and procedures;
   c. implementation of KKS culture; and
   d. implementation of prevention and handling of KKS.

(2) The KKS management is responsible to the highest management for the implementation of KKS activities.

(3) In implementing the KKS management as referred to in section (1), the KKS management may cooperate with other parties.

Article 14

(1) Providers shall implement the Cyber Risk management as referred to in Article 11 point b in accordance with best practices.

(2) The Cyber Risk Management as referred to in section (1) shall encompass the protection aspect against:
   a. confidentiality;
   b. integrity; and
   c. availability

   of information in supporting the continuity of business process.

Article 15

(1) Providers shall implement the Cyber-Risk management as referred to in Article 14 at least through:
   a. integration of Cyber Risk management into risk management process of Providers;
   b. identification, assessment, mitigation and evaluation of Cyber Risk toward a Cyber Threat or a Cyber Attack; and
   c. periodic measurement of maturity level of KKS.
(2) Further provisions on the measurement of maturity level of KKS as referred to in section(1) point c shall be regulated in a Regulation of the Members of the Board of Governors.

Article 16

(1) Providers shall implement the KKS audit as referred to in Article 11 point c as a means to ensure the compliance with regulations, policies, standards and procedures, as well as the effectiveness of control in the implementation of KKS.
(2) The KKS audit as referred to in section(1) shall at least include:
   a. governance;
   b. prevention; and
   c. handling.

Article 17

(1) Providers shall carry out the KKS audit as referred to in Article 16 periodically.
(2) The implementation of the KKS audit as referred to in section (1) shall carried out by an internal party and/or external party independently.
(3) Further provisions regarding the implementation of KKS audit as referred to in section (1) shall be regulated in a Regulation of the Members of the Board of Governors.

Part Three
KKS Culture

Article 18

(1) The KKS culture as referred to in Article 7 point b shall be implemented as a means to increase Cyber Risk awareness as well as positive behavior and Cyber ethics.
(2) The KKS culture as referred to in section (1) shall be implemented by Providers through a KKS culture improvement program.
(3) The KKS culture improvement program as referred to in section (2) shall be provided to:
   a. internal party;
   b. third party; and
   c. consumer.
(4) The KKS culture improvement program as referred to in section (2) shall be implemented periodically by involving the highest management as a role model.

Article 19

Further provisions regarding the KKS culture as referred to in Article 18 shall be regulated under a Regulation of the Members of the Board of Governors.

CHAPTER IV
PREVENTION

Part One
General

Article 20

(1) The prevention as referred to in Article 6 point b to include:
   a. identification;
   b. protection; and
   c. detection.

(2) The prevention as referred to in section (1) shall be implemented by Providers to anticipate a Cyber Incident.

Part Two
Identification

Article 21

(1) The identification as referred to in Article 20 section (1) point a shall include:
   a. preparation of Cyber Risk profile; and
   b. periodic updating of Cyber Risk profile.

(2) The preparation of Cyber Risk profile as referred to in section (1) point a shall include:
   a. identification of Cyber Risk;
   b. assessment of Cyber Risk ; and
   c. analysis of business impact.

(3) The identification as referred to in section (1) shall be carried out by Providers in order to understand the Cyber Risk profile in order to obtain a comprehensive picture related to Cyber Risks that they face as well as the prioritization of required control.

(4) Further provisions regarding the identification as referred to in section (1) shall be regulated in a Regulation of the Members of the Board of Governors.

Paragraph 1
Assessment of Cyber Risk

Article 22

(1) Assessment of Cyber Risk as referred to in Article 21 section (2) point b shall be conducted at least by:
   a. Cyber Vulnerability and Cyber Threat from human, process and technological aspects; and
   b. objects to be protected.

(2) Cyber Vulnerability and Cyber Threat information as referred to in section (1) point a may be sourced from an information exchange facility established by Bank Indonesia or other information facilities.

Paragraph 2
Assessment of Cyber Risk

Article 23

Assessment of Cyber Risk as referred to in Article 21 paragraph (2) letter b shall be conducted at least by:

a. determining the relevant Cyber Risk assessment methodology;
b. conducting impact assessment of Cyber Vulnerability and Cyber Threat that affect the operational services; and
c. prioritize the mitigation of Cyber Vulnerability and Cyber Threat from the highest to the lowest.

Paragraph 3
Analysis of Business Impact

Article 24

The analysis of business impact as referred to in Article 21 section (2) point c shall be conducted at least by:

a. carrying out business impact assessments relating to Cyber Vulnerability against financial and non financial aspects, including the impact on stability of the Financial System;
b. analyzing the criticality of business function and Information System as well as the prioritization of risk control; and
c. analyzing critical Information System that has a broad impact on stability of the Financial System.

Article 25

Critical Information System with broad impact as referred to in Article 24 point c shall be categorized as vital information infrastructure.

Part Three
Protection

Article 26

(1) The protection as referred to in Article 20 section (1) point b to include:
    a. development of defense system; and
    b. securing and protecting data and/or information.
(2) The protection as referred to in section (1) shall be carried out by Providers in order to develop a defense system that is able to prevent the occurrence of a Cyber Attack based on the risk profile as well as to secure data and/or information at each stage of the data and/or information management cycle.

Paragraph 1
Development of Defense System

Article 27

The development of defense system as referred to in Article 26 section (1) point a in aspects of human, process, and technology shall be conducted at least by:

a. ensuring the security of internal party and third party at every stage of work cycle as well as provide education to KKS in accordance with the role and responsibility;
b. implementing security control for business process as well as implementing security policies, standards and procedures effectively; and
c. implementing the security configuration of Information System that is used.

Paragraph 2
Security and Protection of Data and Information

Article 28

The security and protection of data and/or information as referred to in Article 26 section (1) point b shall be carried out at least by:

a. securing data and/or information at every stage of data and/or information lifecycle based on the classification of data and/or information determined by Providers; and
b. ensuring the compliance of personal data protection in accordance with provisions of laws and regulations.

Part Four
Detection

Article 29

(1) The detection as referred to in Article 20 section (1) point c shall include:
    a. monitoring;
    b. analysis of monitoring results;
    c. analysis of Cyber Attack;
    d. analysis of malicious code or unauthorized code; and
    e. maintenance and testing of detection system.
(2) The detection as referred to in section (1) shall be implemented by Providers to:
    a. discover any Cyber Vulnerability, Cyber Attack and/or Cyber Incident that occur;
    b. provide early warning; and
    c. strengthen the KKS in a sustainable manner.

Paragraph 1
Monitoring

Article 30

The monitoring as referred to in Article 29 section (1) point a shall be conducted at least by:

a. monitoring the logical and physical accesses that have the potential to lead to a Cyber Attack;

b. determining threshold indicator as a trigger for the activation of early warning system; and
c. performing Cyber Vulnerability scan,
consistently and sustainably.

Paragraph 2
Analysis of Monitoring Results

Article 31
The analysis of monitoring results as referred to in Article 29 section (1) point b shall be conducted at least by:
a. analyzing the Cyber activity record; and
b. analyzing Cyber Vulnerability and the potential for a Cyber Attack.

Paragraph 3
Analysis of Cyber Attack

Article 32
The analysis of a Cyber Attack as referred to in Article 29 section (1) point c shall be conducted at least by:
a. conducting an assessment of the source, type, and time of the occurrence of a Cyber Attack, including fraud;
b. conducting an assessment of the impact of a Cyber Attack on the system and other connected systems; and
c. conducting an escalation, if there is a potential for a Cyber Incident.

Paragraph 4
Analysis of Malicious Code or Invalid Code

Article 33
The analysis of malicious code or invalid code as referred to in Article 29 section (1) point d shall be conducted at least by:
a. analyzing any malicious code or invalid code which has the potential to give rise to a Cyber Attack; and
b. carrying out a follow-up escalation and/or an evaluation of detection of malicious code or invalid code.

Paragraph 5
Maintenance and Testing of Detection System

Article 34
(1) The maintenance and testing of detection system as referred to in Article 29 section (1) point e shall be conducted periodically at least by ensuring:
    a. the monitoring system is maintained with the latest software version; and
    b. the reliability of monitoring system has been tested.
(2) Further provisions on the maintenance and testing of detection system as referred to in section (1) shall be regulated in a Regulation of the Members of the Board of Governors.

CHAPTER V
HANDLING

Part One
General

Article 35

(1) The handling as referred to in Article 6 point c to include:
   a. response; and
   b. recovery.

(2) The handling as referred to in section (1) shall be implemented by Providers to:
   a. mitigate a Cyber Incident; and
   b. return services to normal conditions.

Part Two
Response

Article 36

(1) The response as referred to in Article 35 section (1) point a to include:
   a. formulation of a Cyber Incident handling and recovery plan;
   b. implementation of simulation and trial for the handling and recovery of a Cyber Incident;
   c. handling of a Cyber Incident; and
   d. implementation of communication for the handling of a Cyber Incident.

(2) The response as referred to in section (1) shall be implemented by Providerss in order to:
   a. prepare the handling process of a Cyber Incident;
   b. prevent the expansion of impact of a Cyber Incident; and
   c. communicate the handling of a Cyber Incident.

Paragraph 1
Formulation of Cyber Incident Handling and Recovery Plan

Article 37

(1) The formulation of a Cyber Incident handling and recovery plan as referred to in Article 36 section (1) point a shall at least contain:
   a. determination of Cyber Incident status;
   b. Cyber Incident response;
   c. impact limitation; and
   d. recovery plan which takes the recovery time objective and recovery point objective into account.

(2) The Cyber Incident handling and recovery plan as referred to in section (1) shall be prepared by Providers as a part of the business continuity plan of a Providers.

(3) Providers shall establish a Cyber Incident response team at the organizational level which plays a role in the handling of a Cyber Incident.

(4) The Cyber Incident response team as referred to in section (3) may involve personnel from across departments, work units and parts.

Paragraph 2
Implementation of Simulation and Trial of the Handling and Recovery of Cyber Incident

Article 38

(1) The implementation of simulation and trial of the handling and recovery of a Cyber Incident as referred to in Article 36 section (1) point b shall be conducted comprehensively and periodically.
(2) The simulation and trial of the handling and recovery of a Cyber Incident as referred to in section (1) may be conducted by involving other parties.
(3) Further provisions regarding the simulation and testing of the handling and recovery of a Cyber Incident as referred to in section (1) shall be regulated under a Regulation of the Members of the Board of Governors.

Article 39

Providers shall evaluate the effectiveness and improvement of a Cyber Incident handling and recovery plan based on the results of simulation and trial of Cyber Incident handling and recovery.

Paragraph 3
Handling of Cyber Incident

Article 40

Handling of Cyber Incident as referred to in Article 36 section (1) point c shall be implemented at least by:
a. activating the Cyber Incident response team at the organizational level;
b. submitting:
    1. an initial notification of a Cyber Incident maximum 1 (one) hour after a Cyber Incident is known by Providers; and
    2. a report on a Cyber Incident maximum 3 (three) calendar days after the occurrence of the Cyber Incident,

    to Bank Indonesia;
c. conduct deepening of a Cyber Incident which includes the source, type and time of the attack, analysis of the impact, as well as forensics of the Cyber Incident;
d. carrying out mitigation of a Cyber Incident and limit their impacts;
e. carrying out the escalation and handling of a Cyber Incident in accordance with the level of impact of the Cyber Incident; and
f. carrying out the handling of a Cyber Incident by using internal and/or external resources.

Paragraph 4
Implementation of Communication for the Handling of Cyber Incident

Article 41

The implementation of communication for the handling of a Cyber Incident as referred to in Article 36 section (1) point d shall be carried out at least by:

a. formulating communication strategy and method for the handling and recovery of a Cyber Incident;
b. communicating the handling of a Cyber Incident to stakeholders based on the communication strategy and method as referred to in point a; and
c. communicating the progress of handling of a Cyber Incident to Bank Indonesia.

Part Three
Recovery

Article 42

(1) The recovery as referred to in Article 35 section (1) point b shall be carried out at least by:
    a. returning services to normal conditions;
    b. continuous improvement; and
    c. implementing Cyber Incident recovery communications.
(2) The recovery as referred to in section (1) shall be conducted by Providers to:
    a. restore services as normal conditions in acoordance with priority; and
    b. strengthening KKS so that the Cyber Incidents does not recur.

Paragraph 1
Returning Services to Normal Conditions

Article 43

(1) In returning services to normal conditions, as referred to in Article 42 section (1) point a, Providers shall stipulate:
    a. alternative work location;
    b. separate data center; and/or
    c. alternative data communication network,
    in accordance with the analysis results of the impact of handling of Cyber Incident.
(2) The return of services to normal conditions as referred to in section (1) shall be in accordance with the Cyber Incident recovery plan and shall refer to the recovery priority.

Paragraph 2
Continuous Improvement

Article 44

The continuous improvement as referred to in Article 42 section (1) point b shall be conducted at least by:

a. evaluating the effectiveness and improvement of the Cyber Incident handling and recovery plan based on the Cyber Incident handling and recovery that has been conducted; and
b. carrying out efforts to strengthen KKS in order to mitigate the risk of similar Cyber Incident.

Paragraph 3
Implementation of Communications for Cyber Incident Recovery

Article 45

The implementation of communication for Cyber Incident recovery as referred to in Article 42 section (1) point c shall be conducted at least by:
a. communicating the recovery of a Cyber Incident to stakeholders by referring to the communication strategy and method as referred to in Article 41 point a; and
b. communicating the progress of Cyber Incident recovery to Bank Indonesia.

CHAPTER VI
SUPERVISION

Part One
General

Article 46

The supervision as referred to in Article 6 point d to include:
a. supervision mechanism; and
b. submission of data and/or information.

Part Two
Supervision Mechanism

Article 47

Bank Indonesia shall conduct supervision to ensure the achievement of KKS in Providers.

Article 48

Bank Indonesia shall supervise Providers by using a risk- and/or compliance-based supervision approach.

Article 49

The mechanism for supervision of Providerss shall be conducted through:
a. indirect supervision; and
b. direct supervision.

Article 50

(1) The indirect supervision as referred to in Article 49 point a shall be conducted through monitoring, identification and/or assessment of reports, data and/or information submitted by Providers to Bank Indonesia.

(2) The indirect supervision as referred to in section (1) may be conducted in an integrated manner, including towards the parent company, subsidiary companies, and/or other affiliated parties.

Article 51

(1) The direct supervision mechanism as referred to in Article 49 letter b shall be conducted through face-to face meetings or other mechanisms as stipulated by Bank Indonesia.
(2) The direct supervision as referred to in paragraph (1) may be conducted in an integrated manner, including towards the parent company, subsidiary companies, and/or other affiliated parties.
(3) Objects of direct supervision as referred to in section (1) to include documents, infrastructure, Information System, and other objects used by Providers.
(4) The period of direct supervision as referred to in section (1) shall be conducted periodically and/or at any time.
(5) In conducting direct supervision, Bank Indonesia may assign other parties for and on behalf of Bank Indonesia.

Article 52

Based on the results of indirect supervision as referred to in Article 50 and direct supervision as referred to in Article 51, Bank Indonesia shall carry out follow-up supervision in the form of requesting Providers to:
a. do or not to do something; and/or
b. limit the activities and/or services of Providers.

Article 53

Bank Indonesia may coordinate with other authorities if the parent company of a Providers, subsidiary companies of a Providers and/or other affiliated parties are under the supervision of other authorities.

Part Three
Submission of Data and Information

Article 54

(1) Providers shall submit data and/or information as referred to in Article 46 point b to Bank Indonesia.
(2) Data and/or information as referred to in section (1) related to the implementation of KKS shall include the areas of:
    a. governance;
    b. prevention; and
    c. handling.
(3) Data and/or information as referred to in section (2) shall be submitted in the form of documents, raw data and/or processed data.
(4) Data and/or information as referred to in section (3) shall be submitted through reporting:
    a. annually, including:
        1. the maturity level of KKS; and

2. identification results of vital information infrastructure, and

b. Incidental at the time of an occurrence of a Cyber Incident.

(5) Further provisions regarding procedures for the submission of data and/or information as referred to in section (1) shall be regulated in a Regulation of the Members of the Board of Governors.

Article 55

(1) The report as referred to in Article 54 section (4) be required to submitted by Providers to Bank Indonesia.

(2) Providers that violate the provisions as referred to in section (1) shall be subject to administrative sanctions in the form of:
   a. reprimand;
   b. obligation to pay;
   c. temporary partial or entire suspension of activities, including the implementation of cooperation; and/or
   d. repeal of license and/or approval that have been granted.

(3) The administrative sanction in the form of an obligation to pay as referred to in section (2) point b, shall be imposed for a maximum of Rp5,000,000.00 (five million rupiah) per report.

(4) Further provisions on procedures for the submission of report and the imposition of administrative sanctions shall be regulated in a Regulation of the Members of the Board of Governors.

CHAPTER VII
COLLABORATION

Part One
General

Article 56

(1) The collaboration as referred to in Article 6 point e shall include:
   a. exchange of information;
   b. prevention of a Cyber Incident and its contagion effects; and
   c. cooperation with SRO.

(2) Bank Indonesia shall conduct the collaboration as referred to in section (1) to:
   a. strengthen the cooperation with Providers and/or association of Providers; and
   b. strengthen the KKS in the prevention and handling of Cyber Incident.

Part Two
Exchange of Information

Article 57

(1) Providers shall exchange information as referred to in Article 56 section (1) point a in relation to the identification results of Cyber Vulnerability, Cyber Threat, Cyber Attack and Cyber Incident that may disrupt the stability of the Financial System to Bank Indonesia.
(2) The exchanged information resulting from the identification as referred to in section (1) shall at least include:
    a. source and patterns of a Cyber Threat and a Cyber Attack;
    b. security gap that impacts the Cyber Vulnerability; and
    c. lessons learned from the handling of Cyber Incident.
(3) Bank Indonesia may forward information on identification results of Cyber Vulnerability, Cyber Threat, Cyber Attack and Cyber Incident as referred to in section (1) to the relevant authorities and/or other Providers.

Article 58

Bank Indonesia may establish sharing facilities as a means of exchanging information on Cyber Vulnerability, Cyber Threat, Cyber Attack and Cyber Incident between Providers.

Part Three
Prevention of Cyber Incident and Contagion Effects

Article 59

Prevention of Cyber Incident and Contagion Effects Article 59 In preventing a Cyber Incident and its contagion effects as referred to in Article 56 section (1) point b, Bank Indonesia may:
a. isolate access to Bank Indonesia infrastructure; and
b. collaborate and coordinate with authorities, institutions and/or other Providers in the handling of a Cyber Incident at Providers.

Article 60

Bank Indonesia may collaborate and coordinate with authorities, institutions and/or Providers to ensure the readiness of the handling of a Cyber Incident.

Part Four
Cooperation with SRO

Article 61

(1) Bank Indonesia may assign an SRO to formulate and establish technical and specific KKS procedures.
(2) In establishing the KKS procedures as referred to in section (1), an SRO must obtain approval from Bank Indonesia.
(3) Bank Indonesia may appoint an SRO as a liaison office with Providers.
(4) Further provisions on mechanism for the submission of application for approval of KKS procedures shall be

regulated in a Regulation of the Members of the Board of Governors.

CHAPTER VIII
IMPLEMENTATION OF KKS

Article 62

(1) Providers shall implement KKS in accordance with the classification of Providers.
(2) The classification of Providers as referred to in section (1) for:
    a. PJP shall refer to Bank Indonesia Regulation on Payment System and Bank Indonesia Regulation on PJP;
    b. PIP shall refer to Bank Indonesia Regulation on Payment System and Bank Indonesia Regulation on PIP;
    c. PUSK PUVA, Money Market Supporting Agency, and Foreign Exchange Market Supporting Agency shall be conducted based on the level of financial market infrastructure risk which refers to Bank Indonesia Regulation on Money Market and Foreign Exchange Market; and
    d. Providers other than Providers as referred to in point a to point c shall be conducted by taking into account the risk level of information technology infrastructure and/or based on the risk level stipulated by Bank Indonesia.
(3) Further provisions on the implementation of KKS in accordance with the classification of Providers as referred to in section (1) shall be regulated in a Regulation of the Members of the Board of Governors.

CHAPTER IX
CLOSING PROVISIONS

Article 63

This Bank Indonesia Regulation comes into force on the date of its promulgation.
In order that any person may know hereof, it is ordered to promulgate this Bank Indonesia Regulation by its placement in the State Gazette of the Republic of Indonesia.

Issued in Jakarta
On 18 April 2024

THE GOVERNOR OF BANK INDONESIA,

PERRY WARJIYO

Promulgated in Jakarta
On 22 April 2024

THE MINISTER OF LAW AND HUMAN RIGHTS
OF THE REPUBLIC OF INDONESIA,

YASONNA H. LAOLY

STATE GAZETTE OF THE REPUBLIC OF INDONESIA OF 2024 NUMBER 9/BI

ELUCIDATION
OF
REGULATION OF BANK OF INDONESIA
NUMBER 2 OF 2024
ON
INFORMATION SYSTEM SECURITY AND CYBER RESILIENCE FOR PAYMENT SYSTEMS PROVIDERS, MONEY MARKET AND FOREIGN EXCHANGE MARKET PARTICIPANTS, AS WELL AS OTHER PARTIES REGULATED AND SUPERVISED BY BANK INDONESIA

I. UMUM

Law Number 23 of 1999 on Bank Indonesia as amended several times and last by Law Number 4 of 2023 on the Development and Strengthening of Financial Sector, strengthens the authority of Bank Indonesia to regulate and supervise financial sector business actors and the organization of financial sector technological innovation, specifically in relation to the implementation of Information System security and reliability, including Cyber resilience.

The strengthening of this authority is in line with Bank Indonesia's efforts to support the acceleration of the development of sustainable digital financial economy as set out in the Blueprint of Indonesian Payment System 2025. Increasing the digitalization in financial sector will not only assist the sustainable growth of digital financial economy, but also lead to other impacts in the form of increasing in exposure to Cyber Risk. Cyber Incident that occurs within the financial sector may result in financial losses and disrupt the stability of Financial System.

As an effort to mitigate Cyber Risk, Bank Indonesia shall regulate and supervise KKS of Payment System Providers, Money Market and Foreign Exchange Participants, as well as other parties which are regulated and supervised by Bank Indonesia. This is done so that the Providers can develop KKS, among others, by implementing anticipatory, adaptive and proactive activities toward Cyber Risk. In addition, it is necessary to make efforts to strengthen the supervision and collaboration in the prevention and handling of Cyber Incident that has a systemic or non-systemic impact on the Financial System.

Based on this, it is necessary for Bank Indonesia to issue the Bank Indonesia Regulation on Information System Security and Cyber Resilience for Payment System Providers, Money Market and Foreign Exchange Market Participants, as well as Other Parties Regulated and Supervised by Bank Indonesia.

II. ARTICLE BY ARTICLE

Article 1

Sufficiently clear.

Article 2

Sufficiently clear.

Article 3

Sufficiently clear.

Article 4

Point a

The term “Clarity of role and responsibility” means clarity of roles and responsibilities of Providers in order to ensure that KKS has been managed effectively.

Point b

The term “Comprehensive strategy” means implementation of KKS strategy comprehensively.

Point c

The term “Cyber Risk management integrated with enterprise risk management” means integration of KKS in risk management so as to increase the effectiveness of control over dynamic Cyber Threat.

Point d

The term “Integration with KKS culture” means internalization of KKS awareness program through competency improvement and periodic socialization.

Point e

The term "Readiness to deal with Cyber Incidents" means anticipation of the possibility of Cyber Incident as well as the effective recovery of Cyber Incident.

Article 5

Point a

The scope of PJP shall refer to Bank Indonesia Regulation on Payment System and Bank Indonesia Regulation on PJP.

Point b

The scope of PIP shall refer to Bank Indonesia Regulation on Payment System and Bank Indonesia Regulation on PIP.

Point c

The scope of PUSK PUVA shall refer to Bank Indonesia Regulation on Money Market and Foreign Exchange Market.

Point d

The scope of Money Market Supporting Agency shall refer to Bank Indonesia Regulation on Money Market and Foreign Exchange Market.

Point e

The scope of Foreign Exchange Market Supporting Agency shall refer to Bank Indonesia Regulation on Money Market and Foreign Exchange Market.

Point f

The scope of Providers of Foreign Exchange Business Activities Other than Bank shall refer to Bank Indonesia Regulation on Foreign Exchange Business Activities Other than Banks.

Point g

Sufficiently clear.

Article 6

Sufficiently clear.

Article 7

Sufficiently clear.

Article 8

Sufficiently clear.

Article 9

Sufficiently clear.

Article 10

Section (1)

Point a

Sufficiently clear.

Point b

Third parties to include vendors in the Information System service sector.

Point c

The term "Management of fraud" means management of deception or fraud resulting from Cyber Vulnerability.

Section (2)

Sufficiently clear.

Section (3)

Sufficiently clear.

Article 11

Sufficiently clear.

Article 12

Section (1)

Sufficiently clear.

Section (2)

Cooperation with other parties shall be conducted among others with parties that have competence in auditing, Cyber-Risk management, and other sectors that support the implementation of KKS.

Article 13

Section (1)

Sufficiently clear.

Section (2)

The highest management to include the board of directors or other leaders of the highest management who are authorized and fully responsible for the management of the organization.

Section (3)

See the elucidation of Article 12 section (2).

Article 14

Sufficiently clear.

Article 15

Sufficiently clear.

Article 16

Sufficiently clear.

Article 17

Sufficiently clear.

Article 18

Section (1)

Positive behaviors in developing KKS among others are, maintaining the confidentiality of data and information, as well as accessing information safely through the official website.

Cyber Ethic in developing KKS culture, among others are, avoiding the violation of intellectual property rights in Cyber activities, as well as preventing the utilization of Cyber media as a means of spreading false information.

Section (2)

Sufficiently clear.

Section (3)

Point a

Sufficiently clear.

Point b

See the elucidation of Article 10 section (1) point b.

Point c

Sufficiently clear.

Section (4)

See the elucidation of Article 13 section (2)

Article 19

Sufficiently clear.

Article 20

Sufficiently clear.

Article 21

Sufficiently clear.

Article 22

Section (1)

Sufficiently clear.

Section (2)

Other means of information to include providers or communities that share Cyber intelligence.

Article 23

Sufficiently clear.

Article 24

Sufficiently clear.

Article 25

Sufficiently clear.

Article 26

Sufficiently clear.

Article 27

Point a

The term “Ensuring the security of internal party and third party at every stage of work cycle” means ensuring that internal party and third party possess, among others, competence, integrity and Cyber ethics, before, during, and after being employed by Providers.

Point b

Sufficiently clear.

Point c

Implementing the security configuration of Information System that is used to include:

1. control over logical and physical access;
2. software version update (update patch);
3. protection of devices that have the potential to become Cyber Vulnerability entry points (endpoint security); and
4. network segmentation.

Network segmentation to include internet network, intranet network and extranet network.

Article 28

Sufficiently clear.

Article 29

Section (1)

Point a

Sufficiently clear.

Point b

Sufficiently clear.

Point c

Sufficiently clear.

Point d

Malicious code shall refer to software, including computer programs or scripts that are created and sent with the aim of damaging apps system and/or information technology infrastructure.

Malicious code to include codes designed to steal data, damage files, deactivate system or spread malware.

Unauthorized code shall refer to any software, including computer program or scripts that are installed on apps system and/or information technology infrastructure without permission or authorization from Providers.

Point e

Sufficiently clear.

Section(2)

Sufficiently clear.

Article 30

Point a

Logical access to include username and password, authentication token and data communication network.

Physical access to include keys and access card, biometrics and security camera.

Point b

The activation of early warning system will be triggered if the threshold indicator is exceeded.

Point c

Cyber Vulnerability scanning, among others, is a penetration test, which is a test using a system of Providers and aims to break through the existing security system, in accordance with predetermined limits.

Article 31

Point a

Cyber activities may be recorded in a log system or event monitoring.

Point b

Sufficiently clear.

Article 32

Point a

Cyber-related Fraud shall refer to a fraud or deception resulting from a Cyber Vulnerability.

Point b

Sufficiently clear.

Point c

Sufficiently clear.

Article 33

Sufficiently clear.

Article 34

Sufficiently clear.

Article 35

Sufficiently clear.

Article 36

Sufficiently clear.

Article 37

Section (1)

Point a

Sufficiently clear.

Point b

Sufficiently clear.

Point c

Sufficiently clear.

Point d

Recovery time objective shall refer to the period required to recover apps system, information technology infrastructure, and/or critical services that may be received by Providers after a Cyber Incident.

Recovery point objective shall refer to the maximum amount of data loss that can be tolerated after a Cyber Incident.

Section (2)

Business continuity plan is policy and procedures which encompass a series of planned activities to ensure the continuity of

business and/or services of Providers in the event of abnormal circumstances and/or emergency.

Section (3)

Sufficiently clear.

Section (4)

Sufficiently clear.

Article 38

Sufficiently clear.

Article 39

Sufficiently clear.

Article 40

Sufficiently clear.

Article 41

Point a

Sufficiently clear.

Point b

Stakeholders to include internal party of Providers, customers of Providers, Bank Indonesia, the Financial Services Authority, and the State Cyber and Crypto Agency.

Huruc c

Sufficiently clear.

Article 42

Sufficiently clear.

Article 43

Sufficiently clear.

Article 44

Sufficiently clear.

Article 45

Sufficiently clear.

Article 46

Sufficiently clear.

Article 47

Sufficiently clear.

Article 48

Sufficiently clear.

Article 49

Sufficiently clear.

Article 50

Sufficiently clear.

Article 51

Sufficiently clear.

Article 52
Sufficiently clear.

Article 53
Sufficiently clear.

Article 54
Sufficiently clear.

Article 55
Sufficiently clear.

Article 56
Sufficiently clear.

Article 57
Sufficiently clear.

Article 58
Sufficiently clear.

Article 59
Sufficiently clear.

Article 60
Coordination of Bank Indonesia with authorities, agencies and/or Providers shall, among others is to conduct a Cyber Attack simulation in the financial sector.

Article 61
Section (1)
Sufficiently clear.
Section (2)
Sufficiently clear.
Section (3)
SRO shall play an active role as a liaison officer with Providers, among others, coordinating the preparation of proposal for a Cyber Attack simulation scenario in the financial sector.
Section (4)
Sufficiently clear.

Article 62
Sufficiently clear.

Article 63
Sufficiently clear.