www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia

Farouq Aferudin[1], Kalamullah Ramli[2*]
[1,2]*Departement of Electrical Engineering, Universitas Indonesia*
*farouq.aferudin@ui.ac.id**, *kalamullah.ramli@ui.ac.id*

Abstract

The increase of cyber attacks in the Critical Information Infrastructure (CII) requires every organization to collaborate through Cybersecurity Information Sharing (CIS). To support the implementation of the CIS, governance support is needed in the form of a framework that can be used as a reference. This study focuses on developing a CIS framework for the CII sector in Indonesia which consists of three main outputs, namely the proposed ecosystem, the proposed framework and the recommendations for the implementation of the framework. The proposed framework is based on standards including ISO/IEC 27032, NIST SP 800-150 and ENISA ISAC in a Box, based on best practices for implementing CIS and best practices for implementation in other countries including the United States, Australia, United Kingdom, Singapore and Canada. To validate, the expert judgment method was used to obtain suggestions for improvement. The expert judgment method was also carried out quantitatively to measure interrater reliability between experts using Fleiss Kappa Statistics. The measurement results show a kappa value of 0.938, which means that the proposed framework implementation recommendation gets an agreement from the experts at the almost perfect agreement level.

Keywords
cybersecurity information sharing; critical information infrastructure; framework; fleiss kappa statistic

I. Introduction

In the current era of digital transformation, information and communication technology (ICT) has become the main support for the sustainability of critical infrastructure operations so it is known as Critical Information Infrastructure (CII). At this time, disturbances that may threaten the operational sustainability of CII are not only physical disturbances but also cyber threats. The results of cyber security monitoring carried out by the Indonesian National Cyber and Crypto Agency (Badan Siber dan Sandi Negara / BSSN) stated that throughout 2021 there were more than 1.6 billion network traffic anomalies which could indicate a cyber attack targeting various sectors, including government, individual, private sector to the CII sector. (Direktorat Operasi Keamanan Siber, 2021). The number of cyber attacks that are increasingly massive, must be faced with collaborative efforts from each party, one of which is Cybersecurity Information Sharing (CIS) (Pöyhönen, Nuojua, Lehto, & Rajamäki, 2019).

CIS is a collaborative effort within organizations to address cybersecurity challenges quickly and precisely in the CII sector, across sectors, nationally and internationally. (Luijijf & Kernkamp, 2015). The CIS will prepare all stakeholders to better assess vulnerabilities, understand the potential and consequences of incidents, prevent, protect, and respond to and recover from various cyber threats and attacks. *(Critical Infrastructure*

Threat Information Sharing Framework - A Reference Guide to the Critical Infrastructure Community, 2016). In Indonesia, several CIS forums have been established formally and informally. One of the established CIS forums is the ICT-ISAC which was formed by the Ministry of Communication and Information to accelerate cybersecurity risk mitigation. (Kominfo, 2018). Apart from ICT-ISAC, several CIS forums have also been established informally, such as Financial-CIS, which consists of the Association of State-Owned Banks. On the regulatory side, it has also been regulated regarding the implementation of CIS which is contained in Presidential Regulation No. 82 of 2022 concerning the Protection of CII.

The implementation of CIS needs to get support for several aspects such as governance. Especially in the CII sector, CIS must be implemented based on good governance through a structured framework to meet the need for collaboration between CII owners in the private sector and the government in the public sector to achieve cybersecurity situational awareness. Currently, there are several CIS frameworks issued by several organizations such as ISO 27032 Information Technology - Security Technique - Guidelines for Cybersecurity. (Standarization, 2012) , NIST SP 800-150 *Guide to Cyber Threat Information Sharing* (Commerce, 2016) and ENISA ISAC in A Box ((ENISA), 2022). However, none of the above frameworks has specifically provided guidelines for the implementation of CIS in the CII sector.

This research will focus on developing an optimal CIS framework for the CII sector in Indonesia. This framework will be realized through a qualitative approach by analyzing of various CIS standards and guidelines, best practices for implementing CIS, implementing CIS in the CII sector in other countries and adapting to the conditions in Indonesia. The results of the analysis will produce a proposal that will be validated using the expert judgment. This validation aims to measure the quality and get input on the proposed framework. In addition, the proposed framework implementation recommendations will also be assessed quantitatively to measure the level of agreement using Fleiss Kappa Statistics. The final result of this research is a CIS framework for the CII sector which will then be recommended to be implemented in Indonesia.

II. Review of Literature

2.1 Cybersecurity

Cybersecurity is an approach and action related to the security risk management process followed by organizations and countries to protect the confidentiality, integrity and availability of data and assets used in cyberspace (Schatz, Bashroush, & Wall, 2017).

2.2 Critical Information Infrastructure (CII)

CII is an information infrastructure whose failure or operational limitations due to natural or man-made disasters will have a tremendous impact on the vast majority of citizens. This impact is not only direct damage due to the failure of CII but also the indirect damage caused by the effect of CII failure on other infrastructure that has dependence (*CIIP Guidelines Ver. 3.0*, 2016).

2.3 Critical Information Infrastructure Protection (CIIP)

CIIP can be defined as an effort to protect the system provided or operated by critical infrastructure providers such as energy, telecommunications, water, etc (Standarization, 2012) (Osmani). The ASEAN-Japan CIIP framework consists of 6 pillars including policy coordination, CII identification, CII protection, information sharing, incident handling and

capacity building. From the frameworks, it can be seen that the CIS program is part of the pillar of CII protection ((AMS), 2019).

2.4 Cybersecurity Information Sharing (CIS)

The concept of CIS was first put forward by the US Government in the late 1990s which includes the sharing of cybersecurity information between countries, and between governments at all levels (Yang, Ji, Yang, & Xue, 2019). CIS forums are generally built to respond to the need to involve actors in the private and public sectors to collaborate in secure entities to reduce the impact of cyber threat risks (Ghernaouti, Cellier, & Wanner, 2019).

2.5 Cybersecurity Information Sharing Framework

a. NIST SP 800-150

This standard was issued by NIST in 2016 to guide on establishing and participating in CIS relationships. These guide assists organizations in setting CIS goals, identifying sources of information, scope of activities, developing rules for distributing information and making effective use of information to support overall cybersecurity practices. (Commerce, 2016).

b. ISO/IEC 27032

This standard consists of two focus areas wherein the first area focuses on cyber security issues that try to bridge the difference in security domains in the cyber world. (Standarization, 2012). The framework for coordination and sharing of specific information is discussed in section 13 of this standard which consists of general, policies, method and process, people and organization, technical, and implementation.

c. ENISA ISAC in A Box

ENISA ISAC in a Box is a toolkit issued by ENISA to build and develop ISAC which includes activities, documents, and tools needed to prepare and run ISAC ((ENISA), 2022). This toolkit is divided into 4 different phases according to the development of ISAC. Each phase contains different topics to develop the organization in a particular phase. These topics have been classified into 2 types, namely "new" and "established".

2.6 Implementation of CIS in Other Countries

In this section, a comparative study is conducted on the implementation of CIS in the CII sector in other countries. Countries where this comparative study is conducted are countries that are considered good at implementing cyber security based on the 2020 Global Cybersecurity Index (GCI). For Indonesia, it is ranked 24 out of 182 countries (Union, 2020). The results of the comparison can be seen in Table 1.

Table 1. Implementation of CIS in Other Countries

Cybersecurity Coordinator Organization	The Role and Position of the Government in CIIP	Owned Cybersecurity Regulations	CII Sector Identification	CIS Organization	CIS Method	*Success Factor* CIS
AUSTRALIA (Rank 12 out of 182 Countries in the Global Cybersecurity Index)						
The Attorney General's Office oversees CSCP, CERT, (Australia, 2009).	Develop CIIP programs (Australia, 2009)	Security of Critical Infrastructure Act 2018; Critical Infrastructure Bill 2020;	9 Sector (Departement of Home Affairs, 2021) (Government, 2020)	Australian Cyber Security Center (ACSC) (Nevill, 2017).	Via the TISN platform and supported by JCSC (Australia, 2009)	Support university funding and contributions (Australia, 2009)

Cybersecurity Coordinator Organization	The Role and Position of the Government in CIIP	Owned Cybersecurity Regulations	CII Sector Identification	CIS Organization	CIS Method	*Success Factor* CIS
UNITED STATES (Rank 12 out of 182 Countries in the Global Cybersecurity Index)						
Cybersecurity and Infrastructure Agency (CISA) (Agency, 2022).	As an integrator and hub in compiling a program (MITRE, 2017).	CII Act 2002; The Cyber Security Information Act 2015	16 Sector ((CISA), 2022a)	Fusion Center, ISAC, ISAO, HSIN-CI	Via NICC platform, CISA Gateway, PCII,((CISA), 2022b).	Incorporating CIS in the strategy. (Departement of Homeland Security, 2018)
CANADA (Rank 12 out of 182 Countries in the Global Cybersecurity Index)						
Canadian Center of Cyber Security (CCCS)	Building strategic partnerships with CII owners (Cybersecurity, 2021).	The SCIDA 2019 (Canada, 2022); National Strategy CIIP	10 Sector (Cybersecurity, 2021)	Canadian Cyber Threat Exchange (CCTX) (Exchange, 2022).	Using CCTX as an expert discussion forum (Exchange, 2022).	Cooperating with other countries in the CIIP program (Right, 2009)
SINGAPORE (Rank 12 out of 182 Countries in the Global Cybersecurity Index)						
Cyber Security Agency (CSA) (G. o. Singapore, 2022).	Organizing the CII protection program by including it in the Act.	Cyber Security Act 2020; Singapore Cybersecurity Strategy	11 Sector	Operational Technology - ISAC (C. S. A. o. Singapore, 2020).	Using OT-ISAC to share information. (Federation, 2021).	The law requires information sharing in the CII sector.
UNITED KINGDOM (Rank 12 out of 182 Countries in the Global Cybersecurity Index)						
National Cyber Security Center (NCSC) as part of GCHQ ((NCSC), 2021).	Establish Center of Protection of National Infrastructure (CPNI) (Infrastructure, 2021).	Network and Information Systems Regulations 2018; National Cyber Strategy 2022	13 Sector ((NCSC), 2022)	Cyber Security Information Sharing Partnership (CISP) ((NSCS), 2022).	Using CISP Collaboration Tools ((NCSC), 2018).	CIS as a national strategy, raised the issue of CIS in the G7 presidency (Office, 2022).
GENERALIZATION						
Each country has a cybersecurity coordinating organization whose position is adjusted to the form of government of each country.	The role and government in protecting CII as program organizers, as a hub and building strategic partnerships.	Referral countries have law-level regulations related to Cyber Security and CIIP.	There are differences in identification, but generally included: Government, Finance, ICT, Energy Heatlhcare, Transportation.	Each country has a specific organization for the CIS.	Each has a specific platform within the CIS to improve the effectiveness and efficiency of CIS	There are 3 factors : existence of trust, technology support and the adhesive factor.

2.7 Related Works

Several previous studies have been conducted relating to the development of a CIS framework with different output focuses. Development is a change towards improvement (Shah et al, 2020). The development of the CIS framework was carried out to discuss 4 aspects related to collaboration in terms of cyber defense to improve cyber defense information sharing (Fernández Vázquez, Acosta, Brown, Reid, & Spirito, 2012). Another development is carried out by examining the CIS on MSMEs in the UK as a result of increasing cyber threats in the sector by assessing the implications and adopting cybersecurity metrics. (Lewis, Louvieris, Abbott, Clewley, & Jones, 2014). Other research also conducted a literature study related to incentives and challenges that affect organizations in implementing cybersecurity information sharing practices with the Technology, Organization, Environmental (TOE) framework (Kolini & Janczewski, 2021).

III. Research Method

3.1 Research Stages

The research is based on qualitative methods consisting of interviews, observations, literature studies and validation with expert judgment. This framework is prepared based on an analysis of various standards and refers to the best practice issued by various cybersecurity organizations as well as the implementation in other countries and then adapted to ecosystem in Indonesia. The results of this study consist of 3 outputs, namely the proposed ecosystem, the proposed framework and recommendations for its implementation. The 3 outputs were then validated through expert judgment to get advice on the proposal. The validation results will be used to make improvements to the framework. The stages of the research carried out consisted of 7 stages of research which are depicted in Figure 1.

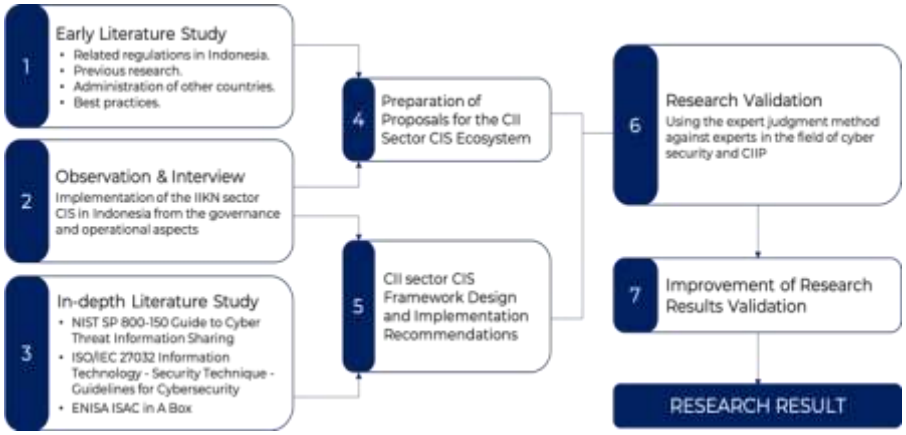

Figure 1. *Research Stages*

3.2 Data Processing Method

Data processing is carried out qualitatively and quantitatively. Qualitative data processing includes 3 steps, namely data reduction, data presentation, as well as drawing conclusions and verification (Sugiyono, 2015). Quantitative data processing uses Fleiss Kappa Statistics to determine the level of agreement of the expert. Fleis Kappa is a developed version of Cohen Kappa Statistics which can be used to measure the level agreement of several raters in several categories (McHugh, 2012). *The level of agreement will be indicated by Kappa Value (κ) and calculated using the formula*:

$$(\kappa) = \frac{\Pr(a) - \Pr(e)}{1 - \Pr(e)}$$

Kappa Value of 0.7 indicates acceptable approval (Brennan & Prediger, 1981). Another interpretation method that defines interpretation into 6 ranges as follows (Landis & Koch, 1977):

Table 2. Landis and Koch's Interpretation of Fleis Kappa Statistics

Kappa Value	Interpretation
$\kappa \leq 0$	*No agreement*
κ *between 0.01 dan 0.20*	*Slight agreement*

between 0.21 dan 0.40	*Fair agreement*
between 0.41 dan 0.60	*Moderate agreement*
between 0.61 dan 0.80	*Substantial agreement*
between 0.81 dan 1.00	*Almost perfect agreement*

IV. Results and Discussion

4.1 Results

a. Analysis of CIS Implementation in Other Countries and Conditions of CIS Implementation in Indonesia

At this stage, an analysis of the implementation of CIS in other countries is carried out. In the organizational aspect, it is found that out of the 5 countries, all countries have cybersecurity organizations. Regarding CIS organizers, 4 out of 5 countries have their own organizations that serve as CIS implementers. The formation of this separate organization shows the government's seriousness in encouraging the CIS ecosystem, this shows that the organization is an important aspect in the development of a CIIP ecosystem. Regarding the regulatory aspect, 2 countries have cybersecurity laws (US and Singapore) and 2 countries have CIIP protection laws (Australia and the US). This shows that a legal at the level of a law is needed by a country to be able to protect the country from all cyber threats. In relation to the role of the government, there are 2 main roles of the government in CIIP, namely as a compiler for the CIIP program and as a liaison (hub) in the implementation of CIS. The government's most appropriate role is as a catalyst in the implementation of the CIS. Several success factors for implementing CIS in the CII sector include trust among members, technological support and adhesive factor in the form of regulations, strategies or other guidance.

The author also collects information related to the conditions of the implementation of CIS in Indonesia in governance and operations aspect by conducting observations and interviews. Interviews were conducted with 2 sources, namely the Director of Cyber and Crypto Governance Policy and the Director of Cybersecurity Operations, BSSN. Based on the results of interviews related to governance, information was obtained that Indonesia does not yet have a special regulation at the level of the law for the implementation of cybersecurity, including the protection of CII. The highest regulation governing CIIP currently is Government Regulations 71 of 2019 concerning Electronic System and Transaction Operation which has been revealed in Presidential Regulation Number 82 of 2022 concerning Protection of CII. More technical regulations regarding the CIS are not yet required in the form of regulations, but rather require guidelines such as a framework. It is necessary to have a CIS framework that will be used as a guide in the implementation of CIS including the CII sector.

Based on the results of interviews with operational aspects information was obtained that the implementation of CIS in Indonesia focuses on sharing Cyber Threat Intelligence (CTI) information from the BSSN to stakeholders including the CII sector. Information sharing is carried out in one direction where BSSN shares CTI information to stakeholders and stakeholders can validate and enrich information. CIS sectoral operations have been carried out non-formally by several CII sector organizations. Several types of information distributed by BSSN to stakeholders include tactical/technical, operational and strategic information. It is necessary to have a special mechanism through an automation system to be used in CIS on national and sectoral scopes.

b. Proposed CII Sector CIS Ecosystem in Indonesia

The following is a proposed CIS ecosystem that has been validated using the expert judgment against 3 experts in the field of cybersecurity and CIIP in Indonesia. Experts provide advice and input based on their experience and knowledge, then researchers refine the framework based on suggestions and input from experts. In the CII sector CIS ecosystem, it is proposed that there are 3 main entities, namely Authority, Information Provide Organization (IPO) and Information Receive Organization (IRO) where these three entities are connected in a CIS ecosystem as shown in Figure 2.

Figure 2. *CII Sector CIS Ecosystem*

IPO and IRO are organizations that are members of a CIS group. Each organization that is incorporated can become an IPO or IRO. An organization will go into an IPO when it has cybersecurity-related information to share with other organizations in the CIS group. An organization will become an IRO when it receives information from an IPO. Authority is an institution or organization tasked with carrying out a supervisory function related to the course of CIS activities. Authority can be either a regulator or an organization mandated according to the group agreement. In Indonesia, the organization is the Sector Regulatory and Supervisory Agency (Instansi Pengatur dan Pengawas Sektor/IPPS). IPPS is an agency tasked with overseeing the implementation of sector tasks and issuing regulations for the sector, for example Ministry of Transportation for the transportation sector.

The proposed CIS ecosystem consists of 2 types of CIS groups, namely Sectoral CIS and National CIS. The National CIS Group is formed and managed by BSSN. The Sectoral CIS can be formed by the IPPS, and each CII sector is proposed to have at least one CIS group. The eight proposed groups are as follows:

1. Government-CIS Group
2. Energy and Mineral Resource-CIS Group
3. Transportation-CIS Group
4. Finance-CIS Group
5. Healthcare-CIS Group
6. ICT-CIS Group
7. Food-CIS Group
8. Defence-CIS Group

The proposed ecosystem is also equipped with a coordination and reporting flow that has been adjusted to the relevant regulations as shown in Figure 3.

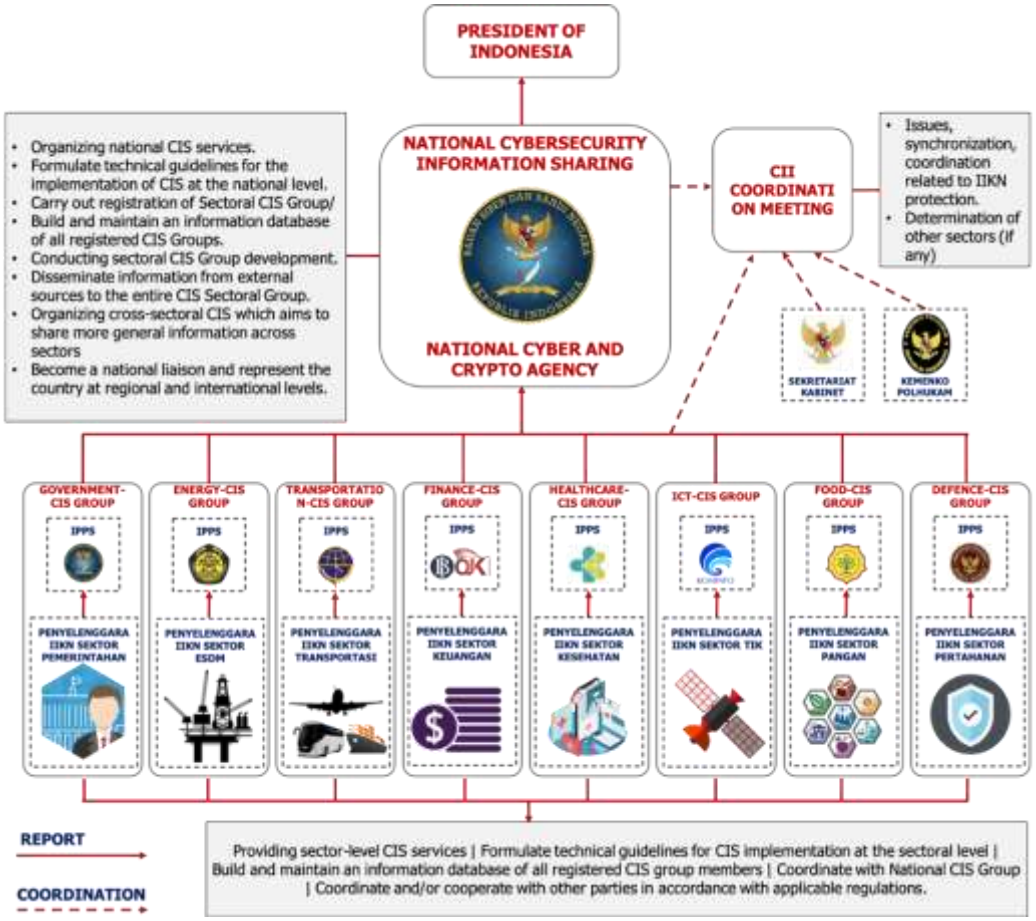

Figure 3. *Coordination and Reporting Flow of CIS Ecosystem*

Figure 3 shows that each CII sector has a CIS group that was formed together with IPPS and reports to the National CIS. Periodically or incidentally, the implementation of CIS can also be reported to the President of the Republic of Indonesia. In addition to carrying out its main activities, the CIS forum can also run a Coordination Meeting which can be held at least once a year with a coordination agenda related to current issues, including the implementation of CIS. The CII sector coordination meeting can also involve relevant ministries outside IPPS such as the Cabinet Secretariat and the Coordinating Ministry for Politics, Law and Security as the coordinating ministry for security.

c. Proposed CII Sector CIS Framework in Indonesia

The following is a proposed CIS framework that has been validated using the expert judgment. This validation is carried out to assess the suitability of the proposed framework with the expected conditions. From the validation results, it was found that the proposed framework has met the optimal conditions to be applied and can be one of the framework options for CIS implementation in the CII sector. The framework's activity components are based on 3 standards, namely ISO/IEC 27032, NIST SP 800-150 and ENISA ISAC in A Box. The framework is based on a process-based approach using the PDCA-Cycle. The results of the mapping are then generalized to the activity components to produce 12 activity components of the CIS framework shown in Table 3.

Table 3. Activity Mapping CIS Framework

Phase	ISO/IEC 27032	NIST SP 800-150	ENISA ISAC in A Box	Generalization
Plan	-	Goals and Objective	Goal and Purpose	Goals and Objective
	Participant	Internal Source	Participants	Participant and Roles
	-	Scope	Areas and Activities	Scope
	Audience	Rules	Governance Structure	Policy and Governance
	NDA			
	Code Practice	Join Community	Funding	
	Contacts			
	Alliances			
Do	Coordination Protocol	Organize Information	Information Exchange	Technique and Tools
	Classification & Categorization	Produce Indicator	Meeting	Produce Information
	Timing and Scheduling	Consume Alerts	Governing Rules	Consume Information
		Consume Indicator		
	Information minimization	-	-	Information Standardization
	Testing&Drills			
	Data Standardization			
	Data Visualization			
	Cryptographic Key			
	Secure File Sharing			
	Testing Sistem			
	-	-	Trust	Building Trust
	Awareness and Training	-	Capacity Building	Capacity Building
Check	-	-	Follow Up & Evaluation	Evaluate
Act	-	-	Develop and Enhance	Improvement
			Outreach	
			Added Value	

The results of the analysis of the activities of the framework are then grouped into PDCA-Cycle to produce a CIS framework for the CII Sector in Indonesia as shown in Figure 4.

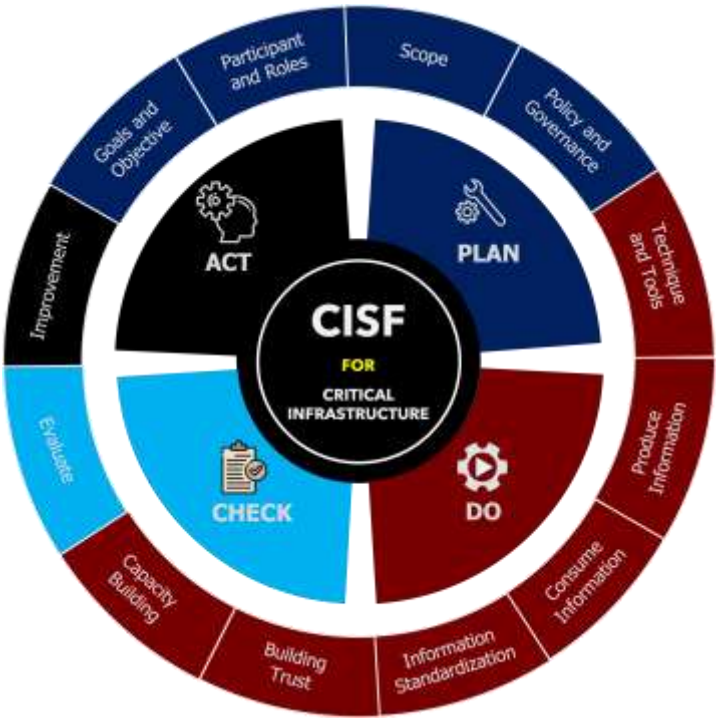

Figure 4. *CII Sector CIS Framework*

The framework consists of 4 stages, namely Plan, Do, Check, Act which is arranged in a life-cycle and consists of 12 activities which are described in Table 4 as follows:

Table 4. Explanation of the CII Sector CIS Framework

Code	Activity	Explanation
PL.01	Define goals and objectives.	Determine the purpose of forming the group, the agreed vision and mission, the expected outcome of the formation of the group.
PL.02	Define participants and member roles	Identify the organizations that can be group participants, the role profile criteria of each group.
PL.03	Determine the scope of activity.	Deciding what services will be implemented in the group
PL.04	Develop governance and regulations.	Developing CIS business processes, compiling SOP, compiling technical guidelines, identifying regulations.
DO.01	Determine the techniques and tools.	Identifying the tools needed to share information can be in the form of email, websites, collaboration platforms.
DO.02	Define CIS mechanisms.	Contains procedures for sharing information, including anonymizing mechanism, determining the classification of information through TLP.
DO.03	Determine the mechanism for receiving information.	Contains the rules for receiving information, including the mechanism for validating the information received, and for storing information.
DO.04	Determine the standardization of the information shared.	Contains rules related to standardization of information to be shared.
DO.05	Build trust between participants	Contains strategies and mechanisms to build trust among CIS group members.
DO.06	Increase the capacity and capability.	Contains plans for establishing programs that can be used to increase the capacity and capability of groups and members.
CH.01	Conducting implementation evaluation	Contains an evaluation mechanism for the implementation of the CIS group.
AC.01	Develop groups based on evaluation results.	Making improvements to the evaluation results of group implementation to produce a better CIS group.

This research produced 44 recommendations consisting of 15 at the Plan stage, 19 at the Do stage, 7 at the Check stage and 3 at the Act stage, where at the validation stage there were 3 additional recommendations based on expert suggestions so that the number of recommendations became 47 recommendations as shown in Table 5.

Table 5. Recommendations for Implementation of the Framework

Activity	No	Recommendation
Recommendation for "Plan" Stage		
Goals and Objective	1	The purpose, vision and mission of the group formation must be defined at the outset.
	2	Goals and objectives are set and agreed upon by group members and documented in writing.
Participant and Roles	3	Ministries/Institutions can facilitate or initiate the formation of groups.
	4	The number of participants in one group must be regulated so that the implementation of CIS can run effectively and efficiently.
	5	Members representing the organization in the group must have sufficient capability.
	6	In the group, the group set consists of at least a chairperson and a secretary
	7	In compiling the CIS group, it is necessary to consider the risk profile and capabilities of each organization in a sector.
Scope	8	Determination of the scope must refer to the goals and objectives of the formation the group.
	9	The scope of information that is divided into groups includes cyber threats, cyber vulnerabilities, cyber incidents, mitigation measures, good practices, security trends, strategic analysis, and lessons learned.
	10	The group can carry out other activities beside main activity.
Policy and Governance	11	In carrying out CIS cooperation, each participant must enter into a cooperation agreement that has been agreed upon by the group.
	12	Ministries/Institutions can form regulations/guidelines for the implementation of CIS
	13	Groups must have a Personal Identifier Information (PII) policy.
	14	The Group prepares SOP for the implementation of CIS.
	15	The Group must have a policy for handling sensitive information.

Activity	No	Recommendation
	16	Funding for the formation and operation of the group can come from member agreements or it can also be by the Government
	17	The Group determines the SOP when there is a dispute in the implementation of information sharing, including if there is a need for sanctions.
Recommendation for "Do" Stage		
Tools and Technique	18	Information can be exchanged through various methods including automation systems, collaboration platforms, encrypted email or physical meetings.
	19	The information shared is classified under the terms of the Traffic Light Protocol (TLP).
Produce Information	20	The IPO must classify and categorize the information to be shared with other members.
	21	The IPO must process the information before it is shared with other members/
	22	The IPO must match the information to be shared with the agreed standard data format.
Consume Information	23	The IRO must agree to and follow the terms of protecting the information being shared.
	24	The IRO must ensure that the information comes from a reliable source.
	25	The IRO must properly manage the information received.
Information Standarization	26	Information sharing timing and scheduling must be clearly defined
	27	Groups can use automated systems for real-time information sharing, analysis and assessment.
	28	Information sharing systems must provide a cryptographic system including key exchange methods to facilitate the sharing of confidential information
	29	The information shared must be based on a predetermined standard format.
Building Trust	30	IPPS held a formal kick-off meeting.
	31	The criteria for additional participants to join the group must be agreed upon by all members.
	32	Trust between members must be built properly.
	33	The Group provides an IPO anonymity service for some sensitive information.
	34	Collaborative platforms used for CIS facilities must be guaranteed to be secure.
	35	Each group member can build other social relationships to increase trust among members.
Capacity Building	36	The Group conducts capacity building for its members.
Recommendation for "Check"Stage		
Evaluate	37	The Group makes an annual report on the organization of the group.
	38	The Term of Reference document should be evaluated regularly.
	39	The quality and effectiveness of information exchange is evaluated.
	40	The contribution of each member needs to be evaluated.
	41	Structured evaluation is carried out using Key Performance Indicators (KPI).
	42	Regulations related to CIS must be evaluated periodically.
	43	The Group conducts a self-assessment of the CIS implementation.
Recommendation for "Act" Stage		
Improve	44	The results of the evaluation of group organization can be used as a basis for consideration of increasing the group's capacity and capability.
	45	Capacity building and capability must be approved by all group members.
	46	When the group has reached a high level of maturity, it is necessary to consider breaking certain themes, topics or activities into working groups.
	47	Review all items in “DO” and “CHECK” and correct them if they don't work perfectly or expand their scope if they work perfectly.

All of the implementation recommendations were then validated quantitatively using Fleiss Kappa Statistics. Experts are asked to respond to the form of approval (agree/disagree) on each point of the proposed recommendation. From the validation results obtained 40 recommendation points where all experts have the same response and 4 recommendation points where experts have different responses. Based on the results of the Fleiss Kappa Statistic calculation, the Kappa Value (κ) is 0.938, which means it can be accepted or is at the level of almost perfect agreement. In addition to measuring the level of agreement, improvements were also made to 4 recommendation points that were experts have different responses.

4.2 Discussion

This framework is expected to be one of the options in determining the guidelines for the implementation of the CII sector CIS in Indonesia. The specificity of the CII sector in Indonesia can be seen in the proposed ecosystem framework. For the framework and recommendations can be used generally by organizations that will implement the CIS. The results of this study are addressed to the CII sector which does not yet have a CIS group. However, it is possible that the CII sector that already has a CIS group can use the framework as a means of evaluating implementation. The activities proposed in the framework are the minimum recommended activities to be carried out by the CII sector which will organize a CIS group. Regarding best practice in other countries, the most compatible country to serve as an example in implementing the CIS is the United States. This is because the country already has maturity in terms of governance and operational implementation of the CIS.

About the results of research validation, the number of experts will affect the quality of the research. The more experts, the more suggestions will be obtained so that the research is more comprehensive. The difference in the number of experts will also affect the Kappa Value. This research is still very open for development, such as evaluating the framework by using a specific locus or by developing a framework by adding or adjusting usage for organizations that have built a CIS group.

V. Conclusion

Some conclusions that can be drawn from this research are that the implementation of the CII sector CIS in Indonesia has been carried out formally and informally. In the national scope, CIS is carried out by BSSN. In the sectoral scope, several CII sectors have initiated the formation of an informal CIS forum. In responding to the challenges of implementing CIS, a CIS framework for the CII sector in Indonesia has been developed which is based on standards, best practices and comparisons from other countries, also adapted to the conditions in Indonesia which consists of 3 main outputs, namely the proposed ecosystem, the proposed framework and the recommendation for the implementation. This framework consists of 12 activities based on the PDCA-Cycle covering the stages of planning, implementation, evaluation and development and accompanied by implementation recommendations consisting of 47 recommendations. All research outputs have been validated through the expert judgment against 3 experts in the field of cybersecurity and CIIP. Validation is also carried out through quantitative methods to measure interrater reliability between experts with Fleiss Kappa Statistics and shows a Kappa Value of 0.938 which means it is acceptable or is in the almost perfect agreement range. The results of this research can be used by BSSN, Ministries/Institutions as IPPS and owners CII as a guide in organizing the CIS group, especially in the CII sector in Indonesia. To develop this research, it can be tested by applying the framework that has been prepared in a CIS group that is national or sectoral or can develop a framework so that it can also be used for the already formed CIS group.

References

(AMS), A. M. S. (2019). *ASEAN Critical Information Infrastructure Protection Framework*.

(CISA), C. a. I. S. A. (2022a). Critical Infrastructure Sector.

(CISA), C. a. I. S. A. (2022b). Information Sharing Vital Resource.

(ENISA), E. U. A. f. C. (2022). ISAC in a Box. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/view#

(NCSC), T. N. C. S. C. (2018). Cybersecurity information Sharing Partnership (CiSP) Terms and Condition V5.0.

(NCSC), T. N. C. S. C. (2021). *Annual Review 2021 : Making the UK the safest place to live and work online*. Retrieved from

(NCSC), T. N. C. S. C. (2022). CNI Hub. Retrieved from https://www.ncsc.gov.uk/section/private-sector-cni/cni

(NSCS), T. N. C. S. C. (2022). CISP - Cyber Security Information Sharing Partnership. Retrieved from https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

Agency, C. a. I. (2022). About CISA. Retrieved from https://www.cisa.gov/about-cisa

Australia, C. o. (2009). *Australian Cyber Security Strategy*.

Brennan, R. L., & Prediger, D. J. (1981). Coefficient Kappa: Some Uses, Misuses, and Alternatives. *Educational and Psychological Measurement, 41*, 687 - 699.

Canada, P. S. (2022). Information Sharing for National Security. Retrieved from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/shrng-ns-nfrmtn-en.aspx

CIIP Guidelines Ver. 3.0. (2016).

Commerce, U. S. D. o. (2016). NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing. In.

Critical Infrastructure Threat Information Sharing Framework - A Reference Guide to the Critical Infrastructure Community. (2016).

Cybersecurity, C. C. o. (2021). Industri Collaboration. Retrieved from https://cyber.gc.ca/en/industry-collaboration

Departement of Home Affairs, A. G. (2021). Protecting Critical Infrastructure Systems. Retrieved from https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

Departement of Homeland Security, U. S. (2018). *United States Cybersecurity Strategy*.

Direktorat Operasi Keamanan Siber, B. S. d. S. N. (2021). *Laporan Monitoring Keamanan Siber 2021*. Retrieved from https://bssn.go.id:

Exchange, C. C. T. (2022). About CCTX : Canada's Only Cyber Threat Collaborations Forum and Source of Cyber Threat Intelligence. Retrieved from https://cctx.ca/about-cctx/

Federation, G. R. (2021). *A Year In Review - OT ISAC*. Retrieved from

Fernández Vázquez, D., Acosta, O., Brown, S., Reid, E., & Spirito, C. (2012). *Conceptual framework for cyber defense information sharing within trust relationships*.

Ghernaouti, S., Cellier, L., & Wanner, B. (2019, 23-25 Oct. 2019). *Information sharing in cybersecurity : Enhancing security, trust and privacy by capacity building.* Paper presented at the 2019 3rd Cyber Security in Networking Conference (CSNet).

Government, A. (2020). *The Australian Government's Critical Infrastructure Resilience Strategy: Plan*.

Infrastructure, C. f. t. P. o. N. (2021). Critical National Infrastructure. Retrieved from https://www.cpni.gov.uk/critical-national-infrastructure-0

Kolini, F., & Janczewski, L. (2021). Exploring Incentives and Challenges for Cybersecurity Intelligence Sharing (CIS) across Organizations: A Systematic Review. *Communications of the Association for Information Systems, 50*. doi:10.17705/1CAIS.05004

Kominfo, H. (2018). Perkuat Pertahanan Siber, Kominfo Bentuk CIIP ICT Sector. Retrieved from https://www.kominfo.go.id/content/detail/14509/perkuat-pertahanan-siber-kominfo-bentuk-ciip-ict-sector/0/berita_satker

Landis, J. R., & Koch, G. G. (1977). An application of hierarchical kappa-type statistics in the assessment of majority agreement among multiple observers. *Biometrics, 33*(2), 363-374. doi:10.2307/2529786

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). Cybersecurity information sharing: A framework for information security management in UK SME supply chains. *ECIS 2014 Proceedings - 22nd European Conference on Information Systems*.

Luijijf, E., & Kernkamp, A. (2015). *Sharing Cyber Security Information - Good Practice from the Dutch Public Private Participation Approach*. Clobal Conference on Cyber Space

McHugh, M. L. (2012). Interrater reliability: the kappa statistic. *Biochemia Medica, 22*, 276 - 282.

MITRE. (2017). Building a National Cyber Information Sharing Ecosystem. In.

Nevill, L. (2017). *Cyber Information Sharing : Lesson For Australia*. Retrieved from

Office, U. C. (2022). *National Cyber Strategy 2022 : Pioneering a cyber future with the whole of the UK*. UK Cabinet Office

Osmani, O. *Critical Information Infrastructure Protection (CIIP) - ITU Perspective*.

Pöyhönen, J., Nuojua, V., Lehto, M., & Rajamäki, J. (2019). Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations. *Information & Security: An International Journal, 43*, 236-256. doi:10.11610/isij.4318

Right, H. M. Q. i. (2009). *Canada National Strategy for Critical Infrastructure*.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law, 12*, 53. doi:10.15394/jdfsl.2017.1476

Shah, M. M., et al. (2020). The Development Impact of PT. Medco E & P Malaka on Economic Aspects in East Aceh Regency. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)* Volume 3, No 1, Page: 276-286.

Singapore, C. S. A. o. (2020). *Singapore Cyber Landscape 2020*. Retrieved from

Singapore, G. o. (2022). CSA Singapore : Our Organization. Retrieved from https://www.csa.gov.sg/Who-We-Are/Our-Organisation

Standarization, I. O. f. (2012). ISO/IEC 27032:2012 - Information Technology - Security Technique - Guidelines for Cybersecurity. In. Switzeerland: ISO

Sugiyono. (2015). *Metode Penelitian Pendidikan : Pendekatan Kuantitatif, Kualitatif, Dan R&D*. Jakarta: Panerbit Alfabeta.

Union, I. T. (2020). *Global Cybersecurity Index 2020*. ITU Publication

Yang, Y., Ji, G., Yang, Z., & Xue, S. (2019, 14-17 July 2019). *Incentive Contract for Cybersecurity Information Sharing Considering Monitoring Signals.* Paper presented at the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).