Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849 e-ISSN: 2548-1398
Vol. 7, No. 12, December 2022

IMPROVING CYBER SECURITY INCIDENT RESPONSE MATURITY OF XYZ ORGANIZATION USING TMPI

Rachmat Budijanto
Swiss German University, Indonesia
Email: rachmat.budijanto@gmail.com

Abstract

This thesis proposes to analyze how an organization can determine the condition of its incident handling capability and how an organization can plan activities for improvement and its relation to increasing resilience of an organization. The method to answer this question, the researcher measures the existing and expected capabilities of handling organizational incidents by using TMPI. The GAP obtained can be made recommendations based on the TMPI with reference to the specified Targets or Expectations. GAP is also analyzed with IPA (Improtant Performance Analysis) to determine priority scale. In this research, the recommendation from TMPI is tested on the CRR (Cyber Resilience Review) to see if there is an improvement on the resilience side. The evaluation and validation process is carried out using the Interview and FGD method with SME (Subject Matter Experts). The results of the research show that TMPI can measure the current condition of an organization's incident handling ability so that a work plan recommendation can be prepared to improve its ability to refer to TMPI according to the desired target. With IPA it can be described Mapping of the priority areas for improvement, namely Post Incident Review, Lesson Learn, Maturity assessment, Threat analysis, Trend Analysis, The Recovery. The results also reveal that from the recommendations for increasing TMPI when measured by CRR, there is an increase in resilience in the Situational Awareness area was an increase of 66%, Incident Management 52%, External Dependency Management 23%, Training and Awareness 17% and the last is Service Continuity Management 8%. However, this thesis has not discussed in the Reality area in resilience. Such as how to apply Protection, Sustainability and Detection to protected assets in accordance with the Organization in cases faced by the organization in improving resilience operations. From the perspective of operational resilience, this study needs to be complemented by Resilience in the Realibility area, This is important because the organization cannot secure everything but the important thing is how the operational organization is running well and security can still be controlled.

Keywords: TMPI, Incident Response, CSIR, BSSN, Maturity Level, Resilience, CRR, IPA.

How to cite:	Budijanto, Rachmat (2022) Improving Cyber Security Incident Response Maturity of XYZ Organization Using TMPI, *Syntax Literate : Jurnal Ilmiah Indonesia (7)12,* http://dx.doi.org/10.36418/syntax-literate.v7i12.11047
E-ISSN:	2548-1398
Published by:	Ridwan Institute

Introduction

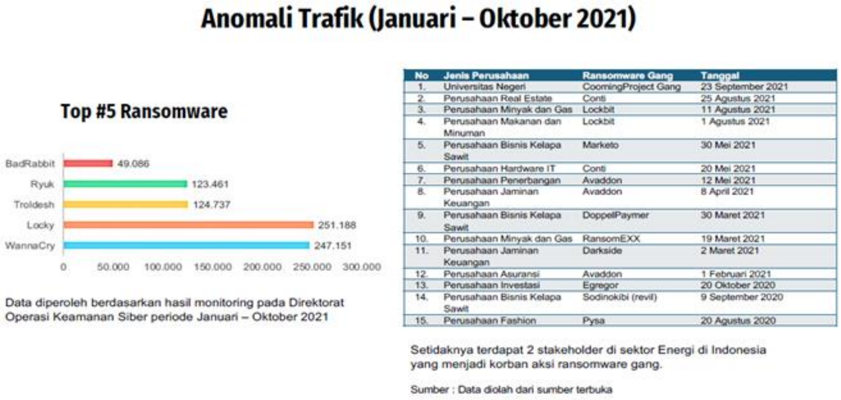
In order to support the management, supervision, and control of cooperation contracts for upstream oil and gas (oil and gas) business activities, security against the Cooperation contract contractors data (KKKS) must be ensured in order to ensure data confidentiality, integrity, and availability (Setiawan & Nugroho, 2016).

1. The KKKS data in question contains information:
2. Development and exploration strategies
3. Data Production / Lifting
4. Data on Oil and Gas Profit Sharing Funds
5. Lifting Performance of OIL for each KKKS

XYZ organization is included in the category of National Vital Object so that viewed from the perspective of cyber crime, this organization is the main target for Cybercriminals.

In the world cybersecurity incidents, such as advanced persistent threats (APTs), which are considered serious cybersecurity attacks, are currently making headlines (Herdiana et al., 2021). This attack had serious repercussions on all organizations – and on governments and international agencies (Windiani, 2017). Methods to respond to this attack comprehensively, quickly and effectively are being actively developed in corporate organizations, government agencies and the international community (World Economic Forum) (Daniri, 2008). This attack is considered a major threat (Creasey, 2013).

The following Figure 1. is a report in Indonesia on reports of attacks during the January – October 2021.



Data diperoleh berdasarkan hasil monitoring pada Direktorat Operasi Keamanan Siber periode Januari – Oktober 2021

No	Jenis Perusahaan	Ransomware Gang	Tanggal
1.	Universitas Negeri	CoomingProject Gang	23 September 2021
2.	Perusahaan Real Estate	Conti	25 Agustus 2021
3.	Perusahaan Minyak dan Gas	Lockbit	11 Agustus 2021
4.	Perusahaan Makanan dan Minuman	Lockbit	1 Agustus 2021
5.	Perusahaan Bisnis Kelapa Sawit	Marketo	30 Mei 2021
6.	Perusahaan Hardware IT	Conti	20 Mei 2021
7.	Perusahaan Penerbangan	Avaddon	12 Mei 2021
8.	Perusahaan Jaminan Keuangan	Avaddon	8 April 2021
9.	Perusahaan Bisnis Kelapa Sawit	DoppelPaymer	30 Maret 2021
10.	Perusahaan Minyak dan Gas	RansomEXX	19 Maret 2021
11.	Perusahaan Jaminan Keuangan	Darkside	2 Maret 2021
12.	Perusahaan Asuransi	Avaddon	1 Februari 2021
13.	Perusahaan Investasi	Egregor	20 Oktober 2020
14.	Perusahaan Bisnis Kelapa Sawit	Sodinokibi (revil)	9 September 2020
15.	Perusahaan Fashion	Pysa	20 Agustus 2020

Setidaknya terdapat 2 stakeholder di sektor Energi di Indonesia yang menjadi korban aksi ransomware gang.

Sumber : Data diolah dari sumber terbuka

Figure 1. Traffic Anomaly - BSSN (January – October 2021)

From the traffic anomaly reports, it can be concluded that cyber attacks are quite serious and need to be addressed. This requires a capable enough cyber incident handling so that most organizations need professionals to help deal with cybersecurity incidents in an appropriate manner. However, organizations find it difficult to find competent experts who can assist in incident response to protect critical organizational information from serious attacks.

At Mei 2021, a Ransomware attack occurred at the XYZ Organization, to improve information security capabilities, activities were made that aim to increase the organization's ability to deal with emerging cyber attacks that cause disruption in carrying out IT Operations in the organization, one of which is making activities for Cyber Security. Incident Response (CSIR).

Cyber risk has become an inseparable part of the company's digitalization process, the magnitude of the potential threat of cyber attacks by individuals, fun hacking, intended hacking and cyber wars between countries can no longer be underestimated (Indarta et al., 2022).

Often organizations focus on how to make preventive defenses such as purchasing Firewalls, IPS, WAF, Endpoint Security and so on. Concerns related to correctives are sometimes ignored even though in terms of probability of occurrence, almost all organizations have experienced the inevitable cyber incidents that were also experienced by the XYZ organization.

XYZ Organizational Management has realized that this is an important thing to be managed properly, this can be seen by the implementation of ISO 27001:2013 initiatives in 2018 and the Security Operation Center starting in 2021.

However, the management does not yet know the extent of the incident response capability in the XYZ organization. Management needs a way of measuring this capability as well as to determine the direction of improvement (targets and roadmaps) that are appropriate.

In the current research, the author focuses on research on measuring maturity levels at the CSIR XYZ Organization with TMPI and making recommendations and work programs aimed at increasing the CSIR maturity level as desired by the organization. This research also examines recommendations for increasing the TMPI maturity level.

This research aims to know Capability and the maturity level CSIR of Organization, to support organizations for improving cyber-security incident Response of Organization and to know Capability and the maturity level resilency of Organization in The context of incident response.

Today's cyber threats are universal and impact all organizations around the world (Balan, S, Otto, J, Minasian, E & Aryal, 2017), As IT activities generate complex cybersecurity risks in organizations, Cybercriminals are learning new ways to attack and quickly adapt to changing environments. The objectives of cyber attacks include stealing new identities, disrupting distribution services and stealing money (Ferdinand, 2015). (Balan, S, Otto, J, Minasian, E & Aryal, 2017) In 2017 254 companies in Australia, Germany, France, Japan, England, Italy and America from the interviews found that the average cost of cybercrimes was around US$11.7 million per organization. The annual cost of cybercrime amounts to billions of US dollars and global losses are around US$400 billion. indicated that 91 percent of organizations in the US experienced economic losses from cyber attack activities (Balan, S, Otto, J, Minasian, E & Aryal, 2017).

Indonesia is the fourth most populous country in the world, and 64.8% of them are active internet users (Permana, 2021). The current development of countries in the face of increasing cyber attacks has become offensive not defensive anymore, and this has become a cyber security policy among countries.

Seeing the escalation of this trend, what is needed by Indonesia is also to prepare itself to face the global cyber war. Given that anonymous actors often use Indonesian territory as a base to carry out attacks, this could have unintended consequences for Indonesia. According to AKAMAI, Indonesia even replaced China in 2013 as the top source of cyber-attack traffic in the world. According to the Ministry of Communication and Information, in 2017 Indonesia was the target of more than 205 million attacks. Indonesia will face multiple attacks that can cripple critical infrastructure, businesses and public services. This means that cyber warfare is a serious threat to Indonesia, which has a vision of becoming the largest digital economy in Southeast Asia by 2020. Indonesia must first publish an official white paper on its international strategy in cyberspace to anticipate increasing capabilities in cyber warfare globally. The document contains an explanation of Indonesia's current offensive cyber capabilities and their impact on security and threats to international stability (Tri Aryadi, 2018).

A clear threat model is essential for setting resilience goals.4 Cyber threats can be variously characterized – for example, in terms of enemy characteristics and in terms of behavior. ability, intent, and targeting can be categorized as enemy Characteristics (Bodeau & Graubart, 2011).

Cyber kill chain is a way of describing the activity or behavior of an adversary who persistently and stealthily gains a foothold from malware present in an organization's system or mission and then uses that foothold to achieve goals. The components of the cyber kill chain are: (Cloppert, 2009).

1. Reconnaissance: A way to obtain information in carrying out an attack.
2. Weapons: payloads placed in delivery vehicles (e.g., hyperlinks to sites contaminated with phishing email malware, malware in email attachments).
3. Delivery: Sending the attack vehicle to the potential victim.
4. Exploitation/installation: Exploiting system vulnerabilities to install malware on the victim system. This is identified as the pivotal point in the cyber kill chain. (Cloppert, 2009)
5. Command and control: Directing the victim system to take actions (e.g., to download additional malware, to perform more advanced reconnaissance within the enterprise information infrastructure, to propagate malware to other systems).

6. Actions to achieve adversary objectives: Depending on the adversary's objectives, these may include exfiltrating data, corrupting mission or organizational data or replacing it with deceptive data, and degrading or denying the functionality of cyber resources.
7. Maintenance: Taking actions to ensure future access (e.g., changing the profile of adversary-installed malware, modifying logs).

The number of violations against information security is increasing every year accompanied by the development of increasingly advanced technology, so that information security control is needed. Some of these types of threats include: viruses, system failures, misuse of information by users, absence of access authorization and theft of access to information (DR Windriya, H Tanuwijaya, 2014)

Indonesia is a country whose cyber security level is still weak. This can be seen from several incidents, In Table 2.2 are described that in mid-May 2014 there was an incident of breaking into the debit card data of a bank that hacked by infiltrating the bank customer card security system. (Ardiyanti, 2014).

Even according to the Minister of Law and Human Rights, Yasonna Laoly in a webinar on the Potential Threat of Cyber Crime for business people, he said that losses due to cyber crime in 2021 will reach 6 trillion USD (Lendong, 2020) Cybercrime crime has increased significantly along with the increasing number of e-commerce players. Utilization of internet services and information technology as a running business platform has the potential to increase cybercrime attacks. One of the existing cybercrime handling is indeed the existence of cyber law (Pratama, 2013).

In business, the proportion of violations identified as having attacks is lower (32%) when compared to 2018 (43%) and 2017 (46%) (Department for Digital, Culture, 2019). The business' findings are consistent with 2017 when this question first arose. When charities first surveyed, the survey showed an increase in cybersecurity incidents from 19% in 2018 and 22% in 2019, to 26% in 2020. This fact shows that charities are either better at identifying attacks or are being targeted. cyber. Of these 46% cybersecurity incidents, 19% have experienced data or material loss, 39% were affected by operational and resource disruptions, even causing a wider business impact. Some charities also reported that 26% of attacks occurred, 25% suffered material losses and 56% were negatively affected (Department for Digital, Culture, 2019).

Associated with Cyber Threats Each organization has specific characteristics against ransomeware attacks depending on the application and infrastructure owned by the organization. To find out the possible threats that can attack an organization can be through several approaches.

In creating a threat model there are several approaches that differ from the means of the device or from the evaluation system(Potteiger et al., 2016):

1. Attacker-centric: Threats are seen from the attacker's point of view by determining how the attacker will damage the system.

2. Asset centered: This threat is seen from the perspective of the protected asset by determining the threats to the asset.
3. System-centric: This threat is seen from the device or system even per component by determining the assessment of each threat to the component.

Method

The process of Data Collection is measuring existing condition level and target condition level for Cyber Security Incident Response on XYZ Organization based on TMPI maturity level assessment questions. It will be carried out to experts in their fields related to the categories of questions in TMPI.

Discussion will be directed to several teams such as:

1. Head of IT Division for this session discuuss related Crown jewels of XYZ Organization, TMPI Questions related and Maturity Level Target That needed.
2. IT Infrastructure Team for this session discuss about infrastructure concern related to TMPI Questions
3. Application Team for this session discuss about application concern related to TMPI Questions
4. Security Team for this session discuss about security management concern related to TMPI Questions
5. CSIR Provider that Handling Insident Respnse in XYZ Organization.

a. Maturity Level Currently

From the results of questions aimed at conducting an assessment of incident handling, a value for the maturity level will be obtained. The value is determined based on the facts that apply to the CSIR XYZ Organization. In this stage, an overview of the maturity value of the existing condition will be obtained so that it is useful for organizations in knowing the current condition of incident handling.

b. Maturity Level Expected

To determine the desired CSIR maturity level, a discussion will be held with the head of the IT Division. In this discussion, it is intended to determine management's expectations of the expected CSIR maturity level of the organization. This maturity level expectation will be used as a target in increasing the maturity level of the organization.

c. Gap Analysis

In this research, researcher will compare the existing conditions and the expected conditions so that an analysis can be carried out on the obtained GAP. Furthermore, this research will include recommendations as a solution in order to fulfill the gap between existing and expected conditions. The purpose of this research is to be able to improve the Incident Response and resilience of the organization can be maintained.

And Researcher also tested the recommendations generated from TMPI by conducting a self-assessment using CRR and seeing the results of the test whether there was an increase or not.

d. Evaluation and Prioritization

In this research, the next step is to analyze and evaluate the results of the existing GAP between the existing and the expected using IPA. The results of the analysis carried out using this IPA can help in this research to determine the focus areas of concern to be improved because they are inline with the needs of the organization.

e. Validation

In this research, the validation that will be carried out is by conducting FGDs together with experts in their fields. This FGD will be carried out together with experts in their fields so that at this stage valid recommendations are produced which are proposed in this thesis to organizations to carry out activities to full fill GAP in areas obtained from the results of IPA analysis. The objective of this activities are increasing cybersecurity. According to (O.Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, 2018), FGD aims to obtain data from a group of deliberately selected individuals. Focus group discussion usually yields both qualitative and observational data where analyses can be demanding. According to (Leech, N. L., & Onwuegbuzie, 2007).

Results and Discussion

A. Mapping Result

From the mapping process carried out between NIST, CRR and TMPI, some similarities and differences between the three frameworks can be conveyed. Table 4.1 describe about convey some similarities and differences from the results of the mapping process:

Table 1.
Similarities and Differences in NIST, CRR and TMPI Mapping Results

No	Equality	
	NIST, CRR And TMPI	Description
1	Sub Categories in Domains at NIST, CRR and TMPI have many similarities.	NIST, CRR and TMPI all talk about Cyber Security, Cyber Risilience and Cyber Security Incident.
2	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Specifically related to Resilience and Sustainability, NIST discusses the PR.PT-5 and TMPI Sub Categories in Question 2.3.6

	2.3.6 Has the technical implementation of defense in your organization included: DMZ implementation, back up/HA (high availability) system and back up configuration?	

No	**Difference**	
	NIST dan CRR	**TMPI**
1	Supply Chain Risk Management (SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks. RM:G1.Q1 RM:G1.Q2 RM:G1.Q3 RM:G1.Q4	TMPI discussed BIA on criticality points, but prioritization was not carried out in the preparation phase, but in the response phase. Meanwhile, if there are assets that are equally critical, they need to be prioritized. TMPI prioritization is done when situational during the response phase
2	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. EDM:G4.Q1 EDM:G4.Q2 EDM:G4.Q3 EDM:G4.Q4	TMPI does not require review/assessment of third parties who are partners in SOC handling / data analysis / incident handling
	PR.DS-7: The development and testing environment(s) are separate from the production environment CCM:G2.Q7	TMPI does not require the separation between development and production.
	PR.IP-6: Data is destroyed according to policy AM:G6.Q6 AM:G6.Q7	TMPI does not set up for data destroy procedure for sensitive data

From the above similarities, it can be concluded that the steps in the phases at TMPI also discussed the domains and sub-domains of Cyber Security and Cyber Resillience. And especially in Step 2.3.6 of Phase 2 at TMPI, and PR.PT-5 at NIST is very specific about Resillience.

When using a framework that supports cyber security resilience, and this framework can also measure the existing conditions, targets and gaps that need to be done, then when we increase the maturity, we will automatically increase the cyber resilience. The enhanced cyber resilience domain is of course in accordance with the focus of this framework and the scope of the research, namely increasing the capability in Incident Response.

B. Data Collection

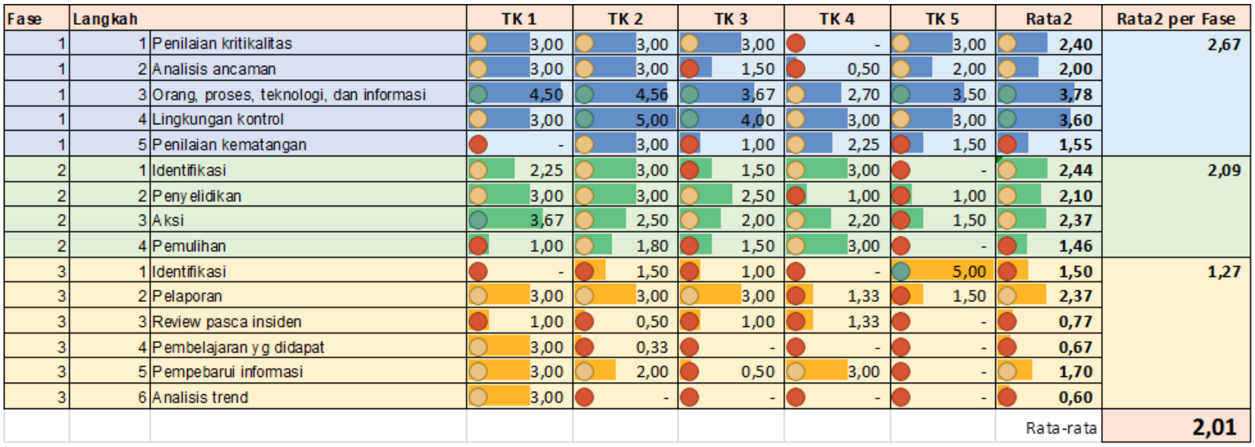
This stage will explain how to collect data for this thesis research, collecting this data through interviews conducted discussions with Head of IT Division, IT Infrastructure Team, Application Team and Security Team. Bellows are results from Self Assessment using TMPI.

For this thesis, research will use TMPI. Detailed Table Result Self Assessment will be attached to the appendix B. This assessment working paper document refers to the assessment question document owned by TMPI which is used to assess the existing and expected conditions.

In this data collection process, there are 3 persons involved, namely from the Application Team, Infrastructure Team, Security Team and 1 Persons from provider that handle CSIR in XYZ Organization. Self-assessment is carried out both offline and online within a period of 4 days.

1. Summary of Existing Maturity Level

   At this stage, the researcher conducted a FGD with the IT Infrastructure Team, Application Team, Security Team and 1 Person from CSIR Provider. From the process of implementing joint discussions in this measurement, the Results Maturity level of TMPI are as Figure 4.1 follows:



Fase	Langkah		TK 1	TK 2	TK 3	TK 4	TK 5	Rata2	Rata2 per Fase
1	1	Penilaian kritikalitas	3,00	3,00	3,00	-	3,00	**2,40**	**2,67**
1	2	Analisis ancaman	3,00	3,00	1,50	0,50	2,00	**2,00**	
1	3	Orang, proses, teknologi, dan informasi	4,50	4,56	3,67	2,70	3,50	**3,78**	
1	4	Lingkungan kontrol	3,00	5,00	4,00	3,00	3,00	**3,60**	
1	5	Penilaian kematangan	-	3,00	1,00	2,25	1,50	**1,55**	
2	1	Identifikasi	2,25	3,00	1,50	3,00	-	**2,44**	**2,09**
2	2	Penyelidikan	3,00	3,00	2,50	1,00	1,00	**2,10**	
2	3	Aksi	3,67	2,50	2,00	2,20	1,50	**2,37**	
2	4	Pemulihan	1,00	1,80	1,50	3,00	-	**1,46**	
3	1	Identifikasi	-	1,50	1,00	-	5,00	**1,50**	**1,27**
3	2	Pelaporan	3,00	3,00	3,00	1,33	1,50	**2,37**	
3	3	Review pasca insiden	1,00	0,50	1,00	1,33	-	**0,77**	
3	4	Pembelajaran yg didapat	3,00	0,33	-	-	-	**0,67**	
3	5	Pempebarui informasi	3,00	2,00	0,50	3,00	-	**1,70**	
3	6	Analisis trend	3,00	-	-	-	-	**0,60**	
								Rata-rata	**2,01**

Figure 2. The Existing Result Recapitulation of Maturity Level

From the figure 1. above, it is obtained that several areas require recommendations for increasing the maturity level value, and it means that these areas require an increase in incident handling capabilities aimed at increasing the security level of the organization.

The following is a table 2. summuray of the areas required for improvement:

Table 2.
Area Required Improvement

Radar Graphic	Steps		
	Fase 1	**Fase 2**	**Fase 3**
1.1 - Criticality assessment	1		
1.2 - Threat analysis	2		
1.3 - People, Process, Technology and Information	-		
1.4 - Control environment	-		
1.5 - Maturity assessment	4		
2.1 - Identification		2	
2.2 - Investigation		2	
2.3 - Action		1	
2.4 - Recovery		4	
3.1 - Incident investigation			5
3.2 - Reporting			2
3.3 - Post incident review			6
3.4 - Lessons learned			5
3.5 - Updating			2
3.6 - Trend analysis			5

From the measurement results in phase 1, it can be seen that there are 7 Steps that need to be improved and the most is in the Area Maturity Assessment, and in phase 2 there are 9 Steps of weakness and the most is in the Recovery step. And for phase 3 there are 25 Steps that need to be improved and the most is the Post Incident Review step.

The following is table 3. which describes the existing gap from the results of the maturity level measurement.

Table 3.
Existing Fase Maturity Level

Radar Graphic	Fase 1	Fase 2	Fase 3
1.1 - Criticality assessment	2,40		
1.2 - Threat analysis	2,00		
1.3 - People, Process, Technology and Information	3,78		
1.4 - Control environment	3,60		
1.5 - Maturity assessment	1,55		
2.1 - Identification		2,44	
2.2 - Investigation		2,10	
2.3 - Action		2,37	
2.4 - Recovery		1,46	
3.1 - Incident investigation			1,50
3.2 - Reporting			2,37
3.3 - Post incident review			0,77
3.4 - Lessons learned			0,67
3.5 - Updating			1,70
3.6 - Trend analysis			0,60

From the average results obtained in the maturity level assessment of incident handling with TMPI, it can be concluded that there are 6 areas in all Phase 1, Phase 2 and Phase 3 that need attention to make improvement steps. The 6 areas are: Post Incident Review, Lesson Learn, Maturity assessment, Threat analysis, Trend Analysis, The Recovery.

And in figure 2, the existing Gap value is described in the form of a Radar image so that it can be seen in graphic form.

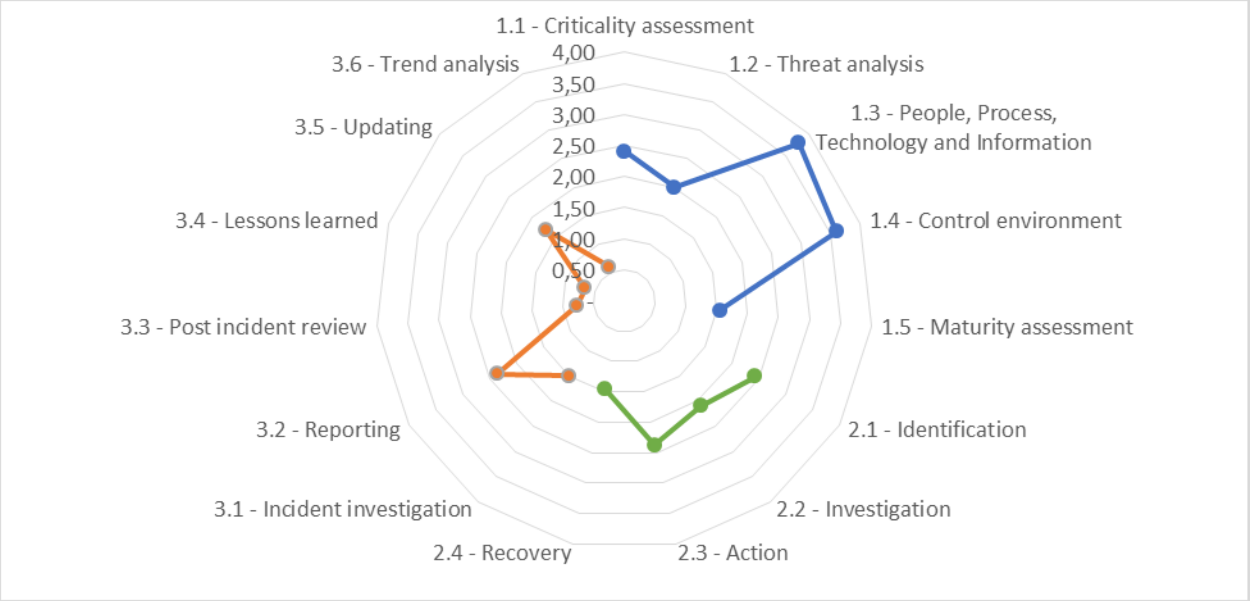


Figure 3. Radar Existing Matury Level

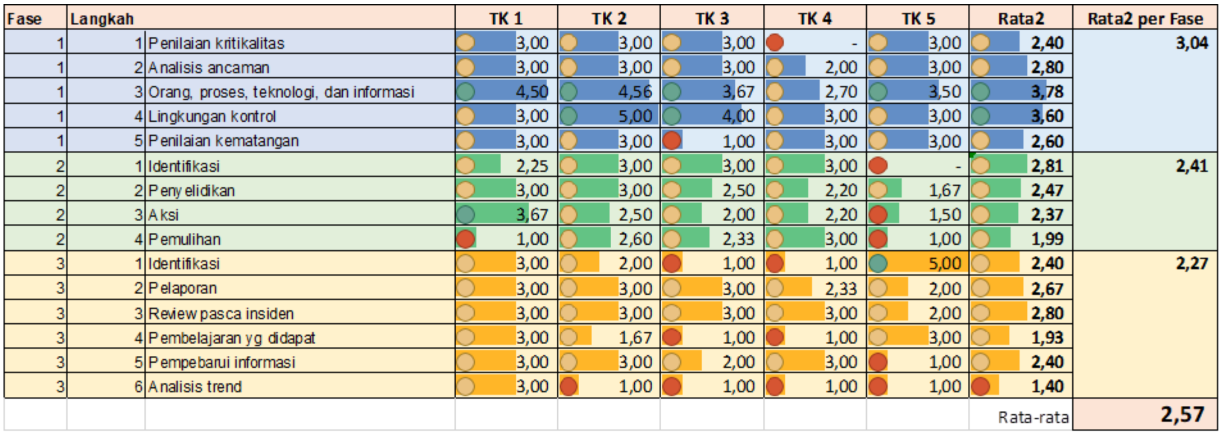
2. Summary of Expectation Maturity Level

From Discussion with Division Head, Researcher get some points from Expects management for this initial target of CSIR Maturity Level:

a. The main target of the organizational maturity level is similar to institutions and ministries
b. For improvement Start from red areas (Weaks Area) but Adjusting to the suitability of the organization's appetite for resources, budget and organizational conditions.

And after the re-measurement is carried out, the expected target from management is obtained to increase the maturity level of the organization.

The Researcher carried out this measurement together with the MSTI Security and SME Team (VP SME). The focus areas that will be improved are discussed and set targets to be achieved by referring to the level of the TMPI. And from figure 3. can be described the results of the implementation of measurements based on the expectations of the management achieved, represented by the Security Team and SME MSTI (VP SME).



Fase	Langkah		TK 1	TK 2	TK 3	TK 4	TK 5	Rata2	Rata2 per Fase
1	1	Penilaian kritikalitas	3,00	3,00	3,00	-	3,00	**2,40**	**3,04**
1	2	Analisis ancaman	3,00	3,00	3,00	2,00	3,00	**2,80**	
1	3	Orang, proses, teknologi, dan informasi	4,50	4,56	3,67	2,70	3,50	**3,78**	
1	4	Lingkungan kontrol	3,00	5,00	4,00	3,00	3,00	**3,60**	
1	5	Penilaian kematangan	3,00	3,00	1,00	3,00	3,00	**2,60**	
2	1	Identifikasi	2,25	3,00	3,00	3,00	-	**2,81**	**2,41**
2	2	Penyelidikan	3,00	3,00	2,50	2,20	1,67	**2,47**	
2	3	Aksi	3,67	2,50	2,00	2,20	1,50	**2,37**	
2	4	Pemulihan	1,00	2,60	2,33	3,00	1,00	**1,99**	
3	1	Identifikasi	3,00	2,00	1,00	1,00	5,00	**2,40**	**2,27**
3	2	Pelaporan	3,00	3,00	3,00	2,33	2,00	**2,67**	
3	3	Review pasca insiden	3,00	3,00	3,00	3,00	2,00	**2,80**	
3	4	Pembelajaran yg didapat	3,00	1,67	1,00	1,00	3,00	**1,93**	
3	5	Pempebarui informasi	3,00	3,00	2,00	3,00	1,00	**2,40**	
3	6	Analisis trend	3,00	1,00	1,00	1,00	1,00	**1,40**	
								Rata-rata	**2,57**

Figure 4. The Expectation Result Recapitulation of Maturity Level

From the measurement of the targeted maturity level, it is obtained that the red points have begun to decrease, although some are still red, but it is because the organization's resources and capabilities require coordination and readiness from other functions or other institutions, such as an internal audit program for potential incidents. security, then there is no cooperation with law enforcement in relation to the applicable positive law.

From the measurement results, it can be described in table 4, in the table it can be seen how many areas are still weak from each phase of TMPI in XYZ Organization.

Table 4.
Area After Improvement Result

Radar Graphic	Steps		
	Fase 1	Fase 2	Fase 3
1.1 - Criticality assessment	1		
1.2 - Threat analysis	-		
1.3 - People, Process, Technology and Information	-		
1.4 - Control environment	-		
1.5 - Maturity assessment	1		
2.1 - Identification		1	
2.2 - Investigation		-	
2.3 - Action		2	
2.4 - Recovery		2	
3.1 - Incident investigation			2
3.2 - Reporting			-
3.3 - Post incident review			-

3.4 - Lessons learned	2
3.5 - Updating	1
3.6 - Trend analysis	5

From the measurement results in phase 1, it can be seen that there are 2 Steps that still need to be improved in the Area CriticallyAssessment, and in phase 2 there are 5 Steps of weakness in the Recovery and action steps. And for phase 3 there are 10 Steps that still need to be improved and the most is the Trend Analysis step.

Some are still low and still require improvement from the maturity level assessment, but these conditions are in accordance with management's expectations. And in Table 5. can be described the value of the target results of the desired improvement.

Table 5.
Expection Fase Maturity Level

Grafik Radar	Fase 1	Fase 2	Fase 3
1.1 - Criticality assessment	2,40		
1.2 - Threat analysis	2,80		
1.3 - People, Process, Technology and Information	3,78		
1.4 - Control environment	3,60		
1.5 - Maturity assessment	2,60		
2.1 - Identification		2,81	
2.2 - Investigation		2,47	
2.3 - Action		2,37	
2.4 - Recovery		1,99	
3.1 - Incident investigation			2,40
3.2 - Reporting			2,67
3.3 - Post incident review			2,80
3.4 - Lessons learned			1,93
3.5 - Updating			2,40
3.6 - Trend analysis			1,40

And in figure 4. the final result is depicted in the form of a Radar graphic as can be seen as follows.

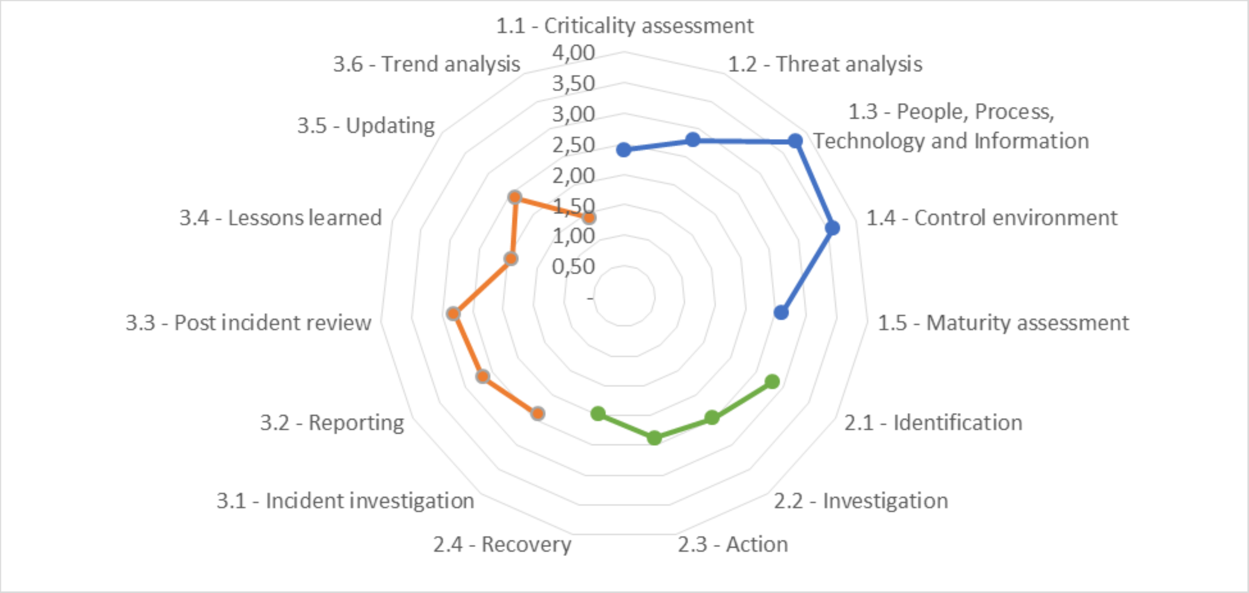


Figure 5. Radar Expectation Matury Level

3. Summary of Existing Relisiliency Assessment Using CRR

   At this stage, mapping of existing conditions to the maturity level of CRR in the context of incident response is carried out, namely focusing on the incident management domain.

   The measurement of the existing condition of handling in the XYZ organization is measured using the Assessment from the CRR Tools, and the results of these measurements are illustrated in Figure 5. as follows:

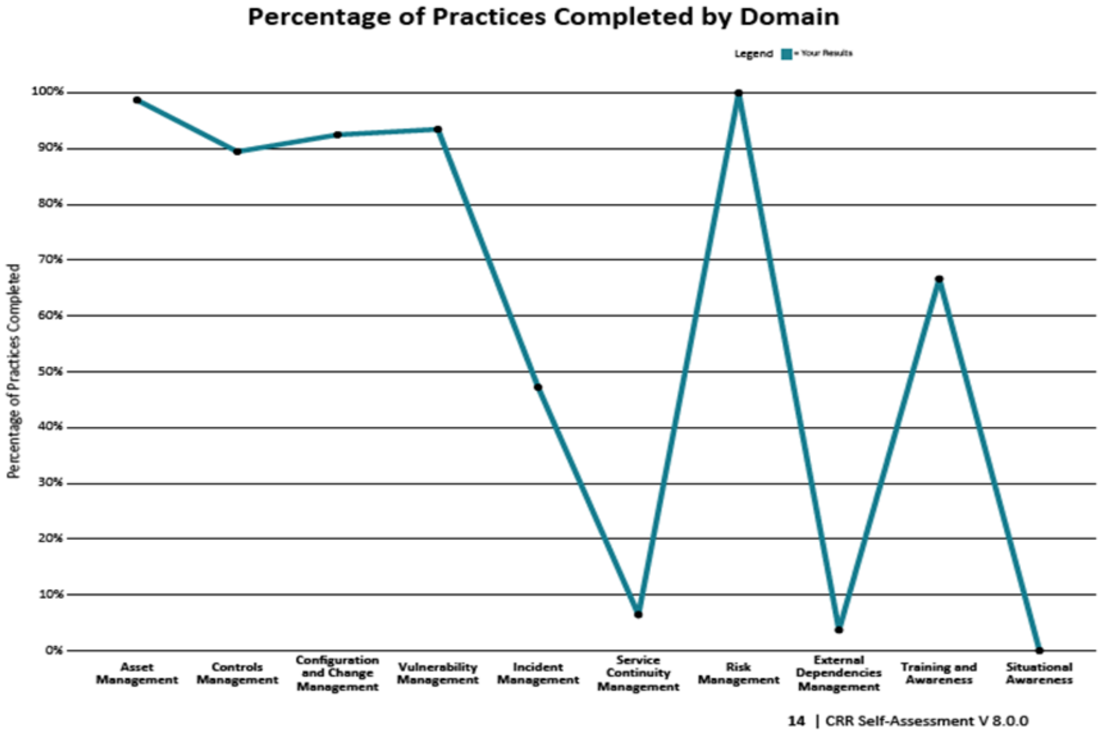


Figure 6. Existing Resilience CRR Maturity Level

4. Summary of Expected Relisiliency Assessment Using CRR

At this stage, a mapping of the expected conditions is carried out according to the expectation assessment from TMPI by using a simulation of these conditions against the maturity level of the CRR in the context of incident response, namely focusing on the incident management domain.

The measurement of the simulation condition from TMPI is measured using the Assessment from the CRR Tools, and the results of these measurements are illustrated in Figure 6. as follows:

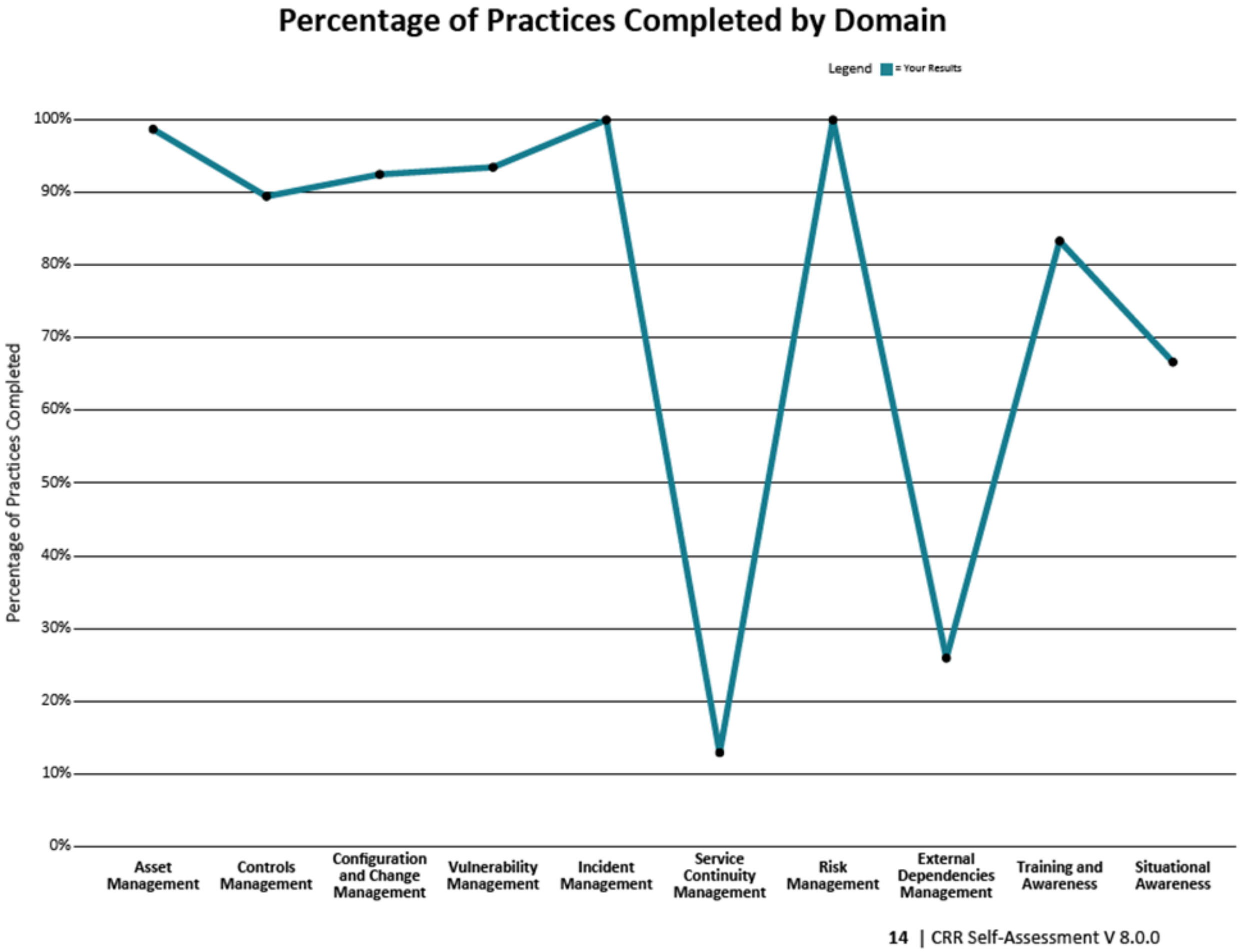


Figure 7. Existing Resilience CRR Maturity Level

If we look at the results of the maturity level measurement with CRR, it can be seen that the incident management domain can increase quite significantly. So that in this test it can be concluded that increasing the handling of incident management at the TMPI pad can also increase the resilience level of organizational conditions, especially in this case in the incident handling area.

C. Data Analysis

1. The Gap Analysis for TMPI

Knowing the GAP is an important step to be able to see and analyze the Self Assessment results. Based on the literature review results in chapter 2, (Rosmiati , Imam Riadi , Yudi Prayudi, 2016).

Table 6.
GAP Maturity Level

Atribut	Existing	Expectation	Gap
Atribute_Fase1			
1.1 - Criticality assessment	2.40	2.40	-
1.2 - Threat analysis	2.00	2.80	(0.80)
1.3 - People, Process, Technology and Information	3.78	3.78	-
1.4 - Control environment	3.60	3.60	-
1.5 - Maturity assessment	1.55	2.60	(1.05)
Rata-rata	**2.67**	**3.04**	**(0.37)**
Atribute_Fase2			
2.1 - Identification	2.44	2.81	(0.38)
2.2 - Investigation	2.10	2.47	(0.37)
2.3 - Action	2.37	2.37	(0.10)
2.4 - Recovery	1.46	1.99	(0.53)
Rata-rata	**2.09**	**2.41**	**(0.32)**
Atribute_Fase3			
3.1 - Incident investigation	1.50	2.40	(0.90)
3.2 - Reporting	2.37	2.67	(0.30)
3.3 - Post incident review	0.77	2.80	(2.03)
3.4 - Lessons learned	0.67	1.93	(1.27)
3.5 - Updating	1.70	2.40	(0.70)
3.6 - Trend analysis	0.6	1.40	(0.80)
	1.27	**2.27**	**-1.00**

Based on the table 6, it can be shown that in phase 1 the threat analysis and maturity assessment factors must be improved, because the existing/performance is lower than the expectation/importance. On the other hand, the critically assessment factor; people, processes, technology and information; and control environment shows that there is no gap between existing and expectation, so overall in phase 1 there is still a gap of about 0.37 more and must be increased in order to achieve expectation.

2. The Gap Analysis for CRR

In this table 7, the changes (both increase/decrease) to the level of resilience are mapped based on the CRR during the existing TMPI conditions and the expected TMPI conditions. To prove the hypothesis that increasing incident response capabilities based on TMPI also increases the level of organizational resilience.

Table 7.
GAP Maturity Level

Atribut	Existing	Expectation	GAP
Asset Management	99%	99%	-
Controls Management	90%	90%	-
Configuration and Change Management	93%	93%	-
Vulnerability Management	94%	94%	-
Incident Management	48%	100%	52%
Service Continuity Management	6%	14%	8%
Risk Management	100%	100%	-
External Dependency Management	4%	27%	23%
Training and Awareness	67%	83%	17%
Situational Awarenes	0%	66%	66%

In particular, the increase in resilience in the Situational Awareness area was an increase of 66%, Incident Management 52%, External Dependency Management 23%, Training and Awareness 17% and the last is Service Continuity Management 8%.

3. Priority Analysis with The Quadrant Performance Analysis Based on TMPI Gap Analysis Table

According to (CR-SAT) In order to aid companies in the correct definition of actions and complement the prioritization of these actions a cyber resilience progression model for SMEs was developed in the methodology. Based on the literature review results in chapter 2, section 2.8 the determination of the priority scale is analyzed using IPA tools.

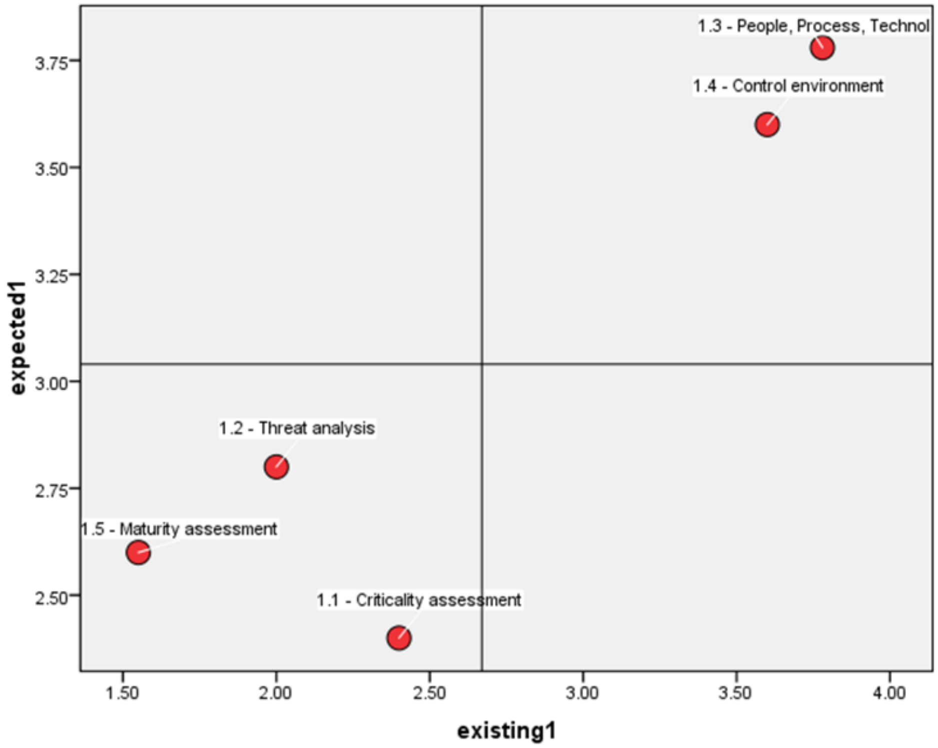


Figure 8. IPA calculation output results in phase 1

Based on the results of the IPA analysis in Figure 4.7, it can be shown that the variables 1.3 people, process, technology and information and the control environment variable 1.4 are already in Quadrant II, which means that both variables have high performance (existing) and important (expected).

Meanwhile for variable 1.1 - Criticality assessment, variable 1.2 - Threat analysis and 1.5 - Maturity assessment are in Quadrant III, which can be interpreted as having low importance and performance. The threat analysis variable can still be improved so that it can be in quadrant I.

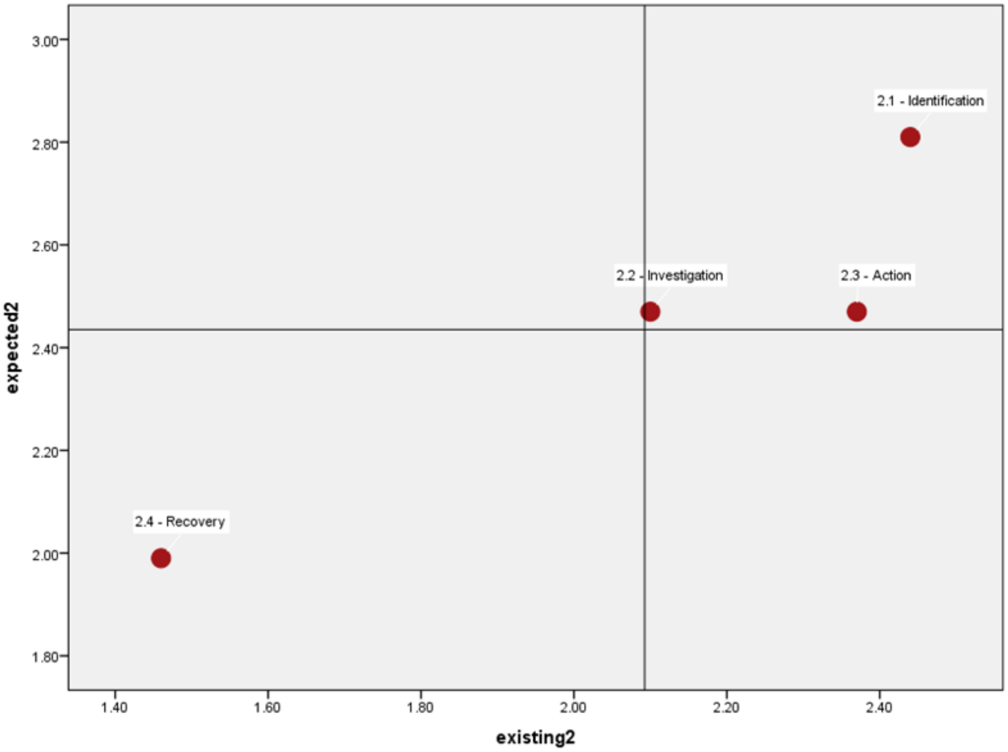


Figure 8. IPA calculation output results in phase 2

Based on Figure 8. above, it can be shown that the Step 2.1 identification, Step 2.2 investigation and Step 2.3 Action are in Quadrant II, which means that both variables have high performance (existing) and important (expected).

While the variable 2.4 Recovery is in Quadrant III, which shows that The Recovery it has low importance and not so special performance.

On the other hand, no action is in Quadrant IV, or shows that no step has a low importance (important/expected), but the performance is high.

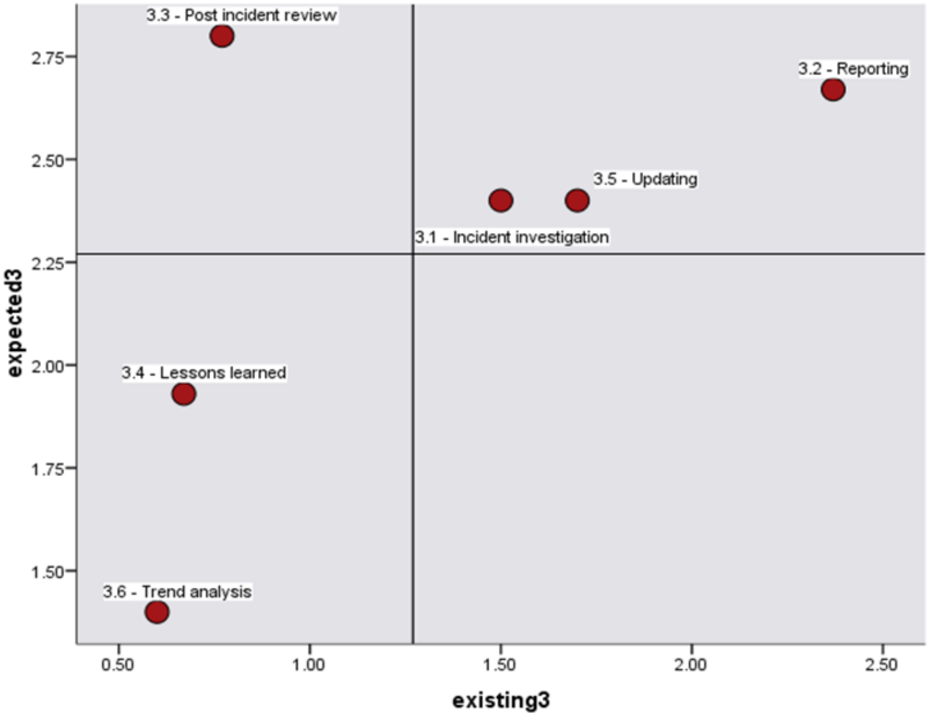


Figure 9. IPA calculation output results in phase 3

Based on Figure 9. above, it can be shown that the variables 3.1 incident investigation, 3.2 reporting, and 3.5 updating are in Quadrant II, which means that both variables have high performance (existing) and important (expected).

Meanwhile, variable 3.3 post incident review is in Quadrant I, which means this factor has high importance and low performance. And from this it can be seen that the Post Incident Review has high management expectations and its performance still needs to be improved, so that Post Incident Review is a top priority that needs to be improved so that the program to improve these Steps will be prioritized first.

Furthermore, for variables 3.4 lessons learned and variable 3.6 trend analysis are in Quadrant III, which means low priority, or low importance and low performance. The next priority in phase 3 that requires improvement is Lesson learned. The condition is that expectations are still quite high and in terms of performance, it still needs to be improved. From the analysis using this IPA, a table can be made to sort the priority of the Phases and Steps expected by management.

And the following is a summary of the GAP Analysis sorted by priority from the results of the analysis using IPA.

a. Top Priority to Improvement
    1) Post Incident Review
b. Second Priorities to Improvement

1) Lesson Learn
2) Maturity assessment
3) Threat analysis
4) Trend Analysis
5) The Recovery

D. Result Discussin / FGD

Regarding the implementation of this FGD, referring to Chapter 3.2.7, the FGD is carried out as follows:

1. Finding and Improvement Strategy

In this thesis research, after a Data has been successfully analysis, the next step is how to make Improvement Strategy. Based on the literature review results in chapter 2. The following is the result of an analysis of what things need to be improved against the current condition so that it can be adjusted to management's expectations.

This recommendation is made based on the weakness of the stages obtained during the maturity level assessment with TMPI. Recommendations are obtained by analyzing existing and expected conditions by strengthening the GAP analysis between the conditions desired by management using IPA.

To formulate the recommendations needed in this research by looking at the requirements of the Basis of Assessment which is a reference in the existing and target/Expectation assessments as outlined in Table 11.

The determination of the recommended activities that are formulated as solutions for improvement was also discussed with several teams involved in Operations in the TMPI assessment process.

Evaluation results This recommendation was submitted by the researcher for validation and expert opinion to ensure that the recommendations that have been made are indeed feasible and in accordance with TMPI and Management's expectations.

Refer to Chapter 4.2.2 has been explained related to the direction of management in formulating recommendations for improvement of this TMPI, namely:

a. The main target of the organizational maturity level is similar to institutions and ministries
b. For improvement Start from red areas but Adjusting to the suitability of the organization's appetite for resources, budget and organizational conditions.

And the Division Head said to discuss technical matters with the Security Team in the details of the proposal that would be formulated and reviewed or validated by SME IT.

This management directive has been discussed with BSSN regarding the organizational strategy in increasing the maturity level of this TMPI, and BSSN said that the strategy can be carried out according to the Appetide of the organization and BSSN added that for the Ministry or institution or agency it is expected to have a maturity level between 2.2 to 3.0.

And in the proposal in table 4.8, recommendations for CSIR improvement have been formulated with reference to the direction of the Division head as stated above.

These recommendations have been analyzed and discussed with the experts, namely HGF, HD and FH. From the existing FGD process, the experts agreed that the proposed recommendations were appropriate to be used to make improvements based on the TMPI.

In this FGD there are 2 suggestions for additional analysis, namely:

a. Grouping recommendations based on 3 categories, namely Documents, Capability and Activity.
b. It is proposed to test the results of the recommendations on the CRR measurement to test the relationship with Resilience.

2. Validation

The validation process will be carried out by conducting interviews with 5 Subject Matter Experts who are experienced in the field of Security. The selection of people is based on an area that is intended to complement from several sides, so that their Opinions and Suggestions can better meet the required aspects.

The implementation is divided into 2 parts, First in the form of a joint FGD consisting of 1 expert from the internal organization who handles CSIR Operations, 2 experts from external but who are involved in handling CSIR in the organization where 1 person is involved in CSIR Operations and 1 person is a consultant from the third party of the establishment of the CSIR in the organization.

Based on the results of the FGD, it was obtained the opinion of Bapak HGF that:

a. TMPI can be used to measure the maturity level of an organization's incident handling, because the questions used for assessment are detailed in the incident handling area.
b. TMPI can be used to map activities aimed at improving incident handling within an organization. With TMPI it can be seen which areas are still weak so that activities can be carried out for improvement in accordance with the expectations of the organization.

Within the XYZ organization itself, activities related to collaboration with non-IT parties or external parties have also become activities that are still not supported by management, and this can be seen from the mapping at TMPI that occurred. It is hoped that TMPI and BSSN can be a factor to convince management regarding this matter. I hope that TMPI also conveys the risk if a domain or activity is not carried out as an illustration that makes it easier for management to reconsider.

c. I agree with determining the priority by giving priority based on the expectations and existing points given. Thus helping the organization in determining which activities should take precedence.
d. Based on observations and evaluations where I participated in these activities using TMPI (incident response capability) and CRR (organizational resilience capability), the XYZ organization is indeed still weak in terms of incident handling execution, this can be seen during the assessment using CRR where the Incident Management & Continuity domain it really needs to be improved. So in this case we can conclude that increasing TMPI can also increase the level of resilience of the organization.

And based on the FGD, the researcher received the opinion of Bapak HD as follows:

a. TPMI in my opinion can be used as a way to measure the maturity level of handling security incidents, because the existing questions lead to existing conditions and open a perspective on handling a security incident and what conditions must be achieved in a company.
b. I think TMPI is very able to map incident response activities with existing questions and open opportunities to provide improvements that must be developed and provide measurable conditions in the XYZ organization
c. What I see is that IPA is very helpful for organizations to see the existing priority scale and provides an overview of the points that must be improved both in terms of expectations or existing conditions so that the manpower and resources, both material and non-material, deployed by the XYZ organization can more focused and on target.
d. From the existing data, it is clear that incident management has made a significant contribution and has also increased in several other points.

And based on the FGD, the researcher got the opinion from Bapak FH as follows:

a. The internal TMPI measurement method that is carried out is intended to measure the CSIR maturity level of an organization with several levels in three stages of maturity phase, making it easier to assess the maturity of the organization towards incident handling

b. With the phase level and assessment points in it, the organization can assess the weaknesses and strengths of incident handling so that the organization can purposefully make improvements to visible weak points.
c. With IPA the results make the organization see in priority the most important things to be improved so that it can manage resources to improve the things that are the highest and highest priority
d. It can be seen that the increase in maturity also increases the maturity level of the CRR because one of the CRR points is incident response which is measured specifically at TMPI.

For validation, the 2 researchers conducted interviews with 2 Experts separately, by explaining the methodology and the results obtained from the existing implementation, the opinion of Bapak BW was obtained. Researcher took his opinion because he was one of the people who followed the development process of the TMPI implementation process in Institutions/ Agencies/ Ministries and Companies in Indonesia. The opinions expressed are as follows:

a. Because the main focus of CSIR is the ability to respond and manage incidents. Maturity in handling incidents will also increase CSIR maturity. One of the parameters in measuring csirt maturity is the ability to respond/handle incidents.
b. Parameters for measuring TMPI maturity can be used as a mapping of what activities should/need to be done to improve the ability to handle incidents and this will have an effect on increasing CSIR maturity.
c. This IPA is very helpful in making priorities that are an important part of incident response in conducting incident triage, determining asset classification/criticality and incident classification. Using quadrants in IPA can greatly help with this priority.
d. Because one of the important components of Resilience is the ability to handle incidents.

And one of the SME's that the researcher took his opinion on is Bapak SW, who has worked at the XYZ Organization for 19 years and his current position is as an SME in Information Technology. The division head provides direction for the recommendation results to be validated from the opinion of the Internal SME and His opinions are as follows:

a. TMPI pays great attention not only to the aspect of fulfilling technology, but also other areas such as compliance with Standard Procedures, Learning Processes, Habituation in dealing with incidents and many things that currently XYZ organization is still not optimal in carrying out these things. So that from TMPI, new insights will be obtained that open up ideas for activities for improvement and of course very useful in efforts to improve the ability of incident handling.

b. Management expectations are something important as a basis for carrying out activities so that the activities carried out are in accordance with the needs of the XYZ Organization, as an analogy that there are many cutting-edge technologies in the market but not the most up-to-date technology that will be adopted for the company, but appropriate technology. with the company that will be implemented, because IPA does map the current level of performance with Management's Expectations, I think that this is the right thing.
c. Seeing the results of measurements carried out at TMPI and the proposed activities are simulated and the results can increase the results of measurements in CRR, of course this is one of the evidences in this case that resilience can also increase.

From the validation results, the researcher can propose that this Methodology can strengthen the hypothesis:

a. The Methodology can increase the maturity and capability of the CSIR to the expected Target based on the maturity level assessment
b. The methodology can increase the maturity of the CSIR as expected by determining some recommendations for improvement
c. With the increasing maturity of TMPI in the case of the XYZ organization, the level of organizational resilience as measured by CRR in the context of incident response also increases.

Kesimpulan

Based on the maturity level assessment using TMPI in chapter 4, this can help XYZ organization to determine what steps can be taken to improve incident handling that is currently being developed by the organization. Chapter 4 can also assist the organization in determining the priority of the program to be carried out so as to assist the organization in determining which of the activities to be carried out first and helping to determine the annual work program in the future.

Based on the results of validation through FGDs and interviews, experts said that measuring maturity level with TMPI can see more fully and help map the shortcomings of the organization's current incident handling and help determine the right work program to improve current incident handling.

Related to the IPA analysis in this research to help provide an overview to the management of the current performance achievements with the target management expectations with the Prioritization. From here, the researcher can provide input to the management of programs that are really needed in improving incident handling, adjusted to suitable management targets in determining the ability of incident handling.

BIBLIOGRAFI

Ardiyanti, H. (2014). Cyber-Security dan Tantangan Pengembangannya di Indonesia. *Politica*, 95–110.

Balan, S, Otto, J, Minasian, E & Aryal, A. (2017). *Data analysis of cybercrimes in businesses', Information Technology and Management Science*. *20*(1), 64–68.

Bodeau, D. J., & Graubart, R. (2011). *Cyber Resiliency Engineering Framework*.

Cloppert, M. (2009). *Security Intelligence: Attacking the Kill Chain. SANS Computer Forensics and Incident Response Blog*. Http://Computer-Forensics.sans.Org/Blog/2009/10/14/Security-Intelligence-Attacking-the-Kill- Chain/.

Creasey, J. (2013). *Cyber Security Incident Response Guide Version 1 2 Cyber Security Incident Response Guide DTP notes A Good Tip A Timely Warning An insightful Project Finding*.

Daniri, M. A. (2008). Standarisasi tanggung jawab sosial perusahaan. *Indonesia: Kadin Indonesia*, *2*(1), 1–36.

Department for Digital, Culture, M. and S. L. (2019). *Cyber Security Breaches Survey*.

DR Windriya, H Tanuwijaya, E. S. (2014). Audit Keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil Berdasarkan ISO 27002. *JSIKA*.

Ferdinand, J. (2015). Building organisational cyber resilience: a strategic knowledge-based view of cyber security management. *Journal of Business Continuity & Emergency Planning*, *9*(2), 185–195.

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber di Masa Pandemi Covid-19. *Jurnal ICT: Information Communication & Technology*, *20*(1), 42–52.

Indarta, Y., Ranuharja, F., Ashari, I. F., Sihotang, J. I., Simarmata, J., Harmayani, H., Algifari, M. H., Muslihi, M. T., Mahmudi, A. A., & Fatkhudin, A. (2022). *Keamanan Siber: Tantangan di Era Revolusi Industri 4.0*. Yayasan Kita Menulis.

Leech, N. L., & Onwuegbuzie, A. J. (2007). *array of qualitative data analysis tools: A call for data analysis triangulation. School Psychology Quarterly*.

Lendong, L. G. N. (2020). *Kerugian Akibat Cybercrime di 2021 Diprediksi Akan Tembus 6 Triliun USD - Tribunnews.com*.

O.Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). *The use of focus group* *discussion methodology: Insights from two decades of application in conservation. Methods in Ecology and Evolution,. 9*, 20–32. https://doi.org/https://doi.org/10.1111/2041-210X.12860.

Permana, A. (2021). *Indonesia's Cyber Defense Strategy In Mitigating The Risk of Cyber Warfare Threats* (Vol. 3, Issue 1).

Potteiger, B., Martins, G., & Koutsoukos, X. (2016). *Software and attack centric integrated threat modeling for quantitative risk assessment*. 99–108. https://doi.org/10.1145/2898375.2898390.

Pratama, E. A. (2013). Optimalisasi Cyberlaw untuk Penanganan Cybercrime pada E-commerce. *Jurnal Bianglala Informatika*.

Setiawan, M. B., & Nugroho, A. (2016). Penerapan Konsep Continuous Auditing: Studi Kasus Audit Kepatuhan Terhadap PTK 007 di SKK Migas. *Info Artha*, *5*(1), 107–126.

Tri Aryadi. (2018). *Indonesia's survival in age of cyber warfare - Opinion - The Jakarta Post*.

Windiani, R. (2017). Peran Indonesia dalam memerangi terorisme. *Jurnal Ilmu Sosial*, *16*(2), 135–152. https://doi.org/10.14710/jis.16.2.2017.135-152.