Study of Critical Information Resources Infrastructure Security Strategy

Kajian Strategi Pengamanan Infrastruktur Sumber Daya Informasi Kritis

Ahmad Budi Setiawan
Pusat Penelitian dan Pengembangan Aplikasi Informatika dan Informasi Komunikasi publik
Jl. Medan Merdeka Barat No.9 Jakarta 10110, Indonesia
e-mail : ahma003@kominfo.go.id

ARTICLE INFORMATION

Manuscript received February 5, 2015
Revised March 17, 2015
Approved March 20, 2015

Kata kunci:
Infrastruktur Informasi Kritis
Proteksi
Keamanan Informasi
Sistem Manajemen Keamanan Informasi

ABSTRAK

Infrastruktur informasi kritis merupakan salah satu infrastruktur kritis yang menggabungkan antara infrastruktur telekomunikasi serta jaringan internet yang digunakan dalam pelayanan publik. Dengan demikian, infrastruktur informasi kritis harus beroperasi dengan aman dan memenuhi aspek keamanan informasi. Kajian ini adalah studi kasus pada infrastruktur informasi kritis sebagai salah satu infrastruktur kritis Nasional yang digunakan dalam pelayanan publik. Adapun infrastruktur informasi kritis yang dijadikan studi kasus adalah pada bidang energi ketenagalistrikan. Tujuan kajian ini adalah memberikan masukan pada kebijakan pengamanan infrastruktur kritis berdasarkan studi kasus yang dilakukan. Kajian ini dilakukan dengan metode gabungan kuantitatif dan kualitatif yang mengkombinasikan hasil penilaian risiko pada obyek riset dengan pendapat pengambil kebijakan, akademisi, pakar dan praktisi. Hasil kajian ini adalah masukan untuk kebijakan dan kerangka kerja pengamanan infrastruktur kritis khususnya sector TIK.

Keywords :
Critical Information Infrastructure
Protection
Information Security
Information Security Management System

ABSTRACT

Critical information infrastructure is one of the critical infrastructure that combines telecommunications infrastructure and Internet networks used in the public service. Thus, the critical information infrastructure must operate safely and meet the aspects of information security. This study is a case study on critical information infrastructure as one of the critical national infrastructure used in public service. The critical information infrastructure which is used as a case study is in the field of electricity energy. The purpose of this sudy is to provide input on critical infrastructure security policy based on case studies conducted. This study was conducted with the combined quantitative and qualitative method that combines the results of the risk assessment on the research object with the opinion of policy makers, academics, experts and practitioners. These results are input to the policy framework and securing critical infrastructure, especially the ICT sector.

1. Introduction

The development and advancement of information and communications technology that are so rapid has changed the pattern of human life in various fields directly or indirectly. Internet technology is currently utilized by various parties including the government, academia, industry, institutions and personal in the search for, acquire, manage and transmit information. Political, economic, social, cultural, defense and security values of the information that runs on the current Internet infrastructure is very high thus increasing the potential threats and disturbances in the use of Internet technology itself (Su, X., 2006).

Today in Indonesia, more than one million attacks occurred daily against information security, internet, such as intercepting transmissions actions occur between one party to the other party, the action which resulted in the termination of communication between the two parties that should have had an interaction, and other measures has the potential to destroy the information that goes over the Internet infrastructure. Cases of incidents related to the security of the internet has been rife in Indonesia and directly threatens the strategic infrastructure in Indonesia. Major cases that occur such as 2004 Elections Site defacing, identity and data theft (information resources) as well as the accounts hacking (email, IM,

DOI: 10.17933/bpostel.2015.130104

social networks) were mostly done for the purpose of fraud, credit card fraud, ATM/EDC skimming, hacking, cracking, phishing (internet banking fraud), malware (virus/worm/trojan/bots), cybersquatting, pornography, online gambling, transnational crime, such as; drug trafficking, mafia, terrorism, money laundering, human trafficking, underground economy which is currently rife, especially in Asia Pacific. Data theft cases in Citybank and Sony Corporation opened our eyes that the attacks are increasingly organized and focused to attack economic means (the Department of Defense, 2012).

The Amendments of 1945 Constitution have mandated that every person has the right to communicate and obtain information to develop personal and social environment, and the right to seek, obtain, possess, store, process and convey information by using all available channels. In carrying out the mandate, the government has issued Law No. 36 of 1999 on Telecommunications that Telecommunication Operators shall provide security and protection of the installation in telecommunications network that is used for the operation of telecommunications. Whereas Government Regulation No. 52 of 2000 on Telecommunications Operations requires that any telecommunications network, the telecommunications infrastructure must be equipped with means of security and protection in order to avoid disruption of telecommunications.

To support the use of IP based telecommunications network that is relatively safe from threats and disturbance, the government made the Regulation of the Minister of Communications and Informatics No. 26/PER/M.KOMINFO/5/2007 on The Security of Utilization of Internet Protocol Based Telecommunication Network which were last amended by Regulation of the Minister of Communications and Informatics No. 24/PER/M.KOMINFO/11/2011 to designate ID-SIRTII in charge of supervising the security of telecommunication networks based on Internet protocol.

Security on the Internet infrastructure is the duty of every party that utilize these technologies. Internet infrastructure security on the one hand depends on the security of Internet infrastructure on the other. Cooperation and coordination is absolutely necessary between telecommunications operators, managers and users of the technology itself to jointly improve security on their internet infrastructure. Pattern of good communication is absolutely necessary in order to better prevention of threats and disturbance, and also countermeasures against an incident that occurred in order for the information that goes over the Internet infrastructure so it can be well protected.

Infrastructure Security of National Critical Information Resources is an absolute prerequisite that must be implemented in order to ensure the effectiveness of reliability, availability and integrity of information networks, both nationally and globally (Henderson, 2007). However, a huge impact and the potential disruption and threat to the national security of critical infrastructure is still not fully realized by the community. This is evident from the unavailability of policy Protection of National Critical Information Infrastructure and unmapped/unclassified National Critical Infrastructure, especially information network infrastructure.

In general, critical infrastructure is a vital service which if not functioning properly will cause economic paralysis, tremendous damage, disorder or riot, or even death. Among others are electricity, water, telecommunications, internet, transportation, finance, distribution of oil, gas and food, national defense, government services, and health. The function of the economy and society are increasingly dependent on information systems and networks that are interconnected and interdependent, both domestically and across sectoral boundaries. A number of systems and networks are extremely important nationally and that the protection of critical information infrastructure is a priority for national policy and in international cooperation. Destruction of information security at critical infrastructure could result in a big impact on the economy (Ko & Dorantes, 2006). Thus the issues to be discussed in this study are; How are the security policy implementation strategy of Critical Information Resources Infrastructure in Indonesia?

2. Desktop Study

2.1. Critical Information Infrastructure Protection

Critical or vital infrastructure is a set of systems that provide resources on which all the functions of society depend. An example is telecommunications, important state information, transport, energy, clean water, health services, emergency care, manufacturing and financial services. Meanwhile, the Organization for Economic Co-Operation and Development (OECD) defines an Critical Information Infrastructure as a collection of information systems that are interconnected and information network system/computerization, which in case of disruption or destruction on such a system would have a serious impact on health, safety, security or economic well-being of society, or on the effective functioning of government or economy (OECD, 2008).

National critical information infrastructure can be identified through the risk assessment process and usually includes one or more of the following:

- Supporting information components for critical infrastructure, and/or
- Information infrastructure that supports critical component of government business; and/or
- Information infrastructure essential to the national economy.

Protection against the Critical Information Infrastructure Protection (CIIP) is generally is known as a vital component of a national information security policy (Suter, 2007). In terms of protection of critical infrastructure, some countries have developed modern and comprehensive CIIP systems and organizations. Framework for National Critical Information Infrastructure Protection or further agreed with the terms CIIP provides a structured view of strategic information services and resources for the infrastructure of nation states. This framework also serves as a common lens from which to view risk, threat, vulnerability, and protective control of these resources.

Plans for a national response and protection of infrastructure determine the risk management process and has the potential to create a stabilizing effect both domestically and internationally. Given the various aspects affiliated with CIIP, the International Telecommunications Union (ITU) introduced the Four Pillar CIIP Model which is a strategic measure CIIP (Suter, 2007).

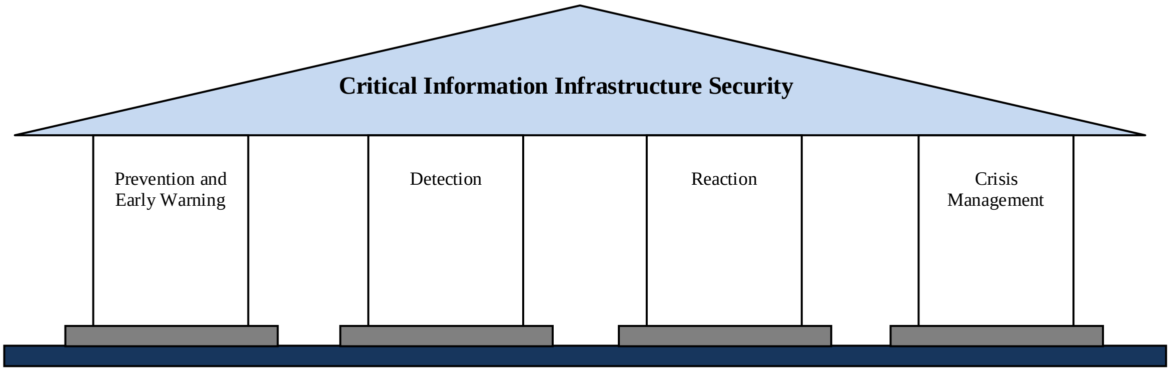
Critical Information Infrastructure Security
Prevention and Early Warning
Detection
Reaction
Crisis Management

Figure 1. Four Pillars CIIP Model (Suter, 2007)

The first step in the development of an effective and efficient critical information infrastructure protection organization is to set priorities and an important responsibility. Important tasks of the CIIP organized in the Four Pillars-CIIP Model. The four pillars of this model are: the prevention and early warning; detection; reaction; and crisis management.

2.2. NISTIR Framework for Critical Infrastructure

National Institute of Standards and Technology -Interagency Report (NSTIR) is a framework regarding cyber security to assist governments and industry in meeting important responsibilities related to critical infrastructure. A recent report was prepared by the Working Group on Cyber Security, Cyber Security Working Group (CSWG) of the Smart Grid Interoperability Panel, a public-private partnership launched by NIST with the Department of Energy, USA. Furthermore, the guidelines issued by NIST is known as NISTIR 7628 (NIST, 2007).

The NISTIR 7628 framework is the main output of the coordination of the working group at NIST as the effort to identify and develop standards needed to convert the smart grid into critical infrastructure, in the advancement of digital technology with two-way capability for communicating information, controlling equipment and distributing energy (NIST , 2014).

Although created by Smart Grid working group, but the NISTIR 7628 framework can also be implemented on other critical infrastructure. The guidelines also provide technical background and details that can inform organizational efforts to securely implement smart grid technology. Provide a technical foundation for utilities, hardware and software manufacturers, energy management service providers, and others to build implementations. Each organization's cyber security requirements should evolve as technology advances and new threats to grid security arise. The report recommends implementing multiple levels of security.

2.3. Information Security Management

Security of data/electronic information becomes a very important thing for the companies that use IT facilities and placing it as essential infrastructure. Because the data/information is an asset to the company. Security of data/information can directly or indirectly maintain business continuity, reduce risk, optimize return on investment and deliver even greater business opportunities. The more corporate information is stored, managed and used jointly, the greater the risk of damage, loss or exposure of data/information to other unauthorized parties.

Information security consists of protection against the following aspects:

1 Confidentiality. Aspect that ensure the confidentiality of data or information, ensuring that information can only be accessed by authorized persons and ensure the confidentiality of data sent, received and stored.

2 Integrity. Aspect which ensures that data is not modified without permission of authorized parties, maintain the accuracy and integrity of information and methods of the process to ensure the integrity of this aspect.

3 Availability. Aspect which ensures that data will be available when needed, ensuring authorized users to use the information and related devices (related assets if necessary).

4 Autenticity. Aspect which ensures that the data or information can not be denied (non-repudiation) by another party who is unauthorized.

Security of information obtained by implementing a set of appropriate controlling tools, which could be policies, practices, procedures, organizational structures and software. In implementation strategy, the management of information security could not be separated from the three (3) scope of information security implementation, namely; people, process, and technology. The fourth aspect of information security and the scope of information security is described in the chart in Figure 2 below;

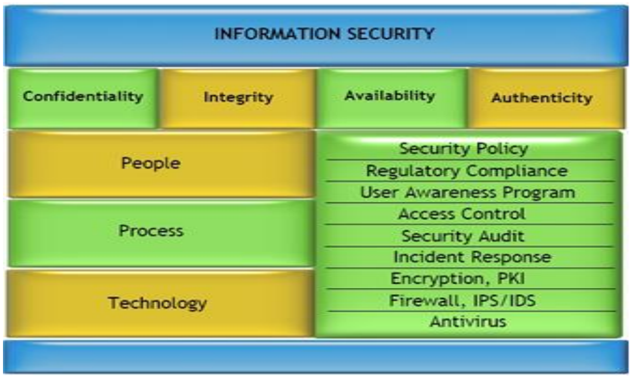

Figure 2. Information Security Management (Nayak, 2010).

Technically, to deny the crime among other require security measures such as encryption, to protect data (encryption to database and storage), communication protection (SSL, SSH, and VPN), mail protection (PGP, SMIME), identity and transaction protection (CA, PKI, authentification, non-repudiation). To ensure that the IT infrastructure is safe from harmful threats and attacks, it requires good information security governance related to the use of ICT. Standard and governance of information security in general adopt the framework of the IT governance of COBIT and ISMS of ISO/IEC 27001 and ISO/IEC 27002 (ISO/IEC 27002: 2013, 2013). ISO/IEC 27001:2005 which was updated with the ISO/IEC 27001:2013 is an information security standard issued by the International Organization for Standardization and the International Electronical Commission in October 2005 to replace the BS7799-2 standard. This standard contains specifications or requirements that must be met in building the Information Security Management System (ISMS). This standard is independent to information technology products, require the use of a risk based management approach, and is designed to ensure that selected security controls are capable of protecting the information assets of various risks and give confidence on the level of security for interested parties (ISO/IEC 27001: 2013, 2013).

2.4. ISO 31000, ISO 31010 Framework

ISO 31000 is a standard implementation of risk management published by the International Organization for Standardization on 13 November 2009, which is the development of AS/NZS 4360: 2004 standards issued by the Australian Standards. This standard is intended to be applied and adapted to all types of organizations to provide structure and guidelines that apply to all generic operations related to risk management. Figure 3 presents the process flow of risk management to be performed by adapting ISO31000.

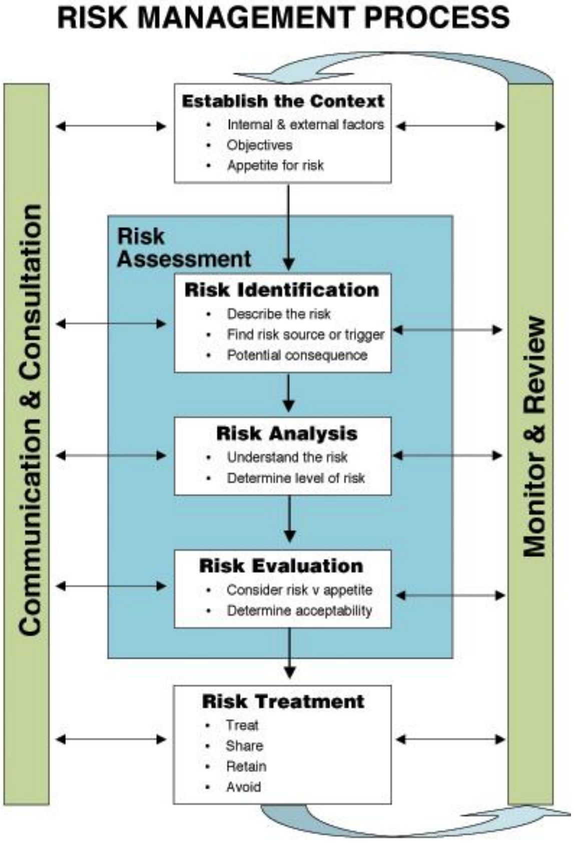

Figure 3. Risk Management Process Framework (ISO 31000:2009, 2009)

ISO/IEC 31010: 2009 Risk management - Risk assessment techniques are supporting standard for ISO 31000 and provides guidance for the selection and application of systematic techniques for assessing/conducting a risk assessment. The first version of this standard was issued in November 2009.

ISO 31000 sets out principles and a framework and process to manage all the risk factors in a transparent, systematic and credible manner. Through risk management based on ISO 31000:2009 companies can develop, implement and improve the performance of corporate risk management as an integral part of the company's management system. ISO 31000:2009 can be applied to any type of organization, whether public, private, community, association, group or individual.

2.5. Research Ever Been Conducted

Researches that have been conducted and relevant as a comparison in this research, namely:

1 Research conducted by Sean P. Gorman, Laurie Schintler, Raj Kulkarni, and Roger Stough with the title "The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure", in 2004 (Gorman, Schintler, Kulkarni, Stough, 2004). The study aims to analyze the impact of the attacks directed against critical infrastructure in the telecommunications sector in line with the increasing security problems in the United States after September 11, 2011. The analysis in the study includes a comparison method used in vulnerability analysis with spatial methods that is built by combining variables of regional and distances. Results of the analysis are used in the context of evaluating national and regional security and economic impact if the attacks on CIIP telecommunications sector occurs.

2 Subsequent research was conducted by Myriam Dunn (Dunn, 2005). Title of the research is "The socio-political dimensions of critical information infrastructure protection (CIIP)". The study discusses the protection of critical infrastructure from social-economic-political aspects. The study demonstrated comparison of critical infrastructure protection policies in some organizations and countries. Results of

the research shows that the effective protection of critical infrastructure that was threatening holistically and strategically is through risk assessment at the physical, virtual, and psychological level as a basis for a comprehensive strategic protection and survival. Thus will require a comprehensive and interdisciplinary R & D agenda tha really encompasses all disciplines ranging from engineering and other sciences, such as policy, political science, and social.

3 Another research was conducted by Eugene Nickolov (Nickolov, 2005). The research provides a brief description of the critical information infrastructure and analyze the extent to which organizations can depend on the functioning of the critical infrastructure, such as as in the organization of banking and financial services, electricity, fuel and water supply networks, as well as information and telecommunications networks. The consequences of attacks on certain elements of the infrastructure are examined, as well as initiatives and issues arising with their protection at national and international levels.

2.6. Research Framework

ISO 31000 framework reflects the circle of Plan, Do, Check, Act (PDCA), which is commonly known in the whole management system design. The standard states that "The framework is not aimed or intended to determine a management system, but rather on an effort or means to help organizations to integrate risks management into the overall risk management system." This statement is intended to encourage organizations to be more flexible in implementing elements of the framework required.

There are two main components in the risk management process in the ISO 31000 standard, namely:

1 Framework, which guides the organization to understand the overall structure and workings of an organization's risk management.

2 Process, which describes the actual method of identifying, analyzing, and managing risk.

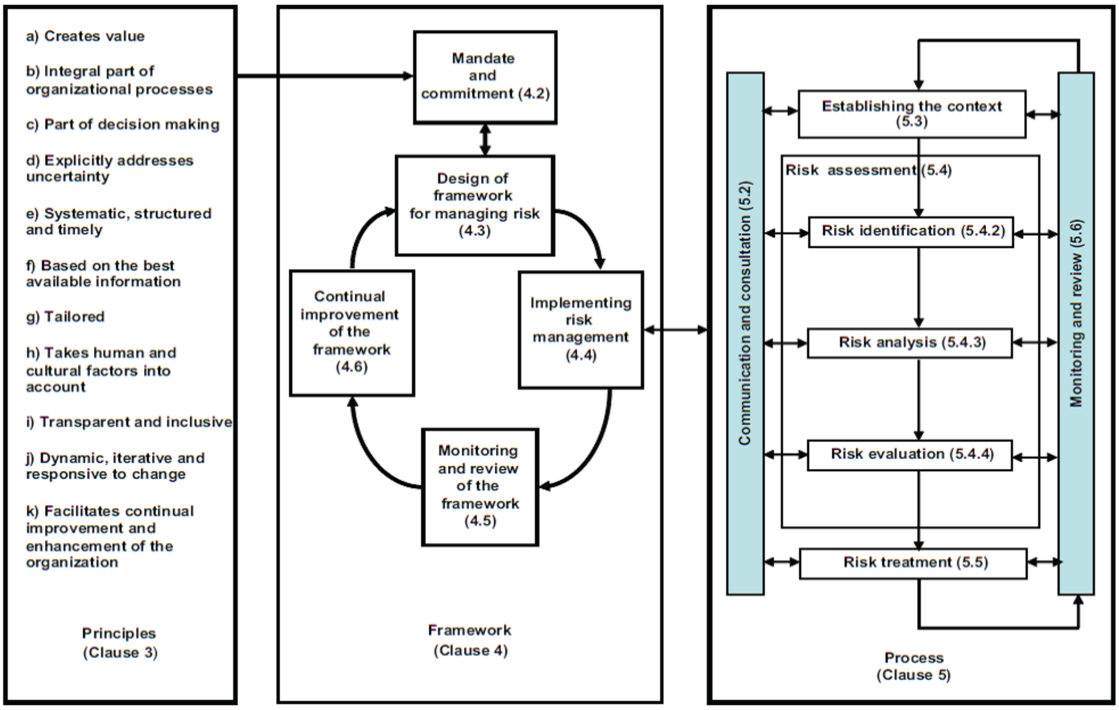
a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles (Clause 3)
Mandate and commitment (4.2)
Design of framework for managing risk (4.3)
Implementing risk management (4.4)
Monitoring and review of the framework (4.5)
Continual improvement of the framework (4.6)
Framework (Clause 4)
Communication and consultation (5.2)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Monitoring and review (5.6)
Process (Clause 5)

Figure 4. Schematic Research Framework based on Risk Management Method of ISO 31000 (ISO 31000:2009, 2009).

Based on this framework, the Risk Management Process consists of several phases, namely:

a Phase I, Determination of Context

Phase I aims to identify problems, determine the scope of the subject matter.

b Phase II, Risk Assessment

Phase II is the stage of risks identification, both inherent risk and residual risk; Risk analysis, which includes risk mapping, calculation of the likelihood to observe which risks are critical and non-critical; and the evaluation of risks.

c Phase III, Risk Treatment

This stage is the process of determining the response to the existing risks. Furthermore, identified responses are filtered to determine the appropriate response in context and determination of control used.

d Phase IV, Communication and Consultation

This phase is done to maintain the suitability of business process management with strategic goals and objectives.

e Phase V, Monitoring and Review

At this stage monitoring mechanisms are designed in the implementation of risk management.

3. Methods

3.1. Study approach

The study was conducted qualitatively and using the Risk Management approach based on ISO 31000. The risk management process according to ISO 31000 should be an integrated, embedded part in the culture and management practices, and customized according to the organization's business processes. According to ISO 31000, the risk assessment is the most important and fundamental in the process of risk management. ISO 31000 provides a framework to guide the implementation of effective risk management.

The purpose of the framework of the implementation of risk management, among others:

1. The assurance that information on risk management resulting from risk management process has been sufficiently reported and used as a basis for decision making
2. Fulfillment of accountability at every level of the relevant organization

Objects that serve as the study is the management of critical information infrastructure in the power plant company, PT. PLN (Persero) Java Bali Generators. In the implementation of the study, in-depth interviews are conducted with the management following a risk assessment and expert judgment.

3.2. Assessment Phase

Referring to the framework of a Risk Management Process, so that the study can be done in a systematic manner, assessment phase was prepared which is an embodiment of the line of thought of the phase of problem definition, the analysis of solutions to the design plan, a detailed flow of study implementation is described below.

a Determination of context.

The process begins by defining the research problem, determine the scope and may include establishment of initial concept involving research object.

b Intervention.

The process of planning, development and taking action to create a construction, model, method, prototype or other resources.

c Risk Assessment.

The process of risk assessment carried out by the observation and measurement of the level of risk that may occur in the critical infrastructure. This process is a validation of the model or design produced by deep interviews and conduct focus group discussions with policy makers and experts.

d *Review and Dissemination.*

The process of reflection and learning for the resulting output. Reflection and learning aimed to evaluate the results and determine its contribution practical and theoretical matters. This process is done by an expert judgment as well as academics. The next stage is to communicate the research results.

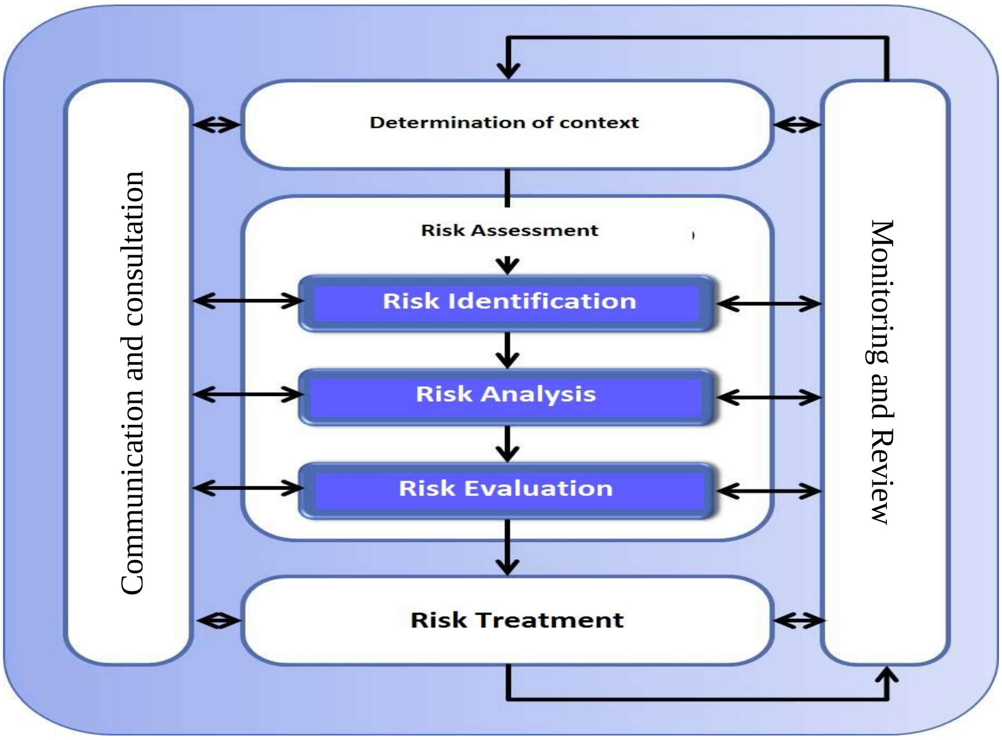

Figure 5. Schematic Assessment Methods

4. Results and Discussion

4.1. Risk Management Process

1. Determination of context

At the beginning of a risk management process is to determine context. The process of determining the context is based on the assessment conducted on the documents of an organization which has a critical infrastructure. Assets that are likely to be threatened so that it can be derived by considering the enabler that allows the process to be identified. Enabler can be reduced by identifying people, places, and products necessary to ensure the process can be done. Every enabler is owned. The owner is the authority responsible for the operational parts of the organization to ensure that appropriate mitigation controls can be implemented. Here's an example of a structural role in an organization that have critical infrastructure:

Table 1 Roles in an enterprise.

Rule	Deskription
Chief Executive Officer (CEO)	The highest official responsible for the overall management of enterprise
Chief Financial Officer (CFO)	The most senior official of the enterprise responsible/accountable for all aspects of financial management, including financial risks and control
Chief Operating	The most senior official of the enterprise responsible/accountable for the operations of the enterprise

Rule	Deskription
Officer (COO)	
Strategic Executive Committee	Set of senior executives appointed by the board of directors to ensure that the board of directors involved in it and stay informed about those things and IT-related decisions. This committee is responsible/accountable in the management of the investment portfolio of IT, IT services and IT assets, as well as ensuring that the value to be delivered and risk to be managed. This committee is generally chaired by a member of the board of directors, not by the CIO.
Chief Risk Officer(CRO)	The most senior official of the enterprise responsible/accountable in all aspects of risk management in the enterprise. IT risk officer function can be set up to oversee the IT-related risks
CISO	most senior official of the enterprise responsible/accountable to the entire enterprise information security
Enterprise Risk Management (ERM) Committee	Set of enterprise executives responsible/accountable to the enterprise-level collaboration and approvals necessary to support the activities and decisions of ERM. IT risk board can be set up to consider a more detailed IT risks and provide advice to the ERM committee
Audit	Function in the enterprise in charge/responsible in the provision of internal audit
Chief Information Officer (CIO)	The most senior official in the enterprise that is responsible/accountable to the alignment of business and IT strategy and is responsible/accountable to the planning, procurement and management of resources in the provision of IT services and solutions to support enterprise goals
Service Manager	The party that manages the development, implementation, evaluation and ongoing management of new/existing products and services for the customer/user or a specific group of customer/users
Information Security Manager	The party who manages, to designs, oversees and/or assesses the information security of the Enterprises
The BCP manager	The party who manages, designs, oversees and/or assesses the ability of enterprise business continuity, to ensure that critical enterprise function continues to run when there is chaos/disturbance
Privacy Officer	In charge/responsible in the supervision of risk and business impact of privacy legislation as well as guiding and coordinating the implementation of policies and activities that will ensure that the privacy instructions are followed. These parties are also commonly referred to as data protection officer

Source: Processed data

2. Identitas Risiko

Threat or risk. The resulting risk sources are derived from each assets enabler that have been described previously. After identifying the assets which are necessary to enable the processing of critical IT infrastructure in the institutions/organizations that have critical electronic systems as well as sources of risk that may occur, the next activity is to identify vulnerabilities of each asset. Vulnerability to asset can be identified through the consideration of potential threats. The process is followed up by describing the level of risk.

3. Risk Analysis

Table 2 Likelihood Table

Likelihood Descriptor	*Likelihood Description Statements*
Very rare	The event is expected to occur in most circumstances.
Jarang	The event will probably occur in most circumstances and is expected at some time
Seldom	The event might occur at some time but is not expected
Often	The event could occur at some time
Very Often	The event may occur in exceptional circumstances

Source: Processed data

The perceived impact when a risk occurs can affect and interfere with the achievement of operational and organizational objectives. The influence could be very mild or extreme. A full description of these impacts can be seen in Table 3.

Table 3 Risk Impact Analysis

Consequence/Impact	Quality of service
Insignificant	In principle, deficiency or absence of service is low, with no comments
Minor	Service deemed satisfactory by the general public, but the employees of the agency are aware of the deficiency
Moderate	Services being considered unsatisfactory by the general public and employees of the organization
Major	General public considers service of the organizations as unsatisfactory
Very significant / risky/Catastrophic	Services fell very far below accepted standards

Source: Processed data

Based on the table of possible risks and impact analysis, it can be made as materials to determine applicable risk rating using the matrix described in Table below. The matrix will serve to determine the treatment/risk priorities from a list of existing risks. Levels of risk consists of three (3) levels, namely; Low, Medium and High. Table 4 shows the ranking of the three levels of risk that are mapped by the possibility of the frequency of occurrence of risk and consequences of the impact of the risk.

Table 4 risks rating

		Consequence				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Likelihood	**Rare**	Low	Low	Low	Low	Medium
	Unlikely	Low	Low	Medium	Medium	High
	Possible	Low	Medium	Medium	High	High
	Likely	Low	Medium	Medium	High	High
	Almost Certain	Medium	Medium	High	High	High

Source: Processed data

Based on the risk level, a risk management need to be classified as a response to risk. This forms of response is associated with anyone acting as a responsible official at each level and what recommendations to follow up based on risk conditions. It is very useful to mitigate against the risk. Here is table 5 on risk rating response.

Table 5 Risk Rating Response

Risk Rating	Responsibility for Risk Acceptance	Action Risiko	Rekomendasi
High	*Risk Manager*	• Will be expected to damage the entire organization's ability to continue to operate with the confidence of the customer base or the owner of the company. Risks that occur can lead to social or economic damage and can seriously affect the organization's ability to continue operations. • It would be expected to have a significant impact on the company's budget and organization's reputation. Might cause serious disruption and inconvenience of an extended service or have a health impact on the broad customer base.	Mitigasi/Transfer
Medium	Risk Manager Senior Manager	May result in short-term, localized, disruption of services and require escalation through management line. Might produce adverse media comment and moderate local penalty or costs may be incurred through normal operating budget.	Mitigasi
Low	Senior Manager	It is impossible to have an impact that could not be satisfactorily be addressed through the normal operational procedures.	Accept/Avoid

Source: Processed data

4. Risk Evaluation

The process of evaluating the risk is having a goal to help the decision-making process based on the results of risk analysis. The process is executed by determining risks that require treatment of risk or risk priority. Risk evaluation involves comparing the level of risk identified during the risk analysis process using risk criteria. Risk evaluation also directs which decision-making related to risk that needs to be addressed. Further action is the process of risk treatment. The process has the objective to determine the types and forms of risk treatment. Selection of risk treatment should reflect the values and perceptions of stakeholders.

5. Communication and Consultation

This section is the identification and involvement of all stakeholders involved in the management of risk in the critical information infrastructure. In addition to the daily operation of the system, it is important to ensure that risk information is communicated through the organization's management and made a brief report to the executive forum that is responsible for risk management organization as a whole.

6. Monitor and Review

Monitoring and reviewing the components that need to be implemented to ensure that:

a Risk exposure is monitored, evaluated and revised from time to time;

b Risk exposure is updated in a timely manner in response to significant events such as changes in the organization's operations and influence external events;

c Ensure that improvements control is identified effectively and efficiently both in design and operation;

d Identification of emerging risks, and

e The risk management framework should operate effectively.

Communication and consultation related to mechanisms is used to implement components of the risk management framework that needs to be applied in the management of the organization accompanied by the monitoring process. Table 6 below provides a guidelines to the successful implementation and effectiveness of the Security Risk Management System sustainability.

Table 6. Management and Monitoring for Security Risk Management System

ISO 27001 SMKI Process	Risk Management System Security
Plan	Assign Security Risk Management Framework, applicable policies, objectives, processes and procedures relevant to managing risk and improving security to deliver results in accordance with the policies and objectives of the entire organization.
Do	Implement and operate the Risk Management Framework policy, controls, processes and procedures.
Check	Assess and, if possible, measure process performance against the Risk Management Framework policy, objectives and practical experience and report the results to management for review.
Act	Take corrective and preventive actions, based on the results of internal audits and management review or other relevant information in order to achieve continual improvement of the Risk Management Framework.

Source: Processed data

4.2. Framework for Information Security

Organizations need a framework that takes into account different types of risks. Organizations should assess how the security involved with the strategy and direction of the organization. Strategic direction and technical implementation guides layered approach to smart grid security. Strategic directions include the requirements and driver for business processes. Technical implementation, including the supporting application security, personal data, data integrity, physical security, network security, security meter, encryption and operational processes. In this approach, each layer of the data used and the impact of security requirements is based on the level of accountability and responsibility within the organization.

Implementation of the technology can change business processes and generate security problems across the organization. To understand the changes and fears can help the implementation team to make the right security decisions. If the business processes are not involved early, the organization may make a decision on long-term technology that is more costly to re-engineer in the later process. It is usually cheaper and more effective to consider things such as the process early.

The increased volume of data from the smart grid system introduces data management and privacy considerations related to data collection, the collection of personal information, incident management and planning of the offense, and leakage of personal data.

The organization shall plan different security scenarios by conducting vulnerability assessment and threat profiling and to develop a security management plan. An effective risk assessment and risk mitigation security must be resolved at the initial stage. It is very important for the selection of vendor or equipment.

- Vulnerability assessment: The organization should identify and assess vulnerabilities for each component of the smart grid infrastructure. The process must provide a gap analysis, risk assessment, observations and recommendations to reduce risks and improve security infrastructure.
- Threats profile: Organizations should utilise scenario planning and exercise testing to address different threat profile. Threats profile including curiousity and tappers, unethical customers, disturbing a third party and an active attacker.

Security management plan: Develop a security management plan including the use of automated vulnerability scanning, manual vulnerability testing and technical configuration assessment services.

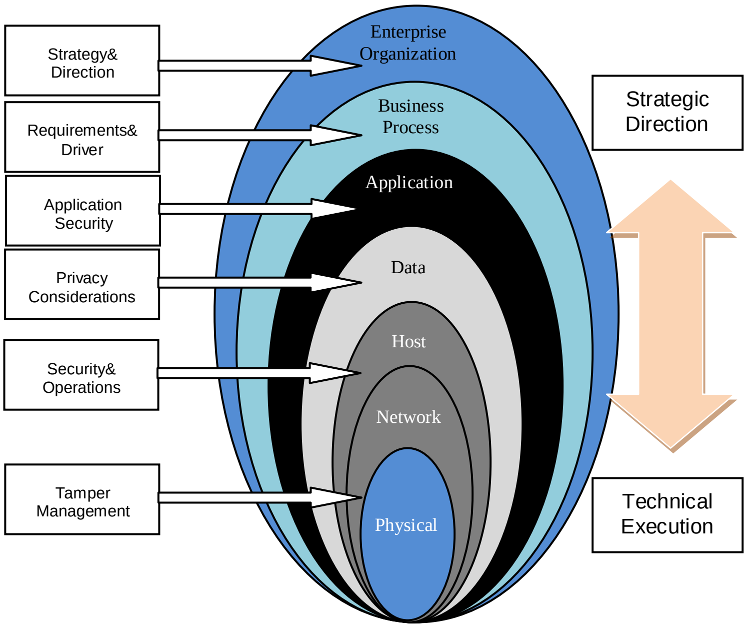

Figure 6. Multi-layered Critical Infrastructure Security Framework

4.3. Information Security Strategy on National Critical Infrastructure

Security of National Critical Information Infrastructure is an absolute prerequisite that must be implemented in Indonesia in order to ensure the effectiveness of reliability, availability, and integrity of information networks, both nationally and globally. However, a huge impact and the potential disruption and threat to the national critical infrastructure security is still not fully realized by the community. It is now lurking on us all. This is evident from the unavailability of National Critical Information Protection policy and the unmapped/unclassified National Critical Infrastructure, especially information network infrastructure.

Threats to the Security of National Critical Information Infrastructure can lead to a loss that is invaluable to stability, economy and even sovereignty. The Government needs to take measures and preventive measures to ensure that every effort that could threaten the stability of the country can be prevented and the perpetrators can be investigated by law and subject to serious criminal threats.

Related to the foregoing, a practitioner of telecommunications and also Chairman of the Indonesian Telecommunication Users Group (IDTUG), Ari Sutedja K in an interview, suggested some of the steps that can be taken by policy makers related to the protection of critical information infrastructure. The first step in protecting the Critical Information Infrastructure includes an introduction to the potential of existing threats (threat profiling) and potentials of infrastructure weaknesses (infrastructure weaknesses profiling) in order to suppress the risk of threats and interference that might occur. Secondly, reduce losses that have occurred and the recovery time in case of a disturbance. The third step is to find and identify the cause or source of the disorder that can then be studied and analyzed forensically (e-forensic) by experts and investigators from the law enforcement officers.

Fourthly, the need for coordination, communication (openness), and cooperation nationally and internationally from stakeholders, including the Agency for the Protection of National Critical Infrastructure Network (if applicable), the police and intelligence apparatus. Efforts such as cooperation should continue to refer to regulations that protect the security of information and rules of law relating to legal aid and the protection of personal rights (privacy law).

He also noted that the government should also be able to apply Eleven Principles of Critical Information Infrastructure Protection proposed by the countries members of the G8 countries in May 2003, includes strategies to reduce the risk against the potential threats and disturbance against national critical information infrastructure, among others;

1. The first principle; stressed that the government should have an emergency early warning networks to monitor weaknesses, threats and occurrence of the National critical information infrastructure.
2. The second principle; the government is obliged to increase the sensitivity in facilitating the understanding of stakeholders on the nature and state of critical information infrastructure at hand, and what role should be played by them.
3. The third principle; and the government should be able to examine and identify the nature of the interdependence of its various critical infrastructure in order to improve the protection of such infrastructure.
4. The fourth principle; the government should encourage a partnership program with stakeholders, both public and private sectors, in sharing and analyzing critical information infrastructure in the framework of prevention, investigation, and actions to loss or disturbances that have occurred to the infrastructure.
5. The fifth principle; government is obliged to establish and maintain a Crisis Information Network and to test and protect its reliability in emergencies.
6. The sixth principle; the government should be able to ensure that the policy on the disclosure of information must also be able to refer to the need for protection of national critical information infrastructure.
7. The seventh principle; the government should facilitate the investigation of the disruption of national critical information infrastructure, and if possible share the information results of the investigation with other countries.
8. The eighth principle; the government should be able to facilitate various forms of training to improve the ability to react and to test the preparedness and contingency plans in case the disruption of national critical information infrastructure and shall encourage stakeholders to undertake similar activities.
9. The ninth principle; the government must ensure the availability of legal products which cover a wide range of activities above, officials who are trained and able to conduct the investigation and prosecution of disturbance, and to coordinate such investigations with other parties, including the countries associated with the disturbance.
10. The tenth principle; the government should actively bridge international cooperation to obtain a wide range of critical information, including developing and coordinating emergency warning systems, sharing and analyzing information weaknesses, threats and occurrence of critical infrastructure, as well as coordinating investigations with reference to the applicable laws and regulations.
11. The eleventh principle; the government should bridge the wide range of research activities, both nationally and internationally, as well as to encourage the use of various security applications that have been certified by the applicable international standards.

What is more important than these eleven principles is the need for coordination among stakeholders, both regulators and operators with regard to critical information infrastructure for the creation of harmonization. In addition, other efforts is to build a culture of cyber security itself that must start from the government (regulator) so that the wider community can also follow and imitate the culture.

4.4. Information Security Policy in Critical Infrastructure

National Critical Information Infrastructure Security is an absolute prerequisite that must be implemented in Indonesia in order to ensure the effectiveness of reliability, availability, and integrity of information networks, both nationally and globally. However, a huge impact and the potential disruption and threat to the national critical infrastructure security is still not fully realized by the public and its now lurking on us all. This is evident from the unavailability of National Critical Information Infrastructure

Protection policy and unmapped/unclassified National Critical Infrastructure, especially information network infrastructure.

Based on the analysis of the case of electricity smart grid as one of the critical information infrastructure, smart grid network system vulnerability will have an impact on aspects of Information Security. Within the framework of multi-layered smart grid security system, it is necessary to ensure that security measures have been performed in all of the activities. The process of securing is not only in real space but also in the cyber space within the smart grid as critical infrastructure. The process of securing cyber space can be done by using the Information Security Certification to ensure all required activities for security has already been done.

In the terminology of Law No. 11 of 2008 on Information and Electronic Transactions (UU ITE) and also on Government Regulation No. 82 of 2012 on the Implementation of the Electronic System and Transactions (PP PSTE), Electronic Transactions is defined as a legal act performed by using a computer, computer network, and/or other electronic media. Meanwhile, the electronic system is a series of electronic devices and procedures that serve to prepare, collect, process, analyze, store, display, publish, transmit and/or distribute electronically. The Electronic System Operator is any person, public operator, enterprises, and communities that provide, manage and/or operate an electronic system individually or jointly to the Electronic System User for his/her purposes and/or purposes of other party. Thus, the smart grid can be categorized as critical electronic systems and smart grid users can be categorized as critical Electronic System Operator.

In order to secure the cyber space in the Electronic System Operator, the ultimate goal is to be able to meet the security aspect of information, namely the Confidentiality, Integrity, and Availability. Furthermore, under Article 15 of UU ITE, it is stated that the Electronic System Operator has the obligation to conduct reliable, safe and responsible electronic systems. In addition, the regulations also set the Electronic System Operator to use an electronic certificate and be certified by the Reliability Certification Agency (Article 10 of UU ITE). In Article 41 of PP PSTE, it is also explained that the Implementation of Electronic Transactions in the public or private sector using the Electronic System for the benefit of public services must use Reliability Certificates and/or the Electronic Certificate.

In addition, given that information is an asset vulnerable to theft and modification, then the application of ISO 27001 certification as an information security management system is very important because it involves the use of information. Information security standards issued by ISO applies to all types of organizations, especially for the Electronic System Operator organizations that have electronic systems infrastructure with critical infrastructure category. The standard set out requirements for establishing, implementing, operating, monitoring, assessing, improving and maintaining Information Security Management System (ISMS) that is documented in the context of the organization's overall business risks.

5. Summary

5.1. Conclusion

Based on the results of the discussion in this study, it can be summed up as follows:

Implementation of risk management on critical information infrastructure can use RMF referring to ISO31000:2009 (Risk management -Principles and guidelines). The process consists of determination of context, risk assessment and risk treatment. Another component that can not be separated in the risk management process is communication, consultation, monitoring and review.

Determination of context of risk can be derived from the assets owned by the organization and the business processes associated with the electronic system operators who have critical information infrastructure. The risk assessment carried out to produce a list of risks, the analysis and evaluation of risks. Treatment of risk is determined as the last step taken to deal with the impact and likelihood of risks that have been identified previously. These processes are important steps in the implementation of a structured and ongoing risk management for critical information infrastructure.

5.2. Suggestion

Based on the study results and conclusions that have been described, some of the suggestions are:

As one of the stakeholders as well as the regulator, government related to the sectors of utilization of critical information infrastructure and Information Security sectors need to coordinate with each other in terms of the classification of critical infrastructure. In addition, regulations and standards should also be made related to securing critical information infrastructures, as well as mitigation.

In relation to the critical information infrastructure, Infrastructure Security policies on Electronic system need to be established which refers to the ISO IEC 31000. In the case of utilization of electronic certificates, the Ministerial Regulation on Root Certification (Root CA) shall be reviewed, in order to pay attention to the pattern of root CA for Critical Infrastructure. Information Security Management Certification is required to ensure that all activities on the infrastructure/critical information systems security has been done. Thus Circular Letter of MCIT on the use of SNI 27001 should need to be revised in view of the improved, relevant ISO.

6. Acknowledgements

The author would like to thank all those who have helped the completion of this research, especially the Research and Development Center of Aptika and IKP as funders.

Bibliography

Department of Defense (2012). DoD Policy and Responsibilities for Critical Infrastructure, Department of Defense USA.

Dunn, M. (2005). The socio-political dimensions of critical information infrastructure protection (CIIP), *Int. J. of Critical Infrastructures*, 1(2/3), 258 - 268

Gorman, S.P., Schintler, L., Kulkarni, R., aStough, R.R., (2004), *The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure*. Journal of Contingencies and Crisis Management, Vol. 12, No. 2, pp. 48-63, June 2004. Available at SSRN: http://ssrn.com/abstract=549768

Henderson, M., (2007). “Protecting Critical Infrastructure from Cyber Attacks,” Department of Homeland Security-USA, 2007.

ISO 31000:2009, (2009). *Risk management – Principles and guidelines*. Geneva

ISO/IEC 27001:2013 (2013). *Information technology -- Security techniques -- Information security management systems – Requirements.* Geneva

ISO/IEC 27002:2013 (2013). *Information technology -- Security techniques -- Code of practice for information security controls.* Geneva

Ko, M. dan Dorantes, C. (2006). *The Impact of Information Security Breaches on Financial Performance of The Breached Firms: an Empirical Investigation*, Journal of Information Technology Management, vol. XVII, pp. 13-22.

Nayak, A. (2010). *Cyber Security: Indian perspective.*

Nickolov, E. (2005). *Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations,* INFORMATION & SECURITY. An International Journal, Vol.17, pp. 105-119

NIST, (2007). *NISTIR 7628 Guidelines for Smart Grid Cyber Security*, Smart Grid Interoperable Panel (SGIP) Cyber Security Working Group, NIST, US Depertement of Commerce.

NIST, (2014). *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, US Depertement of Commerce, v. 1.0

OECD, (2008). *Recomendation of The Council on The Protection of Critical Information Infrastructure, OECD Ministerial Meeting on The Future of Internet Economy*, Seoul, South Korea

Su, X. (2006). *An Overview of Economic Approaches to Information Security Management*, University of Twente, Information Systems Group, Enschede, The Netherlands.

Suter, M. (2007). *A Generic National Framework For Critical Information Infrastructure Protection (CIIP)*, Center for Security Studies, ETH Zurich.