CIIP Guidelines
Ver.3.0

The 9th ASEAN-Japan Information Security Policy Meeting
October 20th, 2016

Contents

Document change history

Revision date	Summary of changes
20th October 2016	The 3rd edition (Ver.3.0) was acknowledged at the 9th ASEAN-Japan Information Security Policy Meeting.
15th October 2015	The 2nd edition (Ver.2.0) was proposed at the 7th ASEAN-Japan Information Security Policy Meeting. The Section 2.1 “Preparation for development of CIIP policies” and Section 2.7 “Cyber Exercises” are included.
8th October 2014	The 1st edition (Ver.1.0) was acknowledged by the 7th ASEAN-Japan Information Security Policy Meeting.

CIIP guidelines

Introduction

The Critical Information Infrastructure Protection (CIIP) guideline is drafted by the CIIP expert panel established as part of the ASEAN-Japan cooperation on CIIP that was adopted in the ministerial statement at the ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation on September 12th and September 13th, 2013. The first edition of the CIIP guidelines reflects the discussions at the CIIP expert panel meetings in Kuala Lumpur (February, 2014) and in Bangkok (May, 2014) and the 6th Government Network Security Workshop in Singapore on August 27th and 28th, 2014.

The second edition is a reflection of continuous discussions in the ASEAN-Japan CIIP Working Group (formerly the CIIP expert panel) in Jakarta (February, 2015), in Hanoi (April, 2015) and at the 1st ASEAN-Japan Information Security Joint Working Group Meeting in Tokyo (June, 2015), and the revised part is especially focused on the preparation stage of the development of CIIP policies.

The third edition reflects the discussion in the ASEAN-Japan CIIP Working Group in Bandar Seri Begawan (February, 2016), in Hanoi (May, 2016) and at the 2nd ASEAN-Japan Information Security Joint Working Group Meeting in Bangkok (July, 2016)

1. Outline/Overview

1-1 Purpose of the guidelines

a) These guidelines are intended to be used as a reference or checklist for the relevant governments and/or regulators of ASEAN Member States to develop basic CIIP policies for their various critical sectors.

b) These guidelines explain the fundamental ideas of CIIP with regards to the minimum protection requirements of and roles of the governments and/or regulators. It also provides basic ideas and processes with which the relevant governments and/or regulators for the CII sector can assist CII operators to understand the significance of CIIP, as well as to help with the implementation of measures for CIIP.

c) The outlines of cyber exercises and the CIIP best practices of leading ASEAN Member States are attached in the appendix for reference.

1-2 Intended users

a) The intended users of these guidelines are mainly policy makers in ministries or agencies that regulate CII industries in each ASEAN Member State.

1-3 Fundamental ideas of CII

a) In these guidelines, CII is defined as follows:
"Information infrastructures whose failure or limited operation due to natural or man-made disasters would surely cause tremendous impact on the vast majority of citizens"

b) "Tremendous impact on the vast majority of citizens" means not only direct damage due to CII failure but also indirect damage caused by the effect of CII's failure on other information infrastructures which are highly dependent on the CII based on formal impact assessment.

c) 'CII owner/operator' in this guideline refers to the owner of the CII as well as the service provider operating the CII.

1-4 Significance of CIIP

1-4-1 Purpose of CIIP

a) In order to continuously provide services using CII and to avoid serious effects on public welfare and socioeconomic activities caused by outages of the information technology (IT) supporting the CII resulting from cyber-attacks or other causes, all stakeholders concerned should protect CII by taking proactive actions to minimize the risk of the IT outages and by ensuring prompt recovery from the outage should one occur.

1-4-2 Fundamental issues and concerns of CIIP

a) When providing necessary guidelines and support with regards to information security measures, the relevant governments and/or regulators for the CII sector should take into consideration the situation in each country, as well as the size and capability of each CII owner/operator.

b) If the governments and/or regulators request the same level of implementation of measures regardless of the size of the CII owners/operators, it may overburden SME operators and negatively affect their business viability.

c) It is preferable that all stakeholders concerned, including the governments and/or regulators and each CII owner/operator, periodically check the progress of their own measures and policies as a part of the initiative to accurately recognize the current CIIP circumstances, and assess the achievement of the goals of the measures. In addition, it is recommended that all stakeholders take the effort to understand the progress of similar efforts by other parties and to establish cooperation with them.

d) In addition to the aforementioned measures, it is important that the governments and/or regulators and the CII owners/operators recognize the need for the following measures to ensure effective implementation of the measures:

- Identify information infrastructure that is required by critical public services. Specifically, determine which function is categorized as CII and the CII owners/operators, and specify the cyber risk sources which may affect the CII.
- Conduct assessments of the cyber risk sources and set forth measures and their priorities to address those risks. Specifically, evaluate each cyber risk source stated above based on the level of impact and the feasibility of establishing mitigation measures, prioritized according to the severity of impact.
- Establish the plan for implementation of measures, in line with the CIIP policies, and monitor the implementation of the measures.
- Evaluate the effectiveness of the measures, including the incident response capability, incident management plans and the information sharing scheme amongst relevant stakeholders through exercises and training.

1-5 Definition of terms

The definition of terms in these guidelines is based on international standards such as ISO 27001:2013, ISO 31000:2009, and ISO 22301 unless otherwise explicitly defined in the guideline.

2. Role of Governments and/or Regulators in CIIP

2-1 Preparation for development of CIIP policies

a) It is preferable for countries developing CIIP policies to conduct necessary preparation before starting the development process.

b) The preparation should, at least, include the following activities:

- To research current status of CIIP measures in the country

- To research current status of CIIP measures in foreign countries
- To research generally accepted International standards (e.g. ISO standards)
- To gather stakeholders' opinions
- To evaluate possible cyber risks regarding CII in their own country
- To identify critical business functions and their supporting critical IT resources that should be protected[i]
- To prioritize available resources to deal with the possible cyber risks

2-2 Establishment of information security policy or strategy

a) It is preferable for the governments to establish a national policy or strategy in which the basic ideas of CIIP are systematically organized.

b) It is preferable to perform Plan-Do-Check-Act (PDCA) cycle and regular periodical review (preferably, at least, annually) on this policy or strategy to ensure that the policy or strategy is not outdated due to changes to the internal or external environment such as emerging new cyber risks and technologies. If there are issues, the governments are expected to revise the policy or strategy in response to such changes.

Examples of items to be included in the policy or strategy are as follows:

- Purpose of CIIP
- Goals of the CIIP strategy
- Definitions of designated CII
- Items concerning governance
- Prioritized areas of measures to improve CIIP
- Outlines of CIIP measures

2-3 Establishment of guidelines for security standards

a) To achieve the goals described in the policy or strategy, it is desirable for each CII owner/operator to establish CIIP security standards according to the features of each industry.

b) In this context "security standards" means a document(s) which describes the necessary or preferable level of information security measures for the industries according to the features of each industry.[ii]

c) It is preferable for the governments and/or regulators to establish security standards or guidelines if the governments and/or regulators themselves are the owners of the CII. In the case that the CII owners/operators are private entities, the governments and/or regulators are expected to establish basic guidelines on which each industry can base their own safety standards, while adhering to international standards.

d) Examples of items to be included in these guidelines for the CII owners/operators are as follows:

- ➢ Purpose of the security standards
- ➢ Scope of the security standards
- ➢ Recommended items to be included in the security standards, and so forth.
- ➢ Practical/appropriate methods for satisfying security standards such as using a certification scheme.

e) In addition to the policy or strategy, items included in the security standards may also be changed according to variations in the internal or external environment such as emergence of new technology and changes in trends in certification systems based on international standards. Therefore, it is preferable for the governments and/or regulators to periodically (preferably, at least, annually) monitor these changes by conducting interviews with CII owners/operators about the situation and issues they are facing, and revise the guideline as necessary in the case there are significant changes in circumstances.

2-4 Establishment of governance structure and identifying stakeholders

2-4-1 Establishment of governance

a) To establish a governance system necessary to implement the strategy set forth in 2-2, the following items should be considered:

- ➢ Clarification of the roles and scope of responsibilities of government agencies involved.

  For example it is preferable to clarify following points:

  - ✓ Coordinating Ministry/Agency and the Chief Executive Officer
  - ✓ Ministry/Agency responsible for establishing strategies
  - ✓ Ministry/Agency controlling or regulating major CII industries.
  - ✓ Ministry/Agency which monitors the implementation status of the strategies, and so forth.

- ➢ Clarification of the decision making process

  For example it is desirable to clarify the following points:

- ✓ Decision making bodies(Primary responsible office) and person, as well as scope of responsibility
- ✓ Responsible officer in each organization (eg. Cyber executive or Chief Information Security Officer (CISO))
- ✓ Participants in decision making
- ✓ Decision making process and related matters including the name of the meeting, the procedure of holding a meeting, and others

2-4-2 Roles and Responsibilities of stakeholders

a) Stakeholders shall be specified in the CII industries as defined above.

- ➢ Clarification of stakeholders

  Examples of stakeholders to be specified are as follows:

  - ✓ CII owners
  - ✓ Service provider operating CII
- ➢ The roles of each stakeholder
  - ✓ Information sharing
  - ✓ Roles in CIIP, including cyber risk recognition, implementation of measures, participation in exercises and so forth

2-5 Establishment of an information sharing scheme between the governments and/or regulators and private sector

-It is preferable to consider a two-way communication system between the governments and/or regulators and private sector;

a) As for information sharing from private sector to the governments and/or regulators, there are two possible approaches (i) Laws and regulations basis and (ii) voluntary basis.

b) With (i) laws and regulations basis, the private sector should share information with the governments and/or regulators according to legal and regulatory requirements. The benefit to the governments and/or regulators is that necessary information is received at the right time, but it also has the disadvantage in that the private sector may protest against the government regulations. It may be necessary for the governments and/or regulators to carefully consider the cyber risks they are facing, effectiveness of the information to be gathered, and accountability.

c) With (ii) voluntary basis, the benefits and disadvantages are reversed. The governments and/or regulators can offer support to encourage the private sector to share information, such as opportunities for information sharing with the private sector.

d) For information sharing from governments and/or regulators to the private sector, for example, in order to evoke attention from the CII owners/operators, or to encourage them to make necessary preparations, the governments and/or regulators could gather necessary information and provide it to the CII owners/operators.

2-6 IT security crisis management

2-6-1 Incident handling

a) It is important for the governments and/or regulators to develop capability to detect cyberattacks against the governmental organizations, and encourage CII owners/operators to develop their own cyberattacks detection capability.

b) It is important for the governments and/or regulators to take necessary measures to protect their critical business functions, and require CII owners/operators to take appropriate measures according to best practices, for example:

- Access control
- Raising awareness and training
- Ensure data security
- Establish data protection procedures
- Anti-malware controls
- DoS / DDoS mitigation
- APT detection
- Establish monitoring systems
- Establish computer security incident response procedures

c) It is important for the governments and/or regulators to provide timely necessary information to relevant persons/organizations when there is an incident which may jeopardize governments or CII owners/operators to continue their critical business functions. The governments and/or regulators should be careful not to reveal unnecessary information to public, or irrelevant organizations so as not to cause overreaction or panic for the incident. Media statements should be prepared in advance to be delivered by a designated spokesperson.

d) It is important for the governments and/or regulators to prepare pool of technical experts to deal with cyber incidents, and dispatch them to the organizations under attack if necessary.

2-6-2 Disaster recovery and Business Continuity Planning (BCP)

a) It is important for the governments and/or regulators to prepare disaster recovery plans in order to recover all the systems and services affected by the cyber incidents as soon as possible, and encourage CII owners/operators to do the same.

b) Especially for their critical business functions identified in the section 2-1-b), it is important for the governments and/or regulators to develop business continuity plans in case there is a strong possibility the incident jeopardizes continuity of critical business functions. It is important for the governments and/or regulators to encourage CII owners/operators to develop their own business continuity plans for their critical business functions as well.

c) For more details of BCP, see Appendix 2.

2-7 Cyber exercise

2-7-1 Significance of cyber exercise

a) It is important to conduct cyber exercises to allow governments and/or regulators to confirm the effectiveness of the information sharing system mentioned in section 2-5, and also address the issues and areas to be improved in the current cyber incident response and management framework.

2-7-2 Government support for industry-level exercises in the private sector

a) If private sector doesn’t sufficiently understand the significance of CIIP, or doesn’t have enough capability to plan and manage cyber exercises by themselves, the governments and/or regulators should at first enlighten them, and if necessary, should prepare the basic scenario and exercise.

b) On the other hand, in countries with advanced cyber security level, there may be some industries in which domestic or global industry-level cyber exercises have been already conducted. In such case, it may be possible to have them manage cyber exercises themselves in order to increase their capability to take countermeasures for any incidents, and governments and/or regulators may provide a certain level of guidance and scenarios.

c) The governments and/or regulators should consider appropriate support based on the situation in its own country and industry.

2-7-3 Government support for cross-industry exercises in the private sector

a) It is preferable to conduct cross-industry exercises among the highly interdependent industries after careful interdependency analysis. “Highly interdependent” means if production or services in a certain company or industry stop, it affects other companies or industries such as a supply chain or the settlement system in financial industries.

b) As many industries may participate in the cross-industry exercises, participants have to discuss scenarios and detailed plans of exercises in advance. This is one way for governments and/or regulators to give support by providing opportunities for discussion or fundamental information to build a scenario so that the private sector can smoothly conduct cyber exercises.

c) The governments and/or regulators should consider the situation in its own country and industry, and consider appropriate support, as well as industry-level exercises.

2-8 Awareness-raising activities for CII owners/operators

a) In order to improve the level of CIIP in the private sector, it is important to deepen the understanding of basic guidelines, its significance, and the content of safety standards established by the governments and/or regulators, and the related international standards.

b) It is also important to promote awareness-raising activities among the private sector by conducting publicity activities.

2-9 ASEAN regional partnership

a) As information technology is advancing, regional partnership becomes much more important to handle cyber threats. It is preferable for governments and/or regulators of ASEAN Member States to establish and strengthen the regional partnership in consideration of this situation.

b) For example, strengthening information sharing systems by establishing a POC (Point of Contact) in the ASEAN region, and conducting periodical meetings. It is also helpful to periodically conduct cyber exercises in the area and check the effectiveness of information sharing.

Appendix:

1. Outline of Cyber Exercises
2. Business Continuity Planning
3. List of References on Best Practices of CIIP

[i] Critical IT resources means IT resources that have high interdependency with critical business functions, and indispensable for marinating critical business functions.

[ii] For example, Japan established 'The Basic Policy of CIIP' which describes basic idea of CIIP and shared action plan between the government and critical infrastructure industries, and also provides 'guideline to establish safety standards for the information security regarding CIIP' for the industries, and 'Management Standards for Information Security Measures for the Central Government Computer Systems' and 'Technical Standards for Information Security Measures for the Central Government Computer Systems' for the government.

CIIP Guidelines
Appendixes

Appendix 1. Outline of Cyber Exercises

a) There are two types of cyber exercises. Table top exercises in which participants discuss countermeasures based on the scenario face-to-face, or via a telecommunication system; and functional exercises in which actual management issues are checked in a more realistic environment using real IT systems or a simulator.

b) Table top exercises can be conducted at relatively lower costs, and they are a useful method for grasping the basic procedures of incident response and to recognize the issues involved. On the other hand, while the cost of functional exercises may be high, it has the advantage that you can check more detailed points in a real operational situation.

c) It is preferable for CII operators to choose the appropriate style of exercise depending on the goals and items to be checked in the exercises.

d) From the viewpoint of the participants, cyber exercises also can be divided into two further types, which are industry-level exercises and cross-industry exercises. In the industry-level exercises, participants come from only one industry, but participants from all related industries can join cross-industry exercises.

e) The number of participants in the industry-level exercise is relatively few, therefore it is easy to set a scenario and contents, and even to conduct the exercise. This method is best suited for checking detailed items within an industry, although the effect on other industries and society cannot be sufficiently checked if a large-scale cyber-attack was to occur.

f) On the other hand, in the cross-industry exercises many industries are involved and the number of participants is larger, making it much harder to prepare for. The following results can be expected from cross-industry exercises:

1. Mutual understanding of the cross-industry threat
2. Enhancement of one industry’s measures through checking other industries which are interdependent with the first industry’s cyber-attack response system.
3. Improvement of the effectiveness of the information sharing system through establishing a human network between government and the private sector.

g) In the implementation stage, one possibility is a step-up approach. In this approach, an industry-level exercise is conducted as a first step to clarify the issues in each industry. After understanding each industry’s preparation, cross-industry exercises are conducted to check the preparation of the other industries under larger scale cyber-attacks, considering interdependency among the related industries.

Appendix 2. Business Continuity Planning (BCP)

1. Objective

This appendix is intended to encourage governments to ensure the availability of critical IT resources in the government and CII operators, by implementing necessary countermeasures against disruptions in their IT resources and putting in place appropriate BCP policies.

2. Expectation for government

It is desirable that the government ensures that government agencies and CII operators identify necessary IT resources in their organizations, take appropriate countermeasures to protect them, and make sure that the BCP management cycle is effectively working in their respective organizations. It is also desirable that the government provides policies or guidelines for government agencies and CII operators to encourage them to make their BCP more effective, as well as advices or supports if needed.

3. BCP management cycle

In order to make BCP effective, it is desirable to establish BCP management cycle in each governmental organization or CII operator.

BCP management cycle contains the following 4 items:

3-1 Understanding the organization

An organization should understand the internal/external environment surrounding their organization. It also has to recognize the characteristic of risks they may face, and evaluate the impact of these risks. Once they become clear, the organization should identify critical IT resources to be protected, utilizing evaluating method such as a Business Impact Analysis (BIA)

3-2 BCP planning and BCP policy development

The organization should plan necessary countermeasures to mitigate risks on the critical IT resources that were identified in the understanding phase (3-1). Moreover, the organization should establish a BCP policy which describes basic ideas and instructions that members of the organization should follow:

The items in the BCP policy should include:

- Objective of BCP
- Risks to be mitigated
- Identified critical IT resources
- Response team and their responsibilities
- Initial actions

- Degeneration operations
- Recovery actions

3-3 Implementation

The organization should implement the countermeasures to protect their critical IT resources and disseminate the BCP policy throughout the organization.

3-4 Exercise and reviewing

The organization should periodically (at least once a year) conduct the exercise to ensure that the BCP policy is appropriately understood in the organization and that the countermeasures are implemented appropriately. The organization should also review the result of the exercise, and reflect lessons learned into the revised guidelines. Reviewing should also include reevaluation of the risks to see if there is any significant change in their environment, eg. there are new risks to be considered, due to the technological advancement, etc.

4. Reference documents criteria

It is desirable to refer to international standards on BCP such as ISO 22301, in order to be at par with international best practices.

Appendix 3. List of References on Best Practices of CIIP

All chapters

- Critical Information Infrastructure Protection Good Practice Guide (November 2016, Global Forum on Cyber Expertise (GFCE))
  Available at https://www.thegfce.com/documents/reports/2016/11/10/ciip-good-practice-guide

Chapter 1-1 to 1-5 Outline/Overview

- The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) (May 2014, NISC, Japan)
  Available at http://www.nisc.go.jp/eng/archive.html#CIP

Chapter 2-1Preparation for development of CIIP policies

- Methodologies for the identification of Critical Information Infrastructure assets and services(Guidelines for charting electronic data communication networks December 2014, ENISA)
  Available at https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

- Presidential Policy Directive -- Critical Infrastructure Security and Resilience (February 2013, DHS, US)
  Available at https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

Chapter 2-2 Establishment of information security policy or strategy

- The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) (May 2014, NISC, Japan)
- The Second Action Plan on Information Security Measures for Critical Infrastructures(NISC, Japan)
  Above material are available at http://www.nisc.go.jp/eng/archive.html#CIP
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' (March 2011 EU Commission, EU)
  Available at
  http://www.sicurezzacibernetica.it/db/[2011]%20COM%20163%20-%20Achievements%20and%20next%20steps%20towards%20global%20cyber-security.pdf

Chapter 2-3 Establishment of guidelines for security standards

- The Second Action Plan on Information Security Measures for Critical Infrastructures(NISC, Japan)
- Principles for Formulating of "Safety Standards, Guidelines, etc." concerning Assurance of Information Security of Critical Infrastructures (Revised on June 2007,NISC, Japan)
- Principles for Formulating of "Safety Standards, Guidelines, etc." concerning Assurance of Information Security of Critical Infrastructures (February 2006)
- Action Plan on Information Security Measures for Critical Infrastructure(NISC, Japan)

  Above material are available at http://www.nisc.go.jp/eng/archive.html#CIP

Chapter 2-4 Establishment of governance structure and identifying stakeholders

- NIST Roadmap for Improving Critical Infrastructure Cybersecurity(February 2014 NIST, US)

Chapter 2-5 Establishment of an information sharing scheme between the governments and/or regulators and private sector

- The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) (May 2014, NISC, Japan)
- The Second Action Plan on Information Security Measures for Critical Infrastructures(NISC, Japan)

  Above material are available at http://www.nisc.go.jp/eng/archive.html#CIP
- ESCAP Knowledge sharing series issue 2 CYBERSECURITY

Chapter 2-6 IT security crisis management

- Framework for improving Critical Infrastructure Cybersecurity Version 1.0(February 2014, NIST)

  Available at http://www.nist.gov/cyberframework
- BS25999 (Part1 November, 2006 Part2 November 2007, British standards institution)

  Available at http://bsigroup.com/en-GB/iso-22301-business-continuity/

Chapter 2-7 Cyber exercise

- National Exercise good practice guide (December 2009 ENISA)
- On National and International Cyber Security Exercises

  Survey, Analysis and Recommendations (October 2012 ENISA)

  Available at http://www.enisa.europa.eu/

Chapter 2-8 Awareness raising activities for CII owners/operators

- None

Chapter 2-9 ASEAN regiornal partnership

- None

CIIP Guidelines Supplementary Document
Check List for Development of CIIP Policies utilizing CIIP Guidelines
Ver. 1.1

The 9th ASEAN-Japan information security Policy Meeting
October 20th, 2016

Contents

1. Introduction

This document is drafted by the CIIP Working Group reflecting series of discussions in the ASEAN-Japan CIIP working group (1st in Jakarta, February 2015, 2nd in Hanoi, April 2015, 3rd in Tokyo, June 2015) and the ASEAN-Japan Information Security Joint Working Group Meeting (June 2015).

2. Purpose of this document and intended users

This document is developed to assist government officials and/or regulators intending to develop CIIP policies utilizing CIIP guidelines in their countries, especially for the telecommunication sector. Therefore, this document is intended to be used as a reference material. Intended users are as same as the CIIP guidelines. This document is not a legal-binding document but supposed to be used as a reference material.

3. Structure of this document

Structure of this document is following the order of the CIIP guidelines. Firstly this document describes fundamental expectation for the government regarding development of CIIP policies utilizing CIIP guidelines. Secondly, it also describes difficulties and obstacles which the government might face on the way of development of CIIP policies. Thirdly this document suggests some solutions to overcome these obstacles etc. and finally provides "to do list" the countries trying to develop CIIP policies must fulfill in order to achieve the objective, indicating necessary steps to the ultimate goal.

4. Check lists to develop CIIP policies utilizing CIIP guidelines

4-1 Preparation for development of CIIP policies

Expectation for Governments	● To understand internal/external environment correctly regarding CIIP. ● To evaluate risks the Government may face in the future. ● To identify CIIs that should be protected. ● To estimate usable resources.
Possible Issues and Obstacles	● Lack of information. ● Lack of skill/method to evaluate risks. ● CII cannot be identified/Good criteria does not exist. ● Lack of resources/lack of understandings of higher management.
Possible Countermeasures to Overcome Issues and Obstacles	● At this stage, important actions are 1) to understand current CIIP situations correctly inside/outside the country, 2) to evaluate possible risks correctly, and then 3) to estimate usable resources and understand gaps between necessary resources. ● With regard to 1) and 2) If you cannot have enough information, or reliable criterial or reference documents: ➢ Refer to international standards such as ISO 27001:2013 “Information Security Management”, ISO 31000:2009 “Risk Management”, and ISO 22301 “Business Continuity Management”. ➢ Refer to reference documents (see list of reference material in the CIIP guidelines). ➢ Invite experts from private sectors or other advanced countries in terms of CIIP to ask advice or to hold workshops. ● With regard to 3) If shortage of resources is due to lack of understandings of your higher management: ➢ Develop detailed plans to compensate gaps between current situation and necessary resources.

To do List

Phase	Action Items	Check
Risk Evaluation	● Understand external/internal environment. ● Identify threats to your organizations. ● Raise all the risks regarding cyber security. ● Establish risk evaluation criteria and method. ● Evaluate impact of the risks. ● Identify risks to be mitigated.	□ □ □ □ □ □
CII Identification	● Establish evaluation criteria. ● Identify critical IT services for your national security. ● Estimate impact on critical IT services. ● Identify IT services to be protected. ● Create IT inventory list regarding the services. ● Identify CII to be protected.	□ □ □ □ □ □
Usable Resources Estimation	● Estimate usable budget. ● Estimate usable human resources (both in skills and numbers). ● Estimate usable IT infrastructures. ● Estimate possible external aids.	□ □ □ □ □

4-2 Establishment of information security policy or strategy

Expectation for Governments	● To establish basic idea of CIIP to be included in information security policy. ● To decide items to be included in the policy (examples are described in the CIIP guidelines 2-2). ● To periodically review policy/strategy to make sure it is not outdated.
Possible Issues and Obstacles	● Lack of examples/templates. ● Lack of human resources/information. ● Conflict among stakeholders (Ministries/Agencies, CII owners/operators, etc.).
Possible Countermeasures to Overcome Issues and Obstacles	● If you cannot establish information security policy: ➢ Refer to the information security policy of the other countries listed on the CIIP guidelines. ● If there is conflict of the interest between stakeholders, following are the examples to solve the problem. ➢ Establish an organization that has enough authority to coordinate conflicts among stakeholders. ➢ Conduct series of intensive discussions in which every stakeholders can freely discuss their opinions to compromise. ➢ Give enough authorities to certain regulatory ministries/agencies to solve the conflicts. ● It is desirable to put periodical review as a responsibility of the government in the information security policy so that you can have enough human resources or organizations within the government.

To do List

Phase	Action Items	Check
Fundamental Idea of CIIP Policy Development	● Decide definition of CII/CIIP. ● Define objectives of the CIIP. ● Define fundamental idea of CIIP.	□ □ □
Fundamental Idea Documentation	● Put fundamental idea into the information security policy. ● Check if there is no contradiction between other policies and CIIP policy.	□ □ □
CIIP Policy Announcement	● Distribute the policy throughout the organization. ● Make sure basic ideas are infiltrated by holding seminar, periodical surveys, and so on.	□ □
Policy Review	● Review CIIP policy periodically to see if it suits with internal/external environmental changes.	□

4-3 Establishment of guidelines for security standards

Expectation for Governments	● To establish guidelines for security standards to encourage government and CII owners/operators to establish their own security standards. ● To periodically review security standard guidelines to see if they are not outdated. ● To decide items to be included in the guidelines and security standards (examples are described in the CIIP Guidelines 2-2).
Possible Issues and Obstacles	● Lack of examples/templates. ● Lack of human resources/information. ● Conflict among stakeholders (Ministries/Agencies, CII owners/operators, etc.).
Possible Countermeasures to Overcome Issues and Obstacles	● If you need examples/templates, please refer to the reference material on the CIIP Guidelines for security standards. ● It is desirable to put periodical review as a responsibility of the Government in the security standards guidelines so that you can have enough human resources or organizations within the Government and the CII owners/operators, etc. ● If there is conflict of interest between stakeholders, following are the examples to solve the problem: ➢ Establish an organization that has enough authority to coordinate conflicts among stakeholders. ➢ Have series of intensive discussions in which every stakeholder can freely discuss their opinions. ➢ Give enough authorities to certain regulatory Ministries/Agencies to solve the conflicts.

To do List

Phase	Action Items	Check
Fundamental Idea of Security Guidelines Development	● Define objectives of the security guidelines. ● Define fundamental idea of security guidelines.	□ □
Basic Idea Documentation	● Put basic idea into the security standard guidelines. ● Check if there is no contradiction between other regulations and security guidelines.	□ □ □
Security Guidelines Announcement	● Distribute the security guidelines throughout the organization. ● Make sure principle ideas are infiltrated by holding seminar, periodical survey, and so on.	□ □
Review	● Review security guidelines periodically to see if it suits with internal/external environmental changes.	□

4-4 Establishment of governance structure and identifying stakeholders

Expectation for Governments	● To identify stakeholders regarding CIIP. ● To clarify decision making process with regard to CIIP. ● To define stakeholder’s roles and responsibilities.
Possible Issues and Obstacles	● Conflict among stakeholders with regard to their roles and responsibilities. ● Lack of best practices. ● Lack of guidelines.
Possible Countermeasures to Overcome Issues and Obstacles	● If you cannot define the roles and responsibilities of each stakeholder properly: ➢ Establish an organization that has enough authority to coordinate conflicts among stakeholders. ➢ Have series of intensive discussions in which every stakeholders can freely discuss their opinions. ➢ Give enough authorities to certain regulatory Ministries/Agencies or make "CIIP executives" who have enough knowledge and experience in each organization to solve the conflicts. ● If you cannot implement governance system because of lack of best practices or guidelines, please refer to reference materials described on the CIIP Guidelines.

To do List

Phase	Action Items	Check
Stakeholder Identification	● Establish criteria for stakeholder identification. ● Identify stakeholders to play roles in the CIIP both in Governmental organization and CII industries.	□ □
Decision Making Process Clarification	● Clarify decision making process regarding CIIP, considering necessary information flow and authority to make decisions.	□
Stakeholder's Roles and Responsibilities Definition	● List up all the roles and responsibilities to develop efficient CIIP systems. ● Assign these roles and responsibilities to identified stakeholders (see examples shown in the CIIP Guidelines). ● Identify responsible person/department in each stakeholder. ● Make sure assignment is accepted by all the stakeholders.	□ □ □ □
Others	● Review stakeholders, their roles and responsibilities periodically to ensure that they can manage all the internal/external issues appropriately.	□

4-5 Establishment of an information sharing scheme between the governments and/or regulators and private sector

Expectation for Governments	● To establish information sharing platform regarding CIIP (Choose either of (1) laws and regulations basis, (2) voluntary basis depending on your current situation regarding CIIP). ● To encourage CII owners/operators to share necessary information for CIIP. ● To provide useful information to the CII owners/operators for improving their own CIIP. ● To provide opportunities for information sharing among Government and CII owners/operators.
Possible Issues and Obstacles	● Lack of best practices/templates. ● Lack of human resource/knowledge. ● Conflict among stakeholders (Ministries/Agencies, Industries, and private sectors, etc.).
Possible Countermeasures to Overcome Issues and Obstacles	● If you don't have enough information or examples; ➢ See best practices and reference documents in the CIIP Guidelines. ➢ Hold information sharing workshops with other advanced countries in terms of CIIP. ● If you have conflicts of interest among shareholders to share necessary information: ➢ Establish regulations to require CII owners/operators to share necessary information with the Government. ➢ Persuade CII owners/operators or other organizations to share information voluntarily by explaining merits of information sharing. ➢ Develop a Ministry/Agency which has enough authority to coordinate conflicts of stakeholder’s interests.

To do List

Phase	Action Items	Check
Information Sharing Platform Establishment	● Decide objectives of information sharing. ● Decide information type to be shared. ● Design efficient platform to achieve the objectives. ● Inform the establishment of information sharing scheme to the necessary stakeholders to be involved.	□ □ □ □
Encourage Participants to Share Information	● Announce importance of information sharing. ● Give examples of information to be shared. ● Explain how shared information will be utilized for improving information security.	□ □ □
Provide Useful Information to the Participants	● Gather useful information for participants in the information sharing system. ● Provide information to the participants.	□ □
Provide Opportunities to Share Information	● Set a meeting/committee where participants can exchange information freely within the industry. ● Exchange information (preferably interactively) between Governments and industries.	□ □

4-6 IT security crisis management

Expectation for Governments	● To enhance capabilities for incident detection for the Government and encourage CII owners/operators to do the same. ● To take necessary countermeasures to mitigate risks of cyber incidents and encourage CII owners/operators to do the same. ● To develop disaster recovery plans for Governments and BCP for critical business functions identified in the CIIP Guidelines 2-1-b, and encourage CII owners/operators to do the same.
Possible Issues and Obstacles	● Lack of information/best practices. ● Lack of skills/methods to introduce disaster recovery plans or BCP. ● Lack of resources/understandings of higher management.
Possible Countermeasures to Overcome Issues and Obstacles	● See best practices and reference documents in the CIIP Guidelines and other international standards (ISO22301, etc.) ● Join the exercise to introduce disaster recovery plans or BCP. ● Try to explain to higher management the importance of exercises to make them assign more resources.

To do List

Phase	Action Items	Check
Establish Incident Response Capabilities	● Establish cyber incident detection features (such as establishing CSIRTs) for the Government. ● Encourage CII owners/operators to establish incident detection features.	□ □
Preparation (As in the CIIP Guidelines 2-1)	● Assess risks and threats. ● Identify critical business functions and critical IT resources. ● Check usable resources. ● Encourage CII owners/operators to do the same.	□ □ □ □
Take Countermeasures for the Risks	● Decide countermeasures to mitigate risks on your critical business functions and critical IT resources. ● Make implementation plans for countermeasures. ● Implement countermeasures based on the implementation plan. ● Encourage CII owners/operators to do the same.	□ □ □ □
Establish Disaster Recovery Procedure	● Establish disaster recovery plans for quick recovery from cyber incidents.	□
Establish BCP Procedure	● Establish business continuity plans (BCPs) to assure business continuity for your core business functions in case your related critical IT resources are not available.	□

These "to do" items are for the exercise organized by the Government. If private sectors take the lead and Government just support them, make sure these "to do" items are properly prepared/conducted, and if not, support them by following the description in the CIIP Guidelines 2-6.

4-7 Cyber exercise

Expectation for Governments	● To improve effectiveness of information sharing systems regarding CIIP. ● To plan and conduct exercises (within Government/cross sectoral exercises). ● To encourage CII owners/operators to conduct industry-level exercises. ● To provide CII owners/operators basic scenarios or tools/templates, etc.
Possible Issues and Obstacles	● Lack of information/best practices. ● Lack of skills/methods to conduct exercises. ● Lack of resources/understandings of higher management.
Possible Countermeasures to Overcome Issues and Obstacles	● See best practices and reference documents in the CIIP Guidelines. ● Join the exercises conducted by other countries/organizations to earn skills. ● Try to explain to higher management the importance of exercises to make them assign more resources.

To do List

Phase	Action Items	Check
Prepare Cyber Exercises	● Decide objective of the exercise.	□
	● Decide participants.	□
	● Establish exercise secretariat.	□
	● Prepare base scenario/injections.	□
	● Prepare standard procedures for information sharing to follow during the exercise.	□
	● Prepare exercise manual and time schedule.	□
	● Assign tasks to the exercise secretariat.	□
	● Prepare the follow-up questionnaire (if necessary).	□
	● Notify the exercise date to the participants.	□
	● Prepare necessary infrastructures/equipment.	□
Conduct Cyber Exercises	● Organize the exercise.	□
	● Conduct troubleshooting.	□
Review Cyber Exercises	● Hot wash after the exercise.	□
	● Conduct follow-up questionnaire (if necessary).	□
	● Gather lessons learned from the exercise.	□
	● Make improvement plans for the next exercise or information sharing procedure.	□

These "to do" items are for the exercises organized by the Government. If private sectors take the lead and Government just support them, make sure these "to do" items are properly prepared/conducted, and if not, support them by following the description in the CIIP Guidelines 2-7.

4-8 Awareness-raising activities for CII owners/operators

Expectation for Governments	● To improve awareness of the private sector regarding significance and risks of information security. ● To gather opinions from the private sector.
Possible Issues and Obstacles	● Lack of best practices. ● Lack of opportunities to hear opinions from the private sector. ● Lack of resources/budgets/ideas.
Possible Countermeasures to Overcome Issues and Obstacles	● See CIIP best practices and reference documents on the CIIP Guidelines. ● Conduct seminar/events where Government and private sector can exchange opinions regarding information security. ➢ Seminars (e.g. for citizens, corporate employees, leaders in the industry). ➢ Events (e.g. Security Contest, CIIP workshop). ● Conduct hearing from important companies/organizations. ● Seek possibilities of joint awareness raising campaign with other countries/learn from experiences of other ASEAN member states.

To do List

Phase	Action Items	Check
Awareness Raising Planning	● Decide objective of awareness raising programs. ● Decide annual plan for awareness raising plans including events and awareness raising material.	□ □
Event Planning	● Plan security awareness raising events. ● Conduct security awareness raising events.	□ □
Awareness Raising Materials Development	● Develop security awareness raising materials. ● Distribute security awareness raising materials.	□ □
Others	● Consider international joint security awareness activities, if possible.	□

4-9 ASEAN regional partnership

Expectation for Governments	● To make an effective and efficient collaboration among international partners in the ASEAN region.
Possible Issues and Obstacles	● Lack of information. ● Lack of best practices.
Possible Countermeasures to Overcome Issues and Obstacles	● Involve more partners to the joint activities in the ASEAN region.

To do List

Phase	Action Items	Check
POC (Point of Contact) Establishment	● Establish POCs among ASEAN member states and its partner countries. ● Make a POC list.	□ □
Periodical Contact Establishment	● Start contact between POCs. ● Set periodical online/face to face meeting with POCs in order to share information regarding IT security.	□ □
Short Term Collaboration	● Start short term collaboration such as security awareness raising campaigns (ex. seminars, short term events, etc.).	□
Long Term Collaboration	● Enhance mutual collaboration to long term cooperation such as mutual information sharing, student exchange, and joint cyber exercises, etc.	□