No. 326 | Received: 2020-06-13 | Revised: 2020-06-23 | Accepted: 2020-07-20

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
http://tip.ppj.unp.ac.id

Jurnal Teknologi Informasi dan Pendidikan
Volume 13, No. 2, Sept 2020
P. 9 – 16 | https://doi.org/10.24036/tip.v13i1

THE IMPLEMENTATION OF CYBER INCIDENT MANAGEMENT FRAMEWORKS IN INDONESIA

Rizky Hendra, S.ST[1]*, Dr. Margaretha Hanita, SH, M. Si[2]
[1] School of Strategic and Global Studies, Universitas Indonesia, Indonesia
[2] School of Strategic and Global Studies, Universitas Indonesia, Indonesia
Jl. Salemba Raya No.4, Kenari, Kec. Senen, Kota Jakarta Pusat, Jakarta
Corresponding Author: xrhendra@gmail.com : 081213314039

ABSTRACT

The rise of cyber attacks occurring in Indonesia could potentially cause incidents in institutions/companies. To anticipate these incidents, each institution/company need to prepare themselves by implementing proper incident management.There are a lot of incident management frameworks that can be used as a guideline in the implementation. But on the other hand, institutions/companies sometimes find it difficult to select the appropriate and suitable framework to use. The authors employed qualitative research methods using the data acquired from primary data (interviews) and secondary data (documentation).The data analysis techniques used were comparative analyses which included theoretical analysis, activity analysis, and analysis of the scope of incident management.The result of the analysis of the incident management scope was then validated using data triangulation method.Based on the theory analysis, there are differences on the 2 (two) compared incident management frameworks. These differences are seen from the definition of the activity-levelling scheme, definition of the maturity level of the incident management implementation, and the number of activities in the frameworks that can be implemented.The framework activities can be categorised into two, namely similar activities and different activities.There are 35 scopes of framework that can be considered as incident management processes.

Keywords: framework, incident management, SIM3, CREST

INTRODUCTION

The rapid development of information technology (IT) has brought significant changes in people's lives.Most Indonesians are familiar with the use of IT.This can be seen in the pattern of community consumption, lifestyle, needs, education patterns, and others. On the other hand, this condition has been utilised by service providers to improve their services to the public. IT utilisation also indirectly promotes good, effective and efficient governance, thus increasing the level of public trust in the service providers both within the scope of public and private sectors.

One of the challenges faced in the utilisation of IT is the emergence of vulnerabilities and threats to the information security system and lack of information security awareness among many of the Indonesians. Based on the Annual Report released by BSSN, there were 290.38 million cyber attacks that invaded Indonesia [1]. The majority attacks were dominated by data breach (137.4 million attempts) and attacks by means of malware/Trojan (117.9 million cyber attacks). The report also asserted that Indonesia is the most targeted country for cyber attacks.

The aspect of planning in anticipating threats and cyber attacks is an issue that service organisers need to take into account, so that the potential impacts resulted from cyber incidents can be minimised. Risk and impact management has become a mandate that must be implemented by all Electronic System Organisers (PSE) based on the Government Regulation No. 82 of 2012 on the Implementation of Electronic System. Therefore, the implementation of incident management is required for every service provider in Indonesia.

There are several frameworks that can be used as a reference in implementing incident management. The challenge, however, is that

Jurnal Teknologi Informasi dan Pendidikan
Volume 13, No. 2, Sept 2020
http://tip.ppj.unp.ac.id

institutions/companies often have difficulty in finding the most suitable framework that best fits in their service business process. Taking this condition into account, the authors conducted a research on 2 (two) incident management frameworks that have been widely used by institutions/companies in managing incidents, i.e. SIM 3 framework and CREST framework.This research is expected to contribute in providing an overview to every institution/company in Indonesia regarding which incident management framework they can employ as well as which level of approach and which activities are in accordance with the capabilities and needs of the institution/company in implementing cyber Incident management in its organisation.

RESEARCH METHODS

The research used qualitative method, in which the researchers conducted this research without using data quantifying process. A qualitative approach is used to construct the real knowledge of the research object based on both constructive or participatory perspectives [2]. The author also used descriptive research approach to present the acquired data.Descriptive research is a study that seeks to describe or explain as closely as possible about a matter based on the data [3].

Two sources of data used by the researchers were primary data and secondary data.Primary data is the data obtained from interviews, while secondary data is the data that can be in the form of journals, policies, and scientific papers.The interviews were conducted to the respondents associated with incident management, both from the perspectives of regulator and practitioner. Regulators are the authorities who regulate the implementation of incident management in Indonesia. The author conducted an interview to one of the officials in the Deputy of Incident Response and Recovery at Badan Siber dan Sandi Negara (BSSN). The practitioner is the person whose duty and function is to perform the incident response. In this case, that person is a Cyber Security Data Organiser in the Deputy of Response and Recovery BSSN. Documentation is the process of retrieving secondary data in the form of written or electronic documents related to information and official publications on incident management, issued by both the agency and individuals.

The data analysis technique used in this research was comparative analysis. Among the issues included in the analysis were: (1) Analysis of the theory between SIM3 and CREST framework; (2) Analysis of the framework activities; and (3) Analysis of the scopes of the frameworks.

The data validation technique used in this research was data triangulation in which the triangulation process was derived from the interviews conducted to the respondents. Data triangulation was conducted to support the analysis of the scopes of the frameworks.

RESULTS AND DISCUSSIONS

Cyber Incident management is a series of sequential processes consisting of a preparatory phase, incident detection phase, containment phase, mitigation phase, recovery phase, and a learning phase of the incident that has occurred. This incident management can also be interpreted as a proactive step in resolving an incident, as described in Figure 1 [4]. The process is done based on the inputs provided by the user, the technical team's report and the results of the monitoring generated by the installed incident management device.

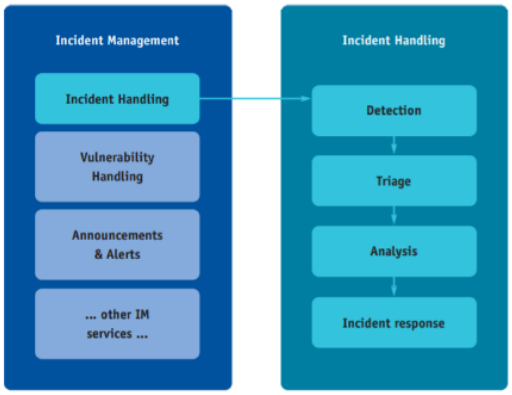

Figure 1. *Incident Management* dan *Incident Handling*

There are several objectives of the implementation of incident management, including to:

1. Quickly detect any incidents;
2. Accurately diagnose the incident;
3. Appropriately manage incidents, defend from attacks and minimise threats;
4. Recover the services to their original conditions;
5. Conduct a search on the major causes of incidents;
6. Implement system development to avoid incidents from occurring.

Institutions/companies often experience difficulties in implementing the existing IT frameworks. The main reason is that many frameworks have similar scopes, thus causing an overlap between one framework and another.In addition, the activity processes that belong to each framework tend to be similar to the others', although there might be differences in the name of the activities.

Therefore, the researchers focused on the use of the frameworks with the scope of incident

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390

management. There are two frameworks discussed in this study, i.e. SIM3 Model and CREST Model. SIM3 and CREST Frameworks are the two major frameworks used in incident management. Those frameworks are widely adopted by researchers, practitioners, and CSIRT to be explored and developed according to the needs of each institution/company.

The application of these frameworks is often deployed by institutions/companies that have an incident response team or commonly known as Computer Security Incident Response Team (CSIRT). In its practice, this CSIRT has numerous names, including Computer Emergency Response Team/Coordination Centre (CERT/CC), Computer Incident Response Team (CIRT), Incident Response Team (IRT), Security Emergency Response Team (SERT), and Warning Advice and Reporting Point (WARPs) [5]. This team is responsible for accepting, addressing and responding to reports and activities of cyber security incidents.

In this article, the researchers focused on 3 (three) aspects, i.e. the levelling scheme of each activity in the frameworks, the maturity level of the implementation of incident management, and the number of activities in the frameworks. Maturity level is a set of characteristics, attributes, indicators, or patterns that represent the capabilities and development in a particular discipline [6]

SIM3 Framework

SIM3 framework is a framework created by Open CSIRT Foundation (OCF). The framework consists of 3 (three) components, i.e. maturity parameters, maturity quadrants, and maturity levels [7]. There are 4 (four) maturity quadrants used in this framework, i.e. O (organisation), H (human), T (tools), and P (process). In addition, there are 44 parameters used in this framework, as described in Table 1.Each parameter has 1 (one) activity that can be done.

Table 1. SIM3 Framework Parameters

No	*Parameter*	*Parameter Number*
1	Mandate & Commitment	O1
2	Constituency	O2
3	Authority	O3
4	Responsibility	O4
5	Service Description	O5
6	Service Level Description	O7
7	Incident Classification	O8
8	Integration in Existing CSIRT systems	O9
9	Organisational Framework	O10
10	Security Policy	O11
11	Code of Conduct /Practice/ethics	H1
12	Personal Resilience	H2
13	Skillset Description	H3
14	Internal Training	H4
15	External Technical Training	H5
16	External Communicating Training	H6
17	External Networking	H7
18	IT Resources List	T1
19	Information Sources List	T2
20	Consolidated E-mail System	T3
21	Incident Tracking System	T4
22	Resilient Phone	T5
23	Resilient Email	T6
24	Resilient Internet Access	T7
25	Incident Prevention Toolset	T8
26	Incident Detection Toolset	T9
27	Incident Resolution Toolset	T10
28	Escalation to Governance Level	P1
29	Escalation to Press Function	P2
30	Escalation to Legal Function	P3
31	Incident Prevention Process	P4
32	Incident Detection Process	P5
33	Incident Resolution Process	P6
34	Specific Incident Processes	P7
35	Audit/Feedback Process	P8
36	Emergency Reachability Process	P9
37	Best Practice Internet Presence	P10
38	Secure Information Handling Process	P11
39	Information Source Process	P12
40	Outreach Process	P13
41	Reporting Process	P14
42	Statistics Process	P15
43	Meeting Process	P16
44	Peer-to-Peer Process	P17

The assessment scheme used in this framework consists of two schemes, the assessment scheme of each activity and the assessment scheme of maturity level. In the assessment scheme each activity is defined into 5 (five) levels [8], i.e.:

1. Level 0, means not available/undefined;
2. Level 1, means implicit (considered but not written down);
3. Level 2, means explicit, internal (written but not formally approved or reviewed);
4. Level 3, means explicit and formalised on authority of CSIRT head (published);
5. Level 4, means explicit, actively assessed on authority of governance levels above the CSIRT management (subject to the control/audit/enforcement process).

Whereas according to the maturity level assessment scheme, the SIM3 framework divides the maturity level into the following levels [9]:

1. **Basic level** shows that the established Incident Response Team demonstrates a good initial preparation. In addition, the Incident Response

Team is able to execute the incident handling process. Assessments in the organisational quadrant largely score 3, and score 1 or 2 in the other quadrants.

2. **Intermediate level** shows that the Incident Response Team has increased its level within the scope of the organisation to a scale of 4, which includes the control side of management. The entire incident handling process has been documented and approved by the management and is at the activity level 3. Moreover, other parameters have also increased compared to those at the basic level.
3. **Advanced level** shows that the Incident Response Team can work closely with other Incident Response Teams and build coordinated incident management capabilities. Most of the parameters in the organisational quadrant are on a scale of 4 and the other quadrants have a minimum score of 3 (even in certain cases, the score is at least 4).

CREST Framework

CREST framework is an incident management framework that can be used to determine the capability of the process of handling cyber incident responses. This framework consists of 3 (three) incident response phases, i.e. the preparatory phase, the response phase, and the follow-up phase. The three phases are elaborated into 15 (fifteen) steps as described in Figure 2 [10]. There are 498 activities that can be executed to support these 15 (fifteen) steps.

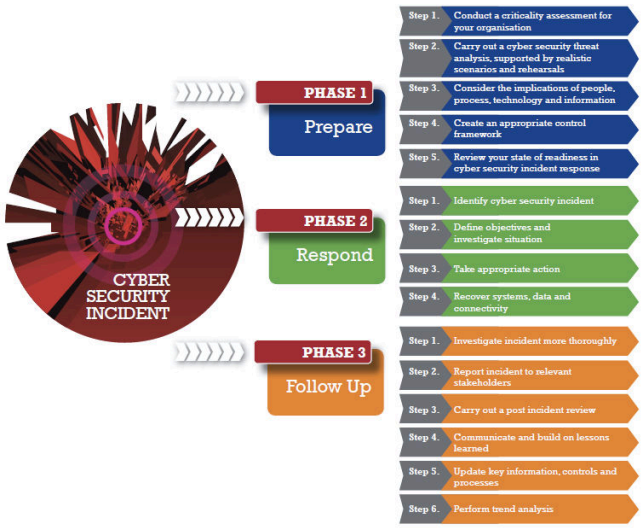

Figure 2. *CREST Framework*

CREST provides a mechanism for assessing the maturity level of incident handling at the institutions/companies. This can be used to measure the level of preparedness in responding to incidents in a quick, effective, and efficient manner. The assessment scheme used consists of the assessment scheme for each activity and the assessment scheme of the maturity level. The assessment scheme for activities is divided into:

1. Level 0, means not implemented/applied;
2. Level 1, means partially implemented/applied;
3. Level 2, means largely implemented/applied;
4. Level 3, means fully implemented/applied.

Meanwhile, judging from the assessment of its maturity level, CREST uses 5 (five) levels to measure the maturity of incident response capability, including:

1. *Foundation*
   The Incident Response Team is in the initial stage of implementing incident management. The incidents that occurred cannot be handled and resolved properly, thus disrupting the organisation's business processes.
2. *Emerging*
   The Incident Response Team has an incident handling guide/procedure, but it is still not consistent in its application. This results on the incidents that have not yet been quickly and effectively dealt with and it requires a considerable amount of time to resolve incidents.
3. *Established*
   The Incident Response Team has sufficient knowledge in handling incidents. Even this is supported by the existence of procedures/policies regarding incident management issued by the management. The incident handling process works accordingly.
4. *Dynamic*
   The Incident Response Team has competencies that are in accordance with the assigned workload. Regulations/policies regarding incident management are tested out and updated regularly. The incidents do not have a significant impact on the services provided to consumers.
5. *Optimised*
   The Incident Response Team has expertise in their fields endorsed by the certification of expertise. Regulations/policies have been adjusted to the development and strategic plan of the organisation. In addition, an incident handling simulation involving internal and external parties has also been performed.

Based on the above explanation, the resulting comparative analysis related to the scheme of the framework activity level can be seen in the table 2.

Table 2. Comparative Analysis of Framework Activity Level

Level	SIM 3 Framework	CREST Framework

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390

Level 0	undefined	not implemented/not applied
Level 1	implicit	partially implemented/applied
Level 2	explicit, internal	largely implemented/applied
Level 3	explicit, formalised on authority	fully implemented/applied
Level 4	explicit, actively assessed on authority of governance levels above the CSIRT management	-

While according to comparative analysis of the level of maturity used, there is a difference between SIM3 framework and CREST framework. In SIM3 framework, the definition of level of maturity is made for each category, in which there are 3 (three) categories used, i.e. basic, intermediate, and advanced. Whereas in CREST framework, it is made for each level based on the level of each activity. The results of the comparative analysis can be seen in table 3.

Table 3. Comparative Analysis of Framework Maturity Levels

Level	SIM 3 Framework	CREST Framework
Level 1	-	Foundation
Level 2	-	Emerging
Level 3	Basic	Established
Level 4	Intermediate	Dynamic
Level 5	Advanced	Optimised

In general, the comparative analysis conducted on the SIM3 framework and CREST framework can be seen in table 4.

Table 4. Comparative Analysis of Frameworks

Aspect	SIM 3 Framework	CREST Framework
Creator	Open CSIRT Foundation (OCF)	CREST
Year of Formulation	2010	2014
Focus of Framework	Service	Service
Incident Management	Yes	Yes
Foundation of Framework	SIM 3	CREST
Number of Activity Level	5 levels (scale 0-4)	4 levels (scale 0-3)
Number of Maturity Level	3 levels (basic, intermediate, advanced)	5 levels (foundation, emerging, established, dynamic, and optimised)
Number of Activities	44 activities	498 activities

However, considering each activity carried out in order to satisfy the framework, there are several activities in the SIM3 framework which are contextually similar to the activities in CREST framework. Examples of similarities in these activities can be seen in table 5.

Table 5. Similarities of the Activities in the Framework

Parameters	No	Activities	SIM3	CREST
Mandate & Commitment	1	Has the established CSIRT acquired legalization/ justification from the leadership of the organisation or other parts of the organisation?	A1	B57, B60
Incident Classification	41	Has the established CSIRT conducted any classification on the incidents, including the type, category, and level of criticality of the incident?	A7	B64, B258

It can be explained that the activity code A1 has similarities with the activity code B57 and B60.

However, there are also activities which are not comparable among both frameworks, as shown in table 6.

Table 6. Differences in Framework Activities

Security Policy	94	Does the established CSIRT have its own security policy?	A10	
	95	Does the organisation's incident response strategy include rules that involve all parts of the company, including the third parties?		B84
	96	Does the organisation's incident response strategy include adjustments between incident response with BCP and the existing rules?		B83

If the incident management framework is in place, it is observable that there are differences in the scope of the two frameworks. The SIM3 framework defines incident management into 44 scopes. Whereas CREST defines incident management into 15 scopes. Therefore, it is necessary to define the scopes of the incident management process based on the framework that is being investigated. Based on the results of identification of the scope of incident management, 50 (fifty) scopes were obtained in supporting the incident management process. The 50 scopes can be seen in table 7.

Table 7. Scopes of Incident Management

No	Categorisation

1	*Mandate & Commitment*
2	*Approach*
3	*Constituency*
4	*Authority*
5	*Responsibility*
6	*Service Description*
7	*Service Level Description*
8	*Incident Classification*
9	*Impact Analysis*
10	*Threat Analysis*
11	*Trend Analysis*
12	*Integration in Existing CSIRT systems*
13	*Organisational Framework*
14	*Security Policy*
15	*Management Performance*
16	*Code of Conduct /Practice/ethics*
17	*Personal Resilience*
18	*Skillset Description*
19	*Internal Training*
20	*External Technical Training*
21	*External Communicating Training*
22	*External Networking*
23	*IT Resources List*
24	*Information Sources List*
25	*Consolidated E-mail System*
26	*Incident Tracking System*
27	*Resilient Phone*
28	*Resilient Email*
29	*Resilient Internet Access*
30	*Incident Prevention Toolset*
31	*Incident Detection Toolset*
32	*Incident Resolution Toolset*
33	*Escalation to Governance Level*
34	*Escalation to Press Function*
35	*Escalation to Legal Function*
36	*Incident Prevention Process*
37	*Incident Detection Process*
38	*Incident Resolution Process / Incident Response Process*
39	*Specific Incident Processes*
40	*Audit/Feedback Process*
41	*Emergency Reachability Process*
42	*Best Practice Internet Presence*
43	*Secure Information and Evidence Handling Process*
44	*Information Source Process*
45	*Outreach Process*
46	*Reporting Process*
47	*Statistics Process*
48	*Meeting Process*
49	*Lesson Learned Process*
50	*Peer-to-Peer Process*

The authors triangulated the data on the scopes that had been identified in table 7. The results of the identification were validated by the respondents through the interview method. This step was conducted in order to obtain proposals/suggestions related to the implementation of industrial management. The results of scope validation by the respondents can be seen in the table 8. From the table it is known that not all scopes are included in the incident management process. Only 35 validated incident management processes can be considered as part of incident management.

Table 8. Scopes of Incident Management

No	Kategorisasi	Regulator	Praktisi
1	*Mandate & Commitment*	√	√
2	*Approach*	√	
3	*Constituency*		√
4	*Authority*	√	√
5	*Responsibility*	√	√
6	*Service Description*		
7	*Service Level Description*		
8	*Incident Classification*	√	√
9	*Impact Analysis*		
10	*Threat Analysis*		
11	*Trend Analysis*	√	
12	*Integration in Existing CSIRT systems*	√	√

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390

13	*Organisational Framework*	√	√
14	*Security Policy*	√	
15	*Management Performance*		
16	*Code of Conduct /Practice/ethics*	√	
17	*Personal Resilience*	√	
18	*Skillset Description*	√	
19	*Internal Training*	√	√
20	*External Technical Training*	√	√
21	*External Comunicating Training*	√	√
22	*External Networking*	√	√
23	*IT Resources List*	√	
24	*Information Sources List*		
25	*Consolidated E-mail System*		
26	*Incident Tracking System*		√
27	*Resilient Phone*		
28	*Resilient Email*		
29	*Resilient Internet Access*		
30	*Incident Prevention Toolset*	√	√
31	*Incident Detection Toolset*	√	√
32	*Incident Resolution Toolset*	√	√
33	*Escalation to Governance Level*	√	√
34	*Escalation to Press Function*	√	√
35	*Escalation to Legal Function*		√
36	*Incident Prevention Process*	√	√
37	*Incident Detection Process*	√	√
38	*Incident Resolution Process / Inciden Response Process*	√	√
39	*Spesific Incident Processes*	√	√
40	*Audit/Feedback Process*	√	
41	*Emergency Reachability Process*		√
42	*Best Practice Internet Presence*		
43	*Secure Information and Evidence Handling Process*		
44	*Information Source Process*	√	
45	*Outreach Process*	√	
46	*Reporting Process*		
47	*Statistics Process*		
48	*Meeting Process*		
49	*Lesson Learned Process*		√
50	*Peer-to-Peer Process*	√	√

CONCLUSIONS

There are several conclusions that can be drawn from this research, including:

1. There are different level schemes used in each activity in the frameworks. In SIM3 framework, there are 5 (five) activity levels used, whereas in CREST framework, there are 4 (four) activity levels;
2. In SIM3 framework, the level of incident management maturity is divided into 3 (levels) based on their categories. Whereas in CREST framework, the level of maturity is divided into 5 (five) levels, where the determination of this level is based on the level of each existing activity.
3. When viewed in terms of the number of activities, SIM3 framework defines the incident management process into 44 activities. Whereas the CREST framework defines the incident management process into 498 activities.
4. Institutions/companies are expected to get an overview regarding the incident management frameworks and adopt them as the reference in implementing incident management in their respective organisations.

SUGGESTIONS

There are several suggestions that can be adopted by both future researchers and institutions/companies who will implement the incident management frameworks, including:

1. For future researchers, it is necessary to validate each activity contained in the framework. This activity validation aims to capture the suitability between the existing activities and the actual conditions;
2. Institutions/companies are expected to be able to implement the incident management framework in their organisations respectively. This aims to minimise the occurrence of incidents and to better prepare for future incidents;
3. Institutions/companies can modify the activities in the framework and adjust them in accordance with the running plans and business processes and the needs of each institution/company.

REFERENCES

[1] BSSN, Indonesia Cyber Security Monitoring Report 2019, Jakarta: BSSN, 2019.

[2] J. Creswell, Research Design-Qualitative, Quantitative, and Mised Methods Approaches, New Delhi: Sage Publication, 2003.

[3] D. Apri, *Strategi Badan Siber dan Sandi Negara (BSSN) dalam Menghadapi Ancaman Siber di Indonesia,* Universitas Indonesia: SKSG, 2018.

[4] E. Team, *Good Practice Guide for Incident Management,* Greece: ENISA, 2010.

[5] B. M, Computer Security Incident Response Teams (CSIRTs): An Overview, United Kingdom: University of Oxford, 2014.

[6] J. Baumgartner, Cybersecurity Capability Maturity Model 9C2M2), US: US Department of Energy (DOE), 2019.

[7] D. Stikvoort, *SIM3: Security Incident Management Maturity Model,* Jerman: S-CURE bv and PRESECURE GmbH, 2015.

[8] ENISA, ENISA CSIRT Maturity Assessment Model, Athens: ENISA, 2019.

Jurnal Teknologi Informasi dan Pendidikan
Volume 13, No. 2, Sept 2020
http://tip.ppj.unp.ac.id

[9] T. v. S. D. S. Hanneke Duijnhoven, Global CSIRT Maturity Framework: Stimulating the development and maturity enhancement of national CSIRTs, Global Forum on Cyber Expertise, 2019.

[10] I. G. Jason Creasey, Cyber Security Incident Response Guide Version 1, UK: CREST, 2013.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390