REGULATION OF THE NATIONAL CYBER AND CRYPTO AGENCY
NUMBER 8 OF 2020
ON
SECURITY SYSTEM IN OPERATION OF ELECTRONIC SYSTEM

BY THE BLESSINGS OF ALMIGHTY GOD

HEAD OF THE NATIONAL CYBER AND CRYPTO AGENCY,

Considering : that in order to implement the provision of Article 24 section (4) of the Government Regulation of the Republic of Indonesia Number 71 of 2019 on Operation of Electronic System and Transaction, it is necessary to issue a Regulation of the National Cyber and Crypto Agency on Security System in Operation of Electronic System;

Observing :

1. Law Number 11 of 2008 on Electronic Information and Transaction (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843) as amended by Law Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transaction (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette Number 5952).
2. Government Regulation Number 24 of 2018 on Electronic Integrated Business Licensing Services (State Gazette of the Republic of Indonesia of 2018 Number 90, Supplement to the State Gazette of the Republic of Indonesia Number 6215);

3. Government Regulation Number 71 of 2019 on Operation of Electronic System and Transaction (State Gazette of the Republic of Indonesia of 2019 Number 185, Supplement to the State Gazette of the Republic of Indonesia Number 6400);
4. Presidential Regulation of the Republic of Indonesia Number 53 of 2017 on National Cyber and Crypto Agency (State Gazette of the Republic of Indonesia of 2017 Number 100) as amended by Presidential Regulation of the Republic of Indonesia Number 133 of 2017 on Amendment to Presidential Regulation of the Republic of Indonesia Number 53 of 2017 on National Cyber and Crypto Agency (State Gazette of the Republic of Indonesia of 2017 Number 277);
5. Presidential Regulation Number 95 of 2018 on Electronic Based Governmental System (State Gazette of the Republic of Indonesia of 2018 Number 182, Supplement to the State Gazette of the Republic of Indonesia Number 6215);
6. Regulation of the National Cyber and Crypto Agency Number 2 of 2018 on Organization and Work Procedures of National Cyber and Crypto Agency (State Bulletin of the Republic of Indonesia of 2018 Number 197);

HAS DECIDED:

To issue : REGULATION OF THE NATIONAL CYBER AND CRYPTO AGENCY ON SECURITY SYSTEM IN OPERATION OF ELECTRONIC SYSTEM.

CHAPTER I
GENERAL PROVISIONS

Article 1

In this Regulation Agency:

1. Electronic System means a series of electronic devices and procedures which function to prepare, collect, process, analyze, store, display, announce, transmit and/or disseminate electronic information.
2. Electronic System Operator means any person, state administrator, business entity and community who

provides, manages, and/or operates Electronic Systems independently or jointly to Electronic System users for their own needs and/or the needs of other parties.

3. Electronic System Operator for Public Scope means Electronic System operator by state administering agency or agency appointed by state administering agency.
4. Electronic System Operator for Private Scope means Electronic System Operator by persons, business entities and community.
5. Electronic System Operation means the use of Electronic Systems by state administrators, persons, business entities and community.
6. Information Security Management System (*Sistem Manajemen Pengamanan Informasi*), hereinafter referred to as SMPI, means the regulation of obligations for Electronic System Operators in the implementation of a risk-based information security management.
7. Information Security means the maintenance of confidentiality, authenticity, integrity, availability and non-repudiation of information.
8. Personal Data mean any data regarding a person that is identified and/or separately identifiable or combined with other information, either directly or indirectly through electronic and/or non-electronic systems.
9. Risk means an undesirable event or condition that can bring negative impacts on the achievement of the performance target of Electronic System services.
10. Information Security Management System Certification Provider, hereinafter referred to as Certification Provider means an Information Security audit agency that issues Information Security Management System Certificate.
11. Information Security Management System Certificate, hereinafter referred to as SMPI Certificate means written evidence provided by a Certification Provider to Electronic System Operators that have met the requirements.
12. Self-Assessment means an evaluation mechanism carried out independently by Electronic System Operators based on certain criteria.

13. Information Security Index (*Indeks Keamanan Informasi*), hereinafter referred to as Indeks KAMI means an evaluation tool to analyze the level of information security readiness in an organization.
14. Information Security Auditor (*Auditor Keamanan Informasi*) hereinafter referred to as ArKI means a person who has the competence to perform an Information Security audit.
15. Ministries or Agencies mean state administering agencies in charge of supervising and issuing regulations on their sectors.
16. Practitioner Experts hereinafter referred to as Experts, mean people who have the competency to implement SMPI.
17. National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*) hereinafter referred to as BSSN means a government agency that carries out government tasks in the cyber security sector.

Article 2

Security system in the Operation of Electronic System is conducted through SMPI.

Article 3

Security system in the Operation of Electronic System includes:

a. the scope of the Electronic System Operator for Public Scope and the Electronic System Operator for Private Scope;
b. Self-Assessment process and Electronic Systems category;
c. the implementation of SMPI which consists of:
   1) SMPI standards according to the category of Electronic Systems;
   2) preparation for implementing SMPI;
   3) implementation of SMPI by Electronic System Operators;
   4) issuance of certificates, certification reporting, and revocation of certificates;
d. guidance and supervision; and
e. sanction.

CHAPTER II
SCOPE OF ELECTRONIC SYSTEM OPERATORS

Article 4

This Regulation Agency regulates the implementation of SMPI by Electronic System Operators for Public Scope and Electronic System Operators for Private Scope.

Article 5

(1) The implementation of SMPI by the Electronic System Operators for Public Scope as referred to in Article 4 includes:
   a. agency; and
   b. provider appointed by the agency.

(2) The implementation of SMPI by the Electronic System Operator for Private Scope as referred to in Article 4 includes:
   a. Electronic System Operators that are regulated or supervised by ministries or agencies based on the provisions of legislation; and
   b. Electronic System Operators that has a portal, site, or application in the network through the internet which is used for:
      1) providing, managing, and/or operating the bidding and/or trade in goods and/or services;
      2) providing, managing, and/or operating financial transaction services;
      3) sending paid digital materials or content through the data network by downloading via a portal or website, sending via electronic mail, or via other applications to the user's device;
      4) providing, managing, and/or operating communication services including but not limited to instant messages, voice calls, video calls, electronic mails and online conversations in the form of digital platforms, networking services and social media;

5) search engine services, services for providing electronic information in the form of text, sound, images, animation, music, videos, films and games or a combination of parts and/or all of them; and/or

6) processing of Personal Data for operational activities serving the public related to electronic transaction activities.

CHAPTER III
SELF-ASSESSMENT PROCESS AND CATEGORY OF ELECTRONIC SYSTEM

Article 6

(1) The Electronic System category based on the principle of Risk consists of:

a. strategic Electronic Systems;

b. high-risk Electronic System; and

c. low-risk Electronic System.

(2) The strategic Electronic System as referred to in section (1) point a is an Electronic System that has a serious impact on public interests, public services, smooth running of the state, or state defense and security.

(3) The high-risk Electronic System as referred to in section (1) point b is an Electronic System with limited impact on the interests of certain sectors and/or regions.

(4) The low-risk Electronic System as referred to in section (1) point c is an Electronic System that is not included in section (2) and section (3).

Article 7

(1) The Electronic System Categorization as referred to in Article 6 section (1) is determined based on the Self-Assessment by the Electronic System Operator on its Electronic System.

(2) Self-Assessment Format as referred to in section (1) is contained in the Annex as an integral part of this Agency Regulation.

(3) Results of the Self-Assessment as referred to in section (1) are required to be reported to BSSN for verification.

(4) The verification as referred to in section (3) is carried out not later than 10 (ten) work days since the results report of the Self-Assessment is received.

Article 8

(1) In the event that the verification result as referred to in Article 7 section (4) states that the Electronic System owned by the Electronic System Operator is a Strategic Electronic System, then it should be issued by the Head of BSSN based on the results of coordination with the related Ministries or Agencies.

(2) In the event that the verification result as referred to in Article 7 section (4) states that the Electronic System owned by the Electronic System Operator is a high Electronic System and/or low Electronic System then it should be issued by the Head of BSSN.

(3) Every issuance made by the Head of BSSN as referred to in section (1) and section (2) is submitted to the Electronic System Operator and the related Ministries or Agencies.

CHAPTER IV
SMPI OPERATION

Part One
SMPI Standard Pursuant to Electronic System Category

Article 9

(1) Electronic System Operators implementing strategic Electronic Systems is obligated to apply:

a. SNI ISO/IEC 27001;

b. other security standards related to cybersecurity issued by BSSN; and

c. other security standards related to cybersecurity issued by the Ministries or Agencies.

(2) Electronic System Operator operating high-risk Electronic System is obligated to apply:

a. SNI ISO/IEC 27001 and/or other security standards related to cybersecurity issued by BSSN; and

b. other security standards related to cybersecurity issued by the Ministries or Agencies.

(3) Electronic System Operators operating low-risk Electronic Systems is obligated to apply:

a. SNI ISO/IEC 27001; or

b. other security standards related to cybersecurity issued by the BSSN.

(4) Other security standards related to cybersecurity as referred to in section (1) point b, section (2) point a, and section (3) point b are regulated by an Agency Regulation.

(5) Other security standards related to cybersecurity as referred to in section (1) point c and section (2) point b are in accordance with the provisions of legislation.

Article 10

In the event that standards as referred to in Article 9 section (1) point b and point c have not been issued, Electronic System Operator is obligated to implement the provisions of Article 9 section (1) point a.

Article 11

In the event that standards as referred to in Article 9 section (1) point b and point c have not been issued, the Electronic System Operator is obligated to implement the provisions of Article 9 section (1) point a.

Part Two
Preparation for SMPI Implementation

Article 12

(1) To prepare the implementation of SNI ISO/IEC 27001 as referred to in Article 9, the Electronic System Operator may conduct an assessment based on Indeks KAMI.

(2) The provisions regarding Indeks KAMI are carried out in accordance with the provisions of legislation.

Part Three
SMPI Implementation by Electronic System Operators

Article 13

(1) The implementation of SMPI is carried out independently by the Electronic System Operator.

(2) In implementing SMPI independently as referred to in section (1), Electronic System Operators employ human resources holding Indonesian citizenship.

(3) In implementing SMPI independently as referred to in section (1), Electronic System Operators may employ:

a. Experts holding Indonesian Citizenship; or

b. consulting company recognized by the BSSN.

Article 14

(1) In the event of no Experts holding Indonesian Citizenship as referred to in Article 13 section (3) point a, the Electronic System Operator may employ foreign Experts who are bound in a confidentiality agreement.

(2) In employing foreign Experts as referred to in section (1), Electronic System Operators are obligated to submit applications to work unit that carry out tasks and functions in the field of monitoring cybersecurity and crypto human resources not later than 14 (fourteen) work days prior to the signing of the employment contract.

(3) The application as referred to in section (2) is completed with the following documents:

a. Risk management related to the use of foreign Experts;

b. 1 (one) 4x6 photograph taken within the past 1 (one) month;

c. copy of passport;

d. curriculum vitae;

e. draft employment contract;

f. copy of evidence or information regarding expertise qualifications or expertise certification in the field of Information Security;

g. copy of temporary stay permit card or permanent stay permit card issued by the authorized agency; and

h. copy of expatriate work permit issued by the authorized agency.

(4) The work unit that carries out tasks and functions in the field of monitoring cybersecurity and crypto human resources conducts assessment on foreign Experts within 14 (fourteen) work days.

(5) The BSSN may issue a license to employ foreign Experts to the applying Electronic System Operator if the proposed foreign Experts has met the assessment criteria.

Article 15

(1) Consulting company as referred to in Article 13 section (3) point b must:

a. be in the form of an Indonesian legal entity;

b. be domiciled in Indonesia; and

c. have an implementer team consisting of at least 1 (one) Indonesian national implementer.

(2) The implementer as referred to in section (1) point c is a person who has competence in implementing SMPI.

Article 16

(1) A candidate for consulting company applies for recognition as SMPI consulting company to the Head of BSSN.

(2) The application for recognition as referred to in section (1) is accompanied by the following documents:

a. application letter;

b. deed of establishment of the company;

c. trading business license in the main trade sector of information technology consulting services;

d. certificate of domicile; and

e. list of members of the implementer team.

(3) The format of the application letter as referred to in section (2) point a is contained in the Annex as an integral part of this Agency Regulation.

Article 17

(1) The work unit that carries out the duty and function in the field of consulting company certification verifies the application for recognition as referred to in Article 16 section (2).

(2) In the event of the verification as referred to in section (1), the application documents are declared complete, the Head of BSSN will give recognition to the consulting company as SMPI consulting company not later than 14 (fourteen) work days after the application documents are declared complete.

(3) In the event of the verification as referred to in section (1), the application documents are declared incomplete, the Head of BSSN will return the application documents to the candidate for consulting company to be completed.

Article 18

(1) The recognition as referred to in Article 17 section (2) is given in the form of a certificate of recognition of the SMPI consulting company.

(2) The certificate of recognition of the SMPI consulting company as referred to in section (1) is valid for a period of 5 (five) years.

(3) A consulting company that has obtained a certificate of recognition of an SMPI consulting company as referred to in section (1) is included in the list of SMPI consulting company.

(4) The format for the certificate of recognition of the SMPI consulting company as referred to in section (1) is contained in the Annex as an integral part of this Agency Regulation.

Article 19

(1) The certificate of recognition of the SMPI consulting company as referred to in Article 18 is declared invalid in the event that:

    a. the certificate of recognition of the SMPI consulting company has expired;

    b. the consulting company violates the legislation; or

c. the consulting company is declared bankrupt in accordance with the legislation.

(2) The consulting company whose certificate of recognition is invalid as referred to in section (1) is removed from the list of SMPI consulting companies.

Article 20

In the event that the certificate of recognition of the SMPI consulting company has expired, the consulting company applies for re-recognition by submitting the documents in accordance with the provisions in Article 16 section (2).

Article 21

(1) A candidate for implementer submits an application for SMPI implementer registration certificate to the Head of BSSN.

(2) Application for registration certificate as referred to in section (1) is accompanied by the following documents:

a. application letter;

b. at least Bachelor Degree;

c. curriculum vitae;

d. certificate of competency in the field of Information Security;

e. certificate of competency as an implementer of SNI ISO/IEC 27001;

f. document stating a period of work experience in the field of information technology, especially in the field of Information Security implementation; and

g. copy of identity card.

(3) The format of the application letter as referred to in section (2) point a is contained in the Annex as an integral part of this Agency Regulation.

Article 22

(1) The work unit that carries out duty and function in the field of monitoring cybersecurity and crypto human resources verifies the application as referred to in Article 21 section (2).

(2) In the event of the verification as referred to in section (1), the application documents are declared complete, the Head of BSSN issues a SMPI implementer registration certificate not later than 14 (fourteen) work days after the application documents are declared complete.

(3) In the event of the verification as referred to in section (1), the application documents are declared incomplete, the Head of BSSN returns the application documents to the candidate for implementer to be completed.

(4) SMPI implementer registration certificate as referred to in section (2) is valid for a period of 5 (five) years.

(5) Implementer who have obtained the SMPI implementer registration certificate as referred to in section (2) is included in the SMPI implementer list.

(6) Format of SMPI implementer registration certificate as referred to in section (2) is contained in the Annex as an integral part of this Agency Regulation.

Article 23

(1) SMPI implementer registration certificate as referred to in Article 22 is declared invalid if:

a. SMPI implementer deceases;

b. SMPI implementer registration certificate has expired; or

c. SMPI implementer violates the legislation.

(2) Implementers whose SMPI implementer registration certificates are not valid as referred to in section (1) are removed from the SMPI implementer list.

Article 24

In the event that the SMPI implementer registration certificate has expired, the implementer applies by submitting the documents in accordance with the provision in Article 21 section (2).

Article 25

(1) A consulting company assigns an implementer team to assist the implementation of SMPI for Electronic System Operators.

(2) The implementer team as referred to in section (1) reports the results of SMPI implementation to the assigning consulting company.

Part Four
Certificate Issuance, Certification Reporting, and SMPI Certificate Revocation

Article 26

SMPI certification is carried out by a Certification Provider that is recognized by BSSN.

Article 27

The provisions regarding the recognition of the Certification Provider as referred to in Article 26 are in accordance with the legislation.

Article 28

(1) SMPI certificates are issued by the Certification Provider.

(2) SMPI certificate as referred to in section (1) is valid for a maximum period of 3 (three) years from the date of issuance.

(3) SMPI certificates must be renewed by the Electronic System Operator not later than 3 (three) months before the validity period ends.

Article 29

SMPI certification must be carried out in accordance with the Electronic System Operation process by taking into account the Electronic System category as referred to in Article 6.

Article 30

(1) The Certification Provider assigns ArKI team to conduct SMPI audits on Electronic System Operators.

(2) ArKI team as referred to in section (1) reports the audit results to the assigning Certification Provider.

(3) Certification Provider reviews the audit results reported by ArKI team.

(4) Certification Provider issues SMPI Certificate for Electronic System Operators that have met the standards as referred to in Article 9.

Article 31

(1) Certification Provider is obligated to submit reports on the results of SMPI certification periodically at least 2 (two) times in 1 (one) year to the Head of BSSN.

(2) The report as referred to in section (1) covers at least:
   a. Electronic System Operator data applying for certification;
   b. Electronic System Operator data that has obtained an SMPI Certificate;
   c. Electronic System Operator data whose certificate ownership has been revoked;
   d. executive summary containing:
      1) condition of organization;
      2) organizational structure;
      3) major findings and minor findings;
      4) recommendations;
      5) corrective action; and
      6) audit follow-up;
      e. changes to the list of the ArKI team; and
      f. changes to the list of the certification decision-making team.

(3) Format of the report as referred to in section (2) is contained in the Annex as an integral part of this Agency Regulation.

Article 32

Certification Provider is obligated to report changes to the ArKI team and the certification decision-making team to the Head of BSSN not later than 2 (two) work days before ArKI team carries out the Information Security audit.

Article 33

Certification Provider is obligated to carry out a surveillance audit at least 1 (one) year and a special audit in the event of an incident against each certified Electronic System.

Article 34

(1) If the results of the surveillance audit as referred to in Article 33 do not meet the standards as referred to in Article 9, a maximum period of 90 (ninety) calendar days is given to comply with the standard.

(2) If after 90 (ninety) calendar days have not been fulfilled, Certification Provider may revoke the related SMPI Certificate.

(3) The revocation as referred to in section (1) is required to be reported by Certification Provider to Head of BSSN not later than 2 (two) work days after the revocation is carried out.

CHAPTER V
GUIDANCE AND SUPERVISION

Article 35

(1) BSSN provides guidance to the implementation of SMPI certification for:

a. Electronic System Operator;

b. Experts;

c. consulting company; and

d. Certification Provider.

(2) The guidance as referred to in section (1) may include counseling, training, technical guidance and/or assistance.

Article 36

(1) BSSN supervises Electronic System Operators, Certification Provider, consulting company and Experts.

(2) The supervision as referred to in section (1) is carried out through monitoring, evaluation, tracing and examination.

CHAPTER VI
SANCTIONS

Article 37

(1) The Head of BSSN imposes administrative sanctions on Electronic System Operators who violate the provisions as referred to in Article 7 section (3), Article 9 section (1), Article 9 section (2), and Article 9 section (3), Article 10, Article 11, Article 14 section (2), and Article 43 section (2).

(2) Administrative sanctions as referred to in section (1) are in the form written reprimands.

(3) Written reprimands as referred to in section (2) are given upon the findings of a violation.

Article 38

Violation of the provisions as referred to in Article 31 section (1), Article 32, Article 33, Article 34 section (3) is subject to administrative sanctions in the form of:

a. written reprimands;

b. suspension of certificate of recognition of Certification Provider; or

c. revocation of the certificate of recognition of Certification Provider.

Article 39

(1) A written reprimand as referred to in Article 38 point a is given in the form of a letter containing:

    a. details of violations;

    b. obligation to carry out corrective action; and

    c. the next sanction to be imposed.

(2) The written reprimand as referred to in section (1) is given 1 (one) time.

(3) The written reprimand as referred to in section (1) must be followed up not later than 15 (fifteen) work days after the written reprimand is issued.

(4) The written reprimand as referred to in section (3) is issued by the National Cyber and Crypto Agency.

Article 40

(1) The suspension of the certificate of recognition of Certification Provider as referred to in Article 38 point b is given in the form of a letter to Certification Provider that ignores the written reprimand as referred to in Article 39 section (3).

(2) The suspension as referred to in section (1) is given for a period of 15 (fifteen) work days.

(3) The suspension as referred to in section (2) is issued by the National Cyber and Crypto Agency.

Article 41

(1) The suspension of the certificate of recognition of Certification Provider as referred to in Article 40 is revoked if the Certification Provider heeds the written reprimand within the period as referred to in Article 39 section (3).

(2) The revocation of the suspension as referred to in section (1) is stated in the form of a letter issued by the National Cyber and Crypto Agency.

Article 42

(1) The revocation of the certificate of recognition of Certification Provider as referred to in Article 38 point c is given to the SMPI Certification Provider which has not made corrective action until the expiration of the suspension period as referred to in Article 40 section (2).

(2) The revocation of the certificate of recognition of Certification Provider as referred to in section (1) is carried out by issuing a decision to revoke the certificate of recognition of the Certification Provider.

(3) The decision to revoke the certificate of recognition of Certification Provider as referred to in section (2) is issued by the Head of the National Cyber and Crypto Agency.

CHAPTER VII
TRANSITIONAL PROVISIONS

Article 43

(1) SMPI certificates that have been issued prior to the promulgation of this Agency Regulation are declared to remain effective.

(2) Electronic System Operators who have used foreign Experts before this Agency Regulation comes into force are obligated to report them to the work unit that carries out duty and functions in the field of monitoring cybersecurity and crypto human resources not later than 30 (thirty) days after this Agency Regulation is promulgated.

(3) The report as referred to in section (2) is completed with:

a. Risk management documents related to the use of foreign Experts;

b. 1 (one) 4x6 photograph taken within the past 1 (one) month;

c. copy of passport;

d. curriculum vitae;

e. employment contract document;

f. copy of evidence or information regarding expertise qualifications or expertise certification in the field of Information Security;

g. copy of temporary stay permit card or permanent stay permit card issued by the authorized agency; and

h. copy of expatriate work permit issued by the authorized agency.

(4) Certification Provider, consulting companies and Experts that have received recognition from the minister in charge of communication and information are still recognized as long as they do not conflict with this Agency Regulation.

CHAPTER VIII
CLOSING PROVISIONS

Article 44

This Agency Regulation comes into force on the date of its promulgation.

In order that every person may know hereof, it is ordered to promulgate this Agency Regulation by its placement in State Bulletin of the Republic of Indonesia.

Issued in Jakarta
on 6 November 2020

HEAD OF THE NATIONAL CYBER
AND CRYPTO AGENCY,

signed

HINSA SIBURIAN

Promulgated in Jakarta
on 23 November 2020

DIRECTOR GENERAL OF LEGISLATION OF
MINISTRY OF LAW AND HUMAN RIGHTS
OF THE REPUBLIC OF INDONESIA

signed

WIDODO EKATJAHJANA

STATE BULLETIN OF THE REPUBLIC OF INDONESIA OF 2020 NUMBER 1375

Jakarta, 28 April 2021
Has been translated as an Official Translation
on behalf of Minister of Law and Human Rights
of the Republic of Indonesia
DIRECTOR GENERAL OF LEGISLATION,

DIREKTORAT JENDERAL
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA RI
PENGAYOMAN
PERATURAN PERUNDANG-UNDANGAN

WIDODO EKATJAHJANA

ANNEX TO
REGULATION OF THE NATIONAL CYBER AND CRYPTO AGENCY
NUMBER 8 OF 2020
ON
SECURITY SYSTEM IN OPERATION OF ELECTRONIC SYSTEM

SELF-ASSESSMENT FORM OF ELECTRONIC SYSTEM CATEGORIZATION

Electronic System Category				
Company name:				
Type of business:				
[Electronic System Category] Low-risk; High-risk; Strategic		**Status**	**Score**	**Evidence**
#	**Agency Characteristics**			
1,1	The investment value of the installed electronic system [A] More than Rp30 Billions [B] More than Rp3 Billions to Rp30 Billions [C] Less than Rp3 Billions			
1,2	Total annual operating budget allocated for management of Electronic Systems [A] More than Rp10 Billions [B] More than Rp1 Billion to Rp10 Billions [C] Less than Rp1 Billion			

1,3	Having compliance obligations with certain Regulations or Standards [A] National and international regulations or Standards [B] National Regulations or Standards [C] No specific Regulations			
1,4	Using special cryptographic techniques for information security in Electronic Systems [A] A special cryptographic technique certified by the State [B] Cryptographic techniques in accordance with industry standards, publicly available or self-developed [C] No use of cryptographic techniques			
1,5	Number of Electronic System users [A] More than 5,000 users [B] 1,000 to 5,000 users [C] Fewer than 1,000 users			
[Electronic System Category] Low-risk; High-risk; Strategic		**Status**	**Score**	**Evidence**

1,6	Personal data managed by Electronic Systems [A] Personal data related to other Personal Data [B] Personal data of an individual nature and/or personal data related to ownership of a business entity [C] No personal data			
1,7	The level of classification/ criticality of Data in Electronic Systems, relative to the threat of attacks or breaches of information security [A] Top Secret [B] Confidential and/or Restricted [C] Unclassified			
1,8	The level of criticality of the processes that exist in Electronic Systems, relative to the threat of attacks or breaches of information security [A] Processes that risk disrupting the life of the people and having a direct impact on public services [B] Processes that risk disrupting the life of the people and having an indirect impact [C] Processes that only impact the company's business			

1,9	Impact of Electronic System failure [A] Unavailability of public services on a national scale or compromise to the defense and security of the country [B] Unavailability of public services in 1 or more provinces [C] Unavailability of public services in 1 regency/municipality or more			
[Electronic System Category] Low-risk; High-risk; Strategic		**Status**	**Score**	**Evidence**
1,10	Potential loss or negative impact from the incidents of Electronic System information security breaches (sabotage, terrorism) [A] Causing fatalities [B] Limited to financial loss [C] Resulting in temporary operational disruption (harmless and not financially detrimental)			
Total Score				
Electronic System Category				

Description:

Status	Score
A	5
B	2
C	1

Assessment Conditions:

Electronic System Category	Strategic	High-Risk	Low-Risk
Total Score	36 - 50	16 - 35	10 – 15

I, the undersigned, declare that the above data is filled in accordance with the actual situation.

(Place, date month year)
HEAD OF COMPANY

(Name)
(Position)

FORMAT OF APPLICATION LETTER FOR RECOGNITION AS CONSULTING COMPANY

[***Name*** of Consulting Company]
[***Address*** of the Consulting Company]
[***Telephone Number and E-Mail*** of the Consulting Company]

[Name of City, Date]

Number :
Type : Unclassified
Attachment :
Subject : Application for Recognition as a Consulting Company of SMPI

Dear Sir/Madam,

Head of National Cyber and Crypto Agency
Jl. Harsono RM. No. 70, Ragunan
In -
South Jakarta

We hereby submit an application for recognition as a SMPI Consulting Company that we organize. For your consideration, we hereby submit the following data:

Name of Consulting Company : [*Filled with the name of the Consulting Company*]
Form of Consulting Company : [*Legal Entity*]
Address of Entity : [*Write down the Entity's full address*]
(*Pursuant to the Certificate of Domicile*)
[*Name of Building, Floor*]
[*Street name followed by Lot Number, etc*]
[*City, Province, Zip Code*]

To complete this application, we attach the supporting documents as follows:

1. Deed of establishment of the company;
2. Trading business license in the main trade sector of information technology consulting services;

3. Certificate of domicile; and
4. list of members of the implementor team.

In witness whereof, this letter is made, thank you for your attention.

[**Head** of Consulting Company],

(..)

FORMAT OF CERTIFICATE OF RECOGNITION OF CONSULTING COMPANY OF INFORMATION SECURITY MANAGEMENT SYSTEM

NATIONAL CYBER AND CRYPTO AGENCY

CERTIFICATE OF RECOGNITION OF CONSULTING COMPANY OF INFORMATION SECURITY MANAGEMENT SYSTEM

NUMBER:

The National Cyber and Crypto Agency hereby grants recognition to:

[***Name*** of the Consulting Company]
[***Address*** of the Consulting Company]

Who has fulfilled requirements as a Consulting Company of Information Security Management System.

This Certificate of Recognition is valid from the date of issuance and ends on the date ...

Issued in Jakarta,
Dated .... 20 ....
On behalf of The Head of National Cyber and Crypto Agency
Deputy of ...,

Signed

[Name]

FORMAT OF APPLICATION LETTER OF FOR THE SMPI IMPLEMENTOR REGISTRATION CERTIFICATE

Latest 4 x 6
Photograph

Dear Sir/Madam.
Head of National Cyber and Crypto Agency
In
Jakarta

The undersigned:

Name : [*Name*]
NIK : [*Residence Identity Card Number*]
Phone Number : [*Phone number 1, phone number 2, etc.*]
E-mail : [*E-mail address 1, e-mail address 2, etc.*]
Address : [*Write down full address according to domicile*] [*Street name followed by Lot Number, etc.*] [*City, Province, Zip Code*]

Hereby submit an application for SMPI Implementor Registration Certificate. Herewith, we also convey complete documents in hardcopy and/or softcopy form.

We agree to submit an application for SMPI Implementor Registration Certificate and we have completed the required documents and/or data and are responsible for the accuracy of the said documents and/or data.

[Name of City, Date Month Year]
Applicant

[Name]

FORMAT OF SMPI IMPLEMENTOR REGISTRATION CERTIFICATE

NATIONAL CYBER AND CRYPTO AGENCY

SMPI IMPLEMENTOR REGISTRATION CERTIFICATE

Registration Number	:	[***SMPI Implementor Registration Number***]
Name	:	[***Name of Implementor***]
Competence	:	[***Competence of Implementor***]
Date of Stipulation	:	[***Date/Month/Year***]
Valid until	:	[***Date/Month/Year of Expiry***]

On behalf of The Head of National Cyber and Crypto Agency
Deputy of ....,

signed

(Name)

Latest 4 x 6 Photograph

**If any errors, this document will be revised accordingly.*

FORMAT OF CERTIFICATION PROVIDER REPORT ON CERTIFICATION RESULTS OF INFORMATION SECURITY MANAGEMENT SYSTEM

CHAPTER I INTRODUCTION

A. Background
B. Purpose
C. Scope
D. Goals
E. Output
F. Expected results (*Outcome*)
G. Outline

CHAPTER II REPORT OF ACTIVITIES

A. Data of electronic system operators applying for certification (including audit scope)
B. Data of electronic system operators obtaining information security management system certificate
C. Data of electronic system operators whose certificate ownership has been revoked
D. Executive summary
    1. Conditions of Organization
    2. Organizational Structure
    3. Major Findings and Minor Findings
    4. Recommendations
    5. Corrective Action
    6. Audit Follow-Up
E. Changes to the list of the of ArKI team
F. Changes to the list the of certification decision-making team

CHAPTER III CLOSING

[*Head of the Provider*],

signed

[*Name of the Provider*]

HEAD OF THE NATIONAL CYBER AND CRYPTO AGENCY,

signed

HINSA SIBURIAN