





Gema Wiralodra

Publication details, including instructions for authors and subscription information:
<https://gemawiralodra.unwir.ac.id>

	Gema WIRALODRA
	Editor-in-Chief: Yudhi Mahmud
	 Publisher: Universitas Wiralodra

IT Maturity Level Analysis Using Framework COBIT 5 Work for Management Cyber Incident: Case Study of Company Z in ICT Field

Inna Madiyaningsih^a, Kalamullah Ramli^b

^aDepartment of Electrical Engineering,
Universitas Indonesia, Indonesia,
inna.madiyaningsih@ui.ac.id

^bDepartment of Electrical Engineering,
Universitas Indonesia, Indonesia,
kalamullah.ramli@ui.ac.id

To cite this article:

Madiyaningsih, I & Kalamullah Ramli, K. (2023). IT Maturity Level Analysis Using Framework COBIT 5 Work for Management Cyber Incident: Case Study of Company Z in ICT Field. *Gema Wiralodra*, 14(2), 952-960.

To link to this article:

<https://gemawiralodra.unwir.ac.id/index.php/gemawiralodra/issue/view/22>

Published by:

Universitas Wiralodra

Jln. Ir. H. Juanda Km 3 Indramayu, West Java, Indonesia

IT Maturity Level Analysis Using Framework COBIT 5 Work for Management Cyber Incident: Case Study of Company Z in ICT Field

Inna Madiyaningsih^{a*}, Kalamullah Ramli^b

^aDepartment of Electrical Engineering, Universitas Indonesia, Indonesia, inna.madiyaningsih@ui.ac.id

^bDepartment of Electrical Engineering, Universitas Indonesia, Indonesia, kalamullah.ramli@ui.ac.id

*Correspondence: inna.madiyaningsih@ui.ac.id

Submit 27-05-2023, accepted 14-08-2023, published 15-08-2023

Abstract

Based on the report security year 2022 from company Z in the ICT sector, it was found that on the report firewall security, 96% of level threat is level critical, and 4% is level high. Report email security is session domain 27.3%; Session limits 15.35 %; Forti Guard AntiSpam-IP 3.11%, and the rest is receipt verification; directory filter and access control relay denied. With the challenge of current cyber-attacks, precious data assets need analysis to measure the the level of IT maturity that can ensure stakeholders' interest and maximize benefits and opportunities through technology information. We overcome limitations by analyzing IT maturity using COBIT 5. Research focused only on the APO13 and DSS05 process domains. A study was done to identify the problems based on results observation, checking, and use of a questionnaire in a direct manner. Measurement is done through method evaluation self and interviews deep with the IT team and all power expert who has COBIT certification 5. Analysis results show that the measurement level for the APO13 domain is 3, and for DSS05 is level 2. These results still need to be below the set level 4 target management; therefore, building a framework to monitor, track, and record security data in real time is necessary. With the build framework, Work can help lower the threat level from a critical level to a high level and increase the COBIT Maturity Level to APO13 and DSS05 according to organizational targets.

Keywords: COBIT 5, Cyber-Incident Management, IT Maturity, APO 13, DSS05

1. Introduction

This digital industry is in the middle of increasing competition and growing tight rapidly, PT Z remained committed to delivering the best service to be the choice foremost for providers of service technology information and communication in the country. The experience Work the same with the company parent at a time partner main, PT. ABC (State Electricity Company) manages more than 65 million customers and revenue of more than IDR 300 trillion, which has become a strength prime for expansion to the external market. PT Z offers deep total solution technology and applications network-based fiber optical in a manner thorough as a very reliable transmission medium. Support asset PT ABC's Right of Way (ROW) strategy allows it to reach customers all over Indonesia, even to the islands' outermost.

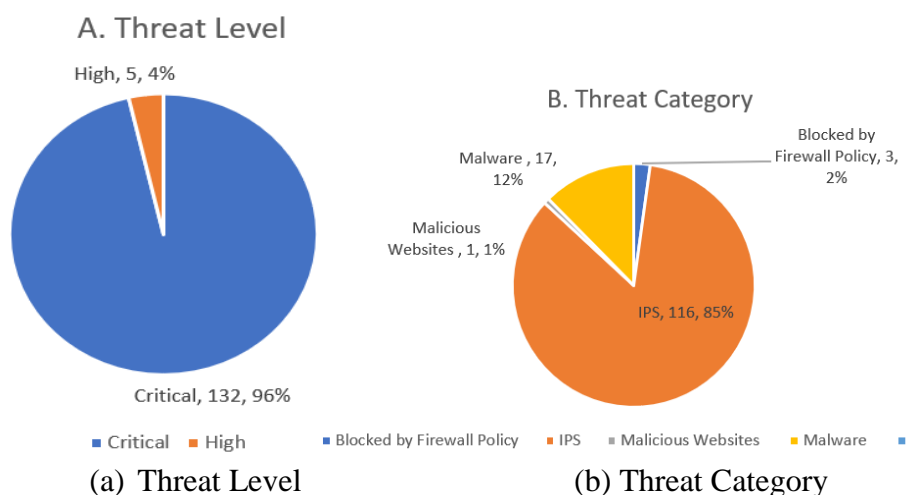
PT Z is a reflection of what should be owned by a company telecommunications in the modern era: comprehensive area coverage, time-fast delivery, and reliable network, as well excellent operational and service for whole stakeholder's interests. PT Z doesn't only provide a connectivity network but also a value plus for business. The goal is to have partners the best they can be and give certainty to customers to grow together going to excellence.

PT Z's vision is to become a provider of Indonesia's leading web-based ICT solution with use means strategic. PT Z's mission is (PT.Z, Company profile, 2022):

- (a) Provide clients with world-class ICT services to improve mark business;
- (b) In a manner proactive fulfil the needs and expectations of PT ABC with offer innovation and value;
- (c) Participation in development telecommunication national.

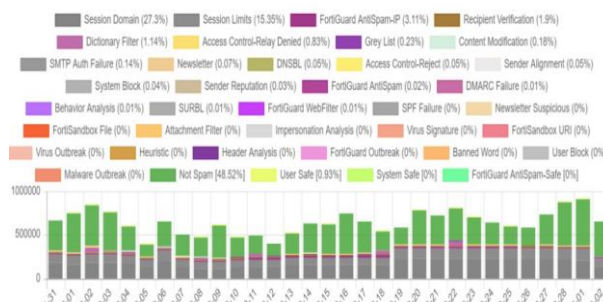
On the other hand, attack cyber matters to reputation company is one challenge faced by PT Z. Based on report security year 2022 from Z company, Firewall security report , 96% threat level at critical level and 4% at High level.

Figure 1
 Firewall Security report



Based on report security year 2022 from company Z, 85 % are IPS, 12 % are Malware, 2 % are blocked by firewall policy and 1 % are malicious websites. Email security report , namely session domain 27.3%; Session limits 15.35 %; FortiGuard AntiSpam-IP 3.11% , the rest receipt verification, directory filter, and access control relay denied. Email security shown in Figure 2.

Figure 2
 Email Security



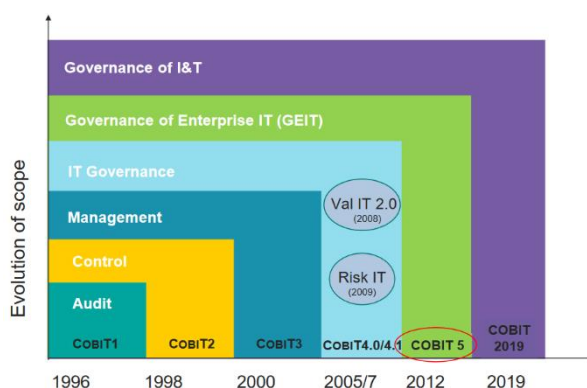
Based on the report Sandbox security, 99% has been cleared, and 1% risk is low. Report average monthly anti-virus security for Malware and PUAs, potentially apps No desired can be handled by anti-virus was 457 incidents (PT.Z, Cyber Security Report, 2022).

For 2023 dangerous attack cyber has been predicted by Gartner (2022). Impact financial in 2023 caused by attacks cyber in technology operational will reach more than \$50 billion. This figure still needs to include mark life human, litigation, insurance, fines rules, and loss of reputation. Gartner predicts that part great CEOs will too responsible and answer in a manner personal on incident cyber this. BSSN has predicted threat predictable cyber will appear in 2023. Threats cyber the including Ransomware, Data Leaks, APT Attacks, Phishing, Crypto-jacking, Distributed denial of service (DDoS), RDP Attacks, as well as Social Engineering, Artificial Intelligence (AI), IoT Cybercrime, and Web Defacement. Significant improvement in the number of years final means that several threats this possibility will continue until 2023 (BSSN, Cyber Security Monitoring Report, 2022).

With challenge attacks, reliable cyber will the higher every year, and the data assets it owns significant value, then needed analysis measurement level capable IT maturity ensure needs, conditions, and goals stakeholders interest evaluated in a manner balanced by goals achieved by the company in order to company capable utilize optimally and maximizing benefits and opportunities through technology information. We tried to overcome limitations by analyzing IT maturity using COBIT 5.

Figure 3

COBIT History



You can see in Figure 3 the history of COBIT. Even though COBIT 2019 has been there, COBIT 5 is considered more suitable used as a tool to analyze PT Z's enterprise IT governance (GEIT). GEIT's advantages are able to fulfill the need of decision targets stakeholders' interest rate in a manner balanced and appropriate with the agreement desired objective achieved by the company through the determination process priority in monitoring taking decisions and performance, and compliance to direction and purpose company. GEIT is not a discipline isolated science or a dedicated domain for IT) but become part of Corporate Governance. GEIT got ensure company can take optimal and maximize profits, benefits, and opportunities through technology information.

This paper serves to review analytics to measure the level of IT maturity at PT. Z uses framework work COBIT 5, which can increase the quality management of cyber incidents. This paper shared into five parts. Part 1 delivers an introduction short about the topic. Section 2 explains the method used. Section 3 delivers details about the results and discussion. Section 5 delivers the conclusion and identification of opportunities for future research.

2. Methods

A study was done to identify problems based on results observation, checking, and use of questionnaire in a manner right on the field. Study next with studies literature through related books, scientific journals, and online articles with problem research in organizations. Study this using COBIT 5 because there is a change significant in existing content that impacts the Governance of the enterprise IT (GEIT) implementation process.

GEIT focuses on goals as follows: Realization benefits- gives the company benefits through IT. Management risk in the IT realm in the company. Optimization source power - ensure adequacy capability to implement plan strategically, correctly, and effectively, plan, in a manner correct, and effective with source available power.

The COBIT 5 process has five domain processes, namely:

- 1) EDM: Evaluate, Direct, and Monitor. Management gives IT directives, monitor results achieved, evaluate alternative strategies, deliver IT direction, and monitoring achieved results.

- 2) APO: Align, plan, and organize. These domains relate to the identification process of how IT should contribute to the achievement of objectives and goals of business.
- 3) BAI: Build, Acquire, and Implement: This domain is related to identifying IT needs and managing programs and projects inside IT investment in these program projects.
- 4) DSS: Deliver, Service, and Support This Domain refers to the realization provision of IT services required to fulfill the needs of the stakeholder's interests.
- 5) Monitor, Evaluate, and Assess (MEA): This domain consists of related processes with evaluation process performance, compliance, evaluation adequacy, internal control, and monitoring obedience to external regulation.

The stage, furthermore, is to choose domains and objectives in the framework COBIT 5 work. This study focused on the APO13 domain and DSS05 to measure capabilities. APO 13 handles security information in the company from meaning to operation until monitoring it. DSS05 is a process in COBIT 5 focusing on setting security information to achieve the target set company. Measurement is done through method assessment self-evaluation and interviews deep with the IT team and all power experts with COBIT 5 certification. Recommendation repair will generate based on best practices of the framework used from the results measurement.

3. Results and Discussion

Based on the results analysis of data and documents, as well as interviews with the IT team and workforce expert who has COBIT 5 certification, the conditions moment this is as follows:

- 1) Report firewall security: 96% rate threat is level critical, and 4% are at a level high. Category threats 85% are IPS, 12% are Malware and firewall policies block 2%, and 1% are malicious websites.
- 2) Report email security: Reports email security is session domain 27.3%; Session limits 15.35%; FortiGuard AntiSpam-IP the remaining 3.11%. Our receipt verification, directory filter, and access control relay were denied.
- 3) Report security box sand: 99% done cleared and 1% risk low.
- 4) Report anti-virus security: The average monthly anti-virus security for Malware and PUAs, potentially apps that cannot be handled by anti-virus, was 457 incidents.

With a level of high threat that is almost 96% is a critical level, and category 85% threat is IPS and reports average monthly anti-virus security for Malware and PUAs, potentially apps No desired can _ handled by anti-virus is 457 incidents, then needed calculation, and IT maturity analysis through the COBIT 5 framework. Table 1 is the COBIT 5 measurement parameters where the level is used from 0-5.

Table 1
Assessment Criteria

Levels Value	Description	Details
0	Incomplete process	Determine whether the process is running or not.
1	Performed process level (One Attribute)	Ensuring the process achieves goals/results, which are determined by the available metrics For measure achievement, the achievement full from attribute This is reflected in each cycle and produces the expected output
2	Managed process level (Two attributes)	<ol style="list-style-type: none"> 1. Measure the degree to which process implementation is managed, with plan and monitoring process implementation. 2. Measure the extent of the product work produced by the process has been managed well, that is reflected in product work and the output of the process
3	Established process level (Two attributes)	<ol style="list-style-type: none"> 1. Measure the degree to which process implementation is managed, with plan and monitoring process implementation. 2. We measure the extent of the product work produced by the process has been managed well, which is reflected from results work and process performance.
4	Predictable process levels (Two attributes)	<ol style="list-style-type: none"> 1. Measure as far as results measurement used to ensure that process execution can support achievement objective organization. 2. Measure the degree to which a process is regulated quantitatively to produce a reliable method.
5	Optimizing process (Two attributes)	<ol style="list-style-type: none"> 1. There is a repair process carried out. 2. There are results obtained from the implementation repair that process.

Table 2 refers to ISO/IEC 15504 in determining rating levels.

Table 2
Rating Levels

Information	Explanation	% achievement
N	Not reached	0 to 15 % achievement
P	Achieved part	>15% to 50 % achievement
L	Almost achieved	> 50% to 85 % achievement
F	Achieved	>85% to 100 % achievement

Manage Security (APO13)

COBIT 5 defines APO13 as having three processes, namely APO13.01 Establish and Maintain System Management Security Information (SMKI), APO13.02 Defining and Managing Risk Treatment Plan Security Information, and APO13.03 Monitors and Supervise System Management Security Information (SMKI). Based on the results mapping role on the RACI Chart is obtained that application management APO13 process security at PT Z is carried out by the Architecture Manager daan security Technology information, Vice President of Systems Technology information, Technology Manager information, Director Network, and infrastructure.

Table 3
RACI Chart Analysis of the process APO13

Component	Organizational title
R	Architecture Manager daan security Technology information
A	Vice President of Systems Technology information
C	Technology Manager information
I	Director Network and infrastructure

Percentage achievement be measured with achievement process characteristics. In the APO13 process, the assessment elements of APO13.01 gets a value of 100% with the category "Highly Achieved," so can the following evaluation characteristic of the APO13.02 process, which also receives a 100% share and is also in the "partial" category significant "achieved" is entered. The APO13.03 process achieves a percentage of 65% classified completed in a manner broad, so it can conclude that the APO13 PT.Z is at level 4, as described in Table 4.

Table 4
APO13 Score

	level 0	Level 1	Level 2	Level 3	Level 4	Level 5
APO13	100 %	100%	100 %	65%	-	-

From the evaluation of the results done, crosscheck validity results and results sheet appraisal. Table 5 explains the effects of Korschek on APO process 13.

Table 5
Crosscheck APO13

	Test results	Depth interview & data processing	crosscheck
APO13	3	matches	V

Furthermore checking between results testing with company targets .

Table 6
APO13 GAP Analysis

Name	this time	Target Levels	GAP
APO13	3	4	1

In the APO13 process, there are 6 recommendations that can be made for repairs so the expected target company can achieved

- 1) Building integrated security information kebaya elements (Server, network device, security device as source of log data
- 2) Every log on element the shipped to the log and activity management server for log parsing and normalization.
- 3) Monitoring all operational logs in the ticketing system and threats security from device network, servers, to security devices to support achievement of SLA disruption cyber security.
- 4) Build helpful security information collect and analyze every log that appears in the ticket system on the infrastructure of PT. Z.
- 5) Monitoring user activity in access Z enterprise internal application
- 6) Record user activity on the device PTZ network.

Manage Security Services (DSS05)

RACI helps in determine functions and tasks employees at the company.

Table 7

RACI DSS05 analysis

Element	Position Level
R	Architecture Manager daan security Technology information
R	Technology Manager information
C	Vice President of IT Systems

Percentage Skills be measured with achievement process characteristics. On the DSS05 process, score DSS05.01 characteristics got percentage of 100 percent for the most categories accomplished, followed score DSS05.02 process characteristics also got percentage of 100 percent and also included. Part big achieved in category. In the DSS05.03 process obtained percentage 58 % entered in category so achieved so can it can be concluded that the DSS05 PT Z process is at level 2 like described in table 8.

Table 8

DSS05 Level Measurement

	L-0	L-1	L-2	L-3	L-4	L-5
DSS05	100%	100%	100 %	58%	-	-

From the evaluation of the results, corscheck validity results and results sheet appraisal. Results from appraisal. Table 9 is results crosscheck DSS05.

Table 9

Triage DSS05

	Test Results	Depth interview & data processing	xcheck
DSS05	2	in accordance	V

PT Z assumes management IT security is at level four. Table 6 explains the GAP analysis DSS05 PT Z.

Table 10

Analysis of GAP DSS05

Name	mark	company targets	GAP
DSS05 (MSC)	3	4	1

4. Conclusion

Based on the evaluation of the result, the achievement of APO 13 PT Z is level 3. For parameters of achievement DSS05 PT Z is level 2 and not yet in accordance with the target of PT. Z. It is indicated that PT. Z needs to build integrated security information to stout elements (Sever, network device, security device as log data sources) and establish an IT security strategy with objective end to support business strategy company with define it into the initiative security: technology, people, and process.

In the APO13 process, there are six recommendations that can be made for repairs so the expected target company can achieve

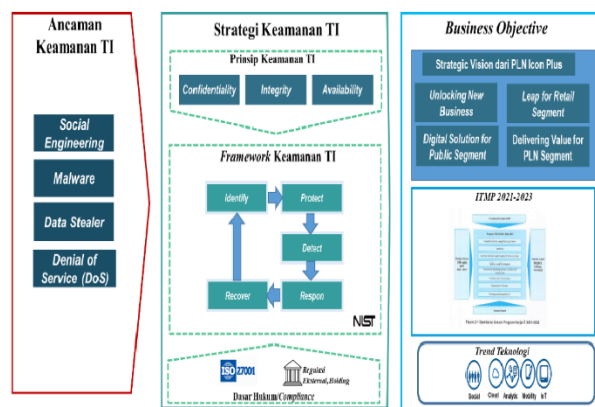
- 1) Building integrated security information kebaya elements (Server, network device, security device as a source of log data.
- 2) Every log-on element the shipped to the log and activity management server for log parsing and normalization.

- 3) Monitoring all operational logs in the ticketing system and threats security from device network, servers, to security devices to support the achievement of SLA disruption cyber security.
- 4) Build helpful security information, collect and analyze every log that appears in the ticket system on the infrastructure of PT. Z.
- 5) Monitoring user activity in accessing Z enterprise internal application.
- 6) Record user activity on the device PTZ network.

In the DSS05 process, there are possible recommendations made for repairs so the expected target company can achieve with establish an IT security strategy with the objective end to support the business strategy company with the proposal as follows.

Figure 4

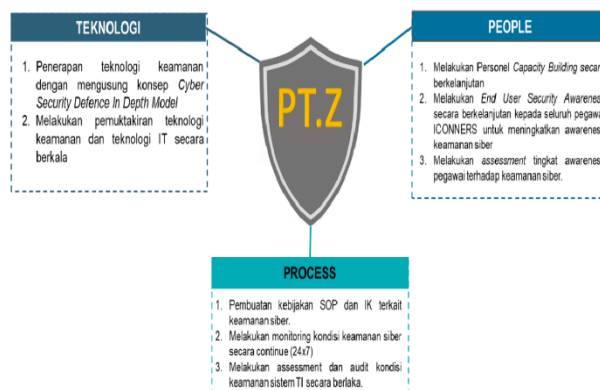
IT security strategy framework



From strategy security it is expected lowered in form initiative initiative security example.

Figure 5

Initiative security



Initiative security shared into 3 namely: technology, people and internal processes activity.

5. References

- Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and it governance under cobit 5 framework: A case study. *Webology*, 18(Special Issue on Information Retrieval and Web Search), 294-310.

- BSSN. (2022). Cyber Security Monitoring Report. <https://www.bssn.go.id/monitoring-keamanan-siber-2022/>
- Amali, L. N., Katili, M. R., Suhada, S., & Hadjaratie, L. (2020). The measurement of the maturity level of information technology service based on COBIT 5 framework. *Telkomnika (Telecommunication Computing Electronics and Control)*, 18(1), 133-139.
- Andry, J. F., & Setiawan, A. K. (2019). IT governance evaluation using COBIT 5 framework on the national library. *Jurnal Sistem Informasi*, 15(1), 10-17.
- Fernandes, A. J., Hartono, H., & Aziza, C. (2020). Assessment IT governance of human resources information system using COBIT 5. *International Journal of Open Information Technologies*, 8(4), 59-63.
- Iqbal, A. (2016). *Evaluasi Business Continuity Plan Menggunakan COBIT 5 (Studi Kasus: DSSDI Universitas Gadjah Mada)* (Doctoral dissertation, Universitas Gadjah Mada).
- Miles, M & Huberman, M. (2014). Analisis Data Kualitatif. Jakarta: UI-Press.
- Nurhidayat, T. (2022). Lanskap keamanan siber Indonesia. Jakarta: BSSN
- Sianida, R. Y., Afiana, F. N., & Wahyudi, R. (2020). IS governance evaluation using COBIT 5 framework on the central statistics agency of banyumas district. *Journal of Computer Science and Engineering (JCSE)*, 1(1), 1-9.
- Utami, E., & Amborowati, A. (2019). Evaluasi Penerapan Sistem Informasi Manajemen Tugas Akhir Di Universitas Amikom Yogyakarta Menggunakan Framework Cobit 5. *Respati*, 14(1).
- <https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we>
- PT.Z. (2022). Cyber security report. PT. Z.
- PT.Z. (2022). Milestone company 2021- 2025. PT. Z.