Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN: 2548-1398
Vol. 7, Special Issue No. 2, Februari 2022

ANALYTICAL AND EVALUATION CAPABILITY LEVEL OF KNOWLEDGE MANAGEMENT FOR PENETRATION TESTER KNOWLEDGE PRESERVATION USING COBIT®5 SELF-ASSESSMENT IN AN IT SECURITY COMPANY

Andriko Perdana, Mohammad Achmad Amin Soetomo, Charles Lim
Swiss German University Indonesia
Email: andriko.perdana@gmail.com, mohammad.soetomo@sgu.ac.id, charles.lim@sgu.ac.id

Abstract

The purpose of this study is to standardize work roles and their level of proficiency and to determine the ability of Knowledge Management in preserving Pentester Knowledge using Confluence® at XYZ Company. The data used and processed in this study were obtained from interviews and observations with the principal for work roles. The results of standardization of job roles are obtained by mapping using the NICE Framework, and proficiency levels can be mapped using the CIISec Framework. Knowledge Management capability assessment is carried out using COBIT®5 Domain APO07 (Manage Human Resources and BAI08 (Manage Knowledge). Observations and interviews are carried out in the order of data collection where respondents are represented by IT Director, HR Head, Confluence Manager, Sales Department Chair, and Team IT Governance The result of Capability Level is 2 (Managed Process), meaning that IT Governance at the time of implementing Knowledge Management has generally been carried out with planning, monitoring and adjustment, but several processes have not yet been implemented, have been presented to the Company's management as feedback and recommendations for improvement of planning process.

Keywords: cobit®5; nice framework; ciisec; knowledge management system; knowledge capability assessment.

Introduction

Like in other countries, the digital economy is currently multiplying in Indonesia, where new companies and start-ups compete to provide digital services as part of their business development. Indonesia is the largest digital economy market or internet economy in Southeast Asia (Prayoga, 2020). IT security projects to ensure data security and applications are popping up a lot. Many government and private organizations, manufacturing industries, and small and medium-sized industries are scrambling to implement them. For example, 13.7 million of those MSMEs have utilized digital technologies in their business activities (Liputab6.com., 2021). Many systems and applications are created and can be accessed by the public through the

How to cite: Perdana. A. et al (2022) Analytical and Evaluation Capability Level of Knowledge Management For Penetration Tester Knowledge Preservation Using Cobit®5 Self-Assessment In an It Security Company, *Syntax Literate: Jurnal Ilmiah Indonesia, 7*(2).
E-ISSN: 2548-1398
Published by: Ridwan Institute

internet. But the contrast is that cyber security engineers are limited in number as many companies try to recruit and maintain their talent.

Along with this growth of technological adoption, cyber-attacks are also multiplying. From 28,430,843 attacks in 2015, the number became 135.672.984 attacks in 2016 (Assidiq, Hasbi, 2020). In 2021, Cisco discovered that one-third of Indonesian SMEs suffered from cyberattacks. Financial loss caused reached $1 million (Jakartapost.com., 2021). Consequently, the requirement for cybersecurity experts also surges and causes a lack of talent. CEO of PT Xynexis International stated that Indonesia needs a lot of cybersecurity talents. The Company also collaborated with Kominfo to search for thousands of cybersecurity talents in (Suhartadi, 2016).

Besides the positive impacts for I.T. security companies in terms of growth and revenues, surges in need of cybersecurity experts also mean a higher turn-over rate for such a company. According to Washington Post, there are nearly 465,000 unfilled cyber jobs in the USA, according to data gathered under a Commerce Department grant (Joseph Marks., 2021). And according to 2021 (ISC)² Cybersecurity Workforce Study (Cybersecurity, I S C, 2021) the world has a shortage of 2.7 million cyber security professionals to defend organizations adequately. ((ISC)² stands for International Information System Security Certification Consortium).

XYZ Company is an I.T. Security company owned by a U.S. investment group in Dubai (UAE). XYZ company has been serving I.T. security since 2004. The Company has helped with more than 450 projects. Since 2017, XYC company has expanded I.T. security services to other countries in Asia Pacific such as Singapore, Thailand, UAE & Australia.

The turn-over rate has become a significant issue many cybersecurity companies have to deal with lately. Any companies cannot forbid some employees planning to leave a company to seek a better future. Especially for the millennial generation, salary and compensation and employee involvement did not significantly influence turn-over intention (Frian, Antonio, 2018). Although employees leave their companies is inevitable, companies must maintain their competitiveness. In today's economy, Knowledge has become a considerable asset for companies.

Moreover, with a high rate of employee turnover in the XYZ Company, it is crucial to retain Knowledge accumulated from past Research or projects. The list of turn-over of the Company's employees in the last three years can be seen in table 1.1.

Table 1
Number of Resign Employers

Year	Number of resign employee
2019	5 (1 principal, 2 Sr pentester, and 2 pentester)
2020	3 (1 Sr. Pentester, 1 pentester, and 1 Jr. pentester)
2021	3 (1 pentester, and 2 Jr. Pentester

Knowledge Management develops systems and processes for acquiring and sharing intellectual property and collecting Knowledge. It aims to increase the amount

of valuable, practical, and meaningful Information and increase learning for both individuals and teams. Additionally, knowledge management can maximize the value of an organization's intellectual foundation beyond function and location. In short, knowledge management is the process of sharing perspectives, ideas, experiences, and information in the right place and at the right time.

Research Method

NICE and CIISec frameworks are used as the basis of the current study's Qualitative Research to map and assess XYZ Company Pentesters KSA with guidance from NIST (NIST., 2021) COBIT® 5 processes APO07 and BAI08 are used to perform a qualitative analysis of the Company's KSA management tool (Confluence®) with COBIT® 5 Self-assessment guidance (ISACA 2013b., 2013). The research method is limited to close interviews and submission of questionnaires by stakeholders, Interviews and Observation (Based on RACI), and self-assessment questionnaires to Top Management and the I.T. governance team (Research schedule can be seen in the appendix C)

There are four milestones to be achieved in the research flowchart, as shown in Figure 1:

1. Mapping work roles from the current Pentesters work role and NICE Framework.
2. The mapping Proficiency level of KSA using CIISec Skills Framework
3. Conduct Knowledge Management capability assessment using COBIT® 5 processes
4. Conclusion and Recommendation

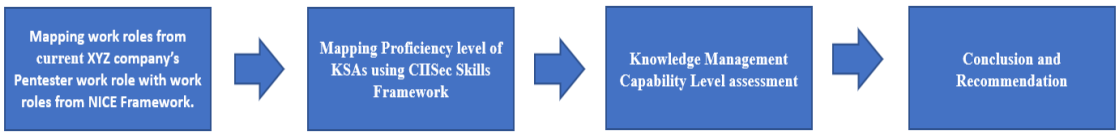


Figure 1
Research Method flowchart

1. **Step 1 - Mapping work roles from the current XYZ company's Pentesters work role and work roles from NICE Framework.**

   Principals and Senior Pentesters assist this step. They review the mapping work roles between the current and the NICE Framework. The result will be the work role from NICE Framework that has similarity function with current Pentesters work roles.

2. **Step 2 - Mapping Proficiency level of KSA using CIISec Skills Framework.**

   In this step, with the help of Principals and Senior Pentesters and validated with the H.R. department and Sales Department, the Researcher will set and measure current KSA proficiency level using the CIISec Skills Framework ("CIISec Skills Framework.," 2019) The result of this step is current level of KSA Proficiency. The

H.R. department involved validating the effect while the Sales department applied to have feedback on current competencies required to conduct I.T. Security Project from clients. The sample result in this step is shown in table 2.

Table 2
Sample result of KSA proficiency level

Penetration Tester		Company XYZ Level			
		Jr. Consultant	Consultant	Sr. Consultant	Principal
Knowledge					
K0001	Knowledge of computer networking concepts and protocols, and network security methodologies.	1	2	5	6
K0002	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1	2	4	5
K0003	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.	1	2	4	5
K0004	Knowledge of cybersecurity and privacy principles.	2	3	4	5
K0005	Knowledge of cyber threats and vulnerabilities.	2	3	5	6
K0006	Knowledge of specific operational impacts of cybersecurity lapses.	2	3	4	5
K0009	Knowledge of application vulnerabilities.	2	3	5	6
K0018	Knowledge of encryption algorithms	1	2	4	5

This step will produce KSA Proficiency Level of XYZ Company Pentesters preserved in Confluence® (figure 2).

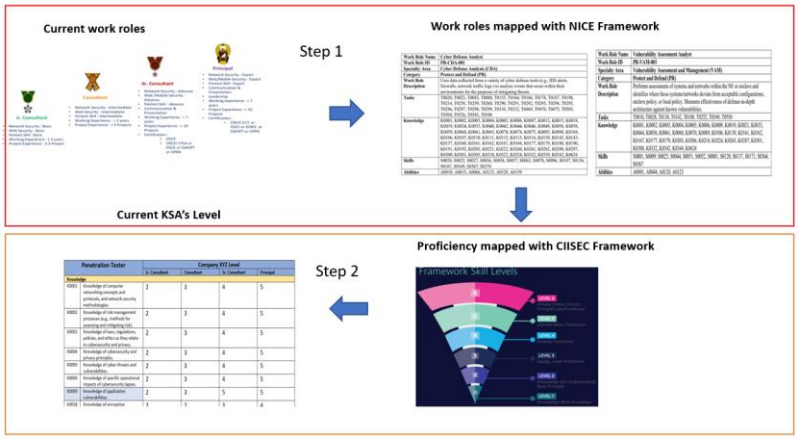


Figure 2
Steps to produce KSA Proficiency Level

3. Step 3 - Knowledge Management Capability assessment

Knowledge Management Capability assessment will be conducted using COBIT® 5 Self-Assessment for APO07 (Manage Human Resources) and BAI08 (Manage Knowledge).

This step is to measure the current Capability level of Knowledge Management of the Company to support the preservation of Pentesters KSA. In this step, the assessment will use questionnaires from COBIT® 5 Self-Assessment (Figure 3.3 and Figure 3.4). The result of this step is the current capability level and Action Plan for Process improvement will be planning in this step (Figure 3.5). Based on guidance (ISACA 2013b., 2013) assessment is undertaken by s small team of I.T. Management

consists of Top-level Management, H.R. Head, Confluence Manager and a representative from the I.T. Governance team.

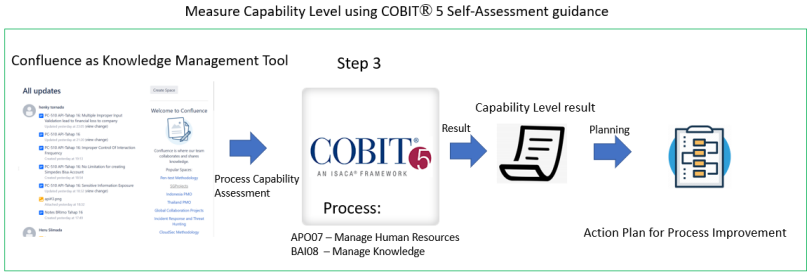


Figure 3
Step 3 using COBIT®5 Self-Assessment

4. Step 4 - Conclusion and Recommendation

In this step, we will conclude the result of the Research and provide a recommendation for KSA Proficiency Mapping Result (Step 1 & 2) and Process improvement that planned in step 3 (figure 3.6). (The detail research activities can be seen in Appendix D)

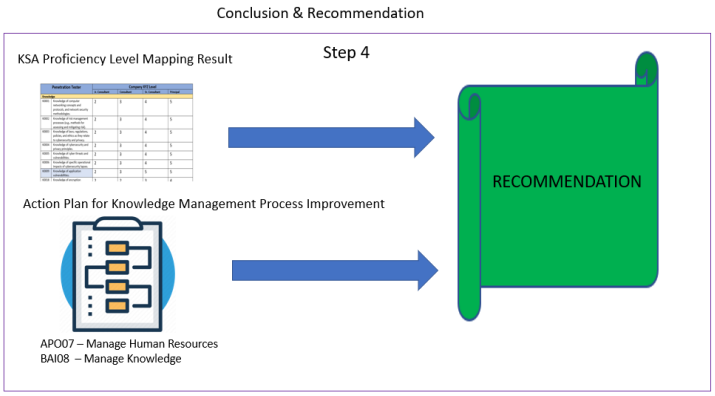


Figure 4
Step 4

Results and Discussion

1. KSA Proficiency Level Mapping Result

From a series of interviews and discussion with principals and senior consultants, all agreed that NICE Framework KSA items is easier to be implemented then CYBOK. Based on the NICE Framework assessment, penetration testing roles in XYZ Company comprise two (2) Work Roles defined by the NICE Framework. They are Vulnerability Assessment Analyst (PR-VAM-001) and Cyber Defense Analyst (PR-CDA-001) (Table 2.6 dan table 2.7). Both these roles are under Protect and Defend (P.R.) category.

As defined by the NICE Framework, the P.R. category is responsible for identifying, analyzing, and mitigating threats to internal information technology systems and networks. As for the identified Work Roles, Vulnerability Assessment Analyst (VAM) and Cyber Defense Analyst (CDA), NICE Framework defined them as:

Vulnerability Assessment Analyst (PR-VAM-001): Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats ().

Cyber Defense Analyst (PR-CDA-001): Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Table 3
Cyber Defense Analyst Work Role Detail

Work Role Name	**Cyber Defense Analyst**
Work Role ID	**PR-CDA-001**
Specialty Area	**Cyber Defense Analysis (CDA)**
Category	**Protect and Defend (PR)**
Work Role Description	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs.) to analyze events that occur within their environments for the purposes of mitigating threats.
Tasks	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
Skills	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
Abilities	A0010, A0015, A0066, A0123, A0128, A0159

There is knowledge that required in XYZ company but not available in NICE Framework work roles but added in KSA Mapping result (Table 4)

Table 4
Additional knowledge from other work roles

Knowledge	Detail	Work roles in NICE Framework
K0523	Knowledge of product and nomunclature of major vendors (e.g., security suites – Trend Micro, Symantec, McAfee, Outpost, and Panda) and how those products affect exploitation and reduce vulnerabilities	Exploitation analyst
K0529	Knowledge of scripting	Exploitation analyst
K0555	Knowledge of TCP/IP networking protocols	Target Developer

Knowledge	Detail	Work roles in NICE Framework
K0561	K0621Knowledge of the basics of network security (e.g., encyption, firewalls, authentication, honey pots, perimeter protection)	Target Developer
K0621	Knowledge og risk scoring	Target Developer

The mapping results obtained are 99 KSA items divided into 64 knowledge items, 26 skills items, and 9 abilities items. The results of this KSA Proficiency mapping provide an overview of the current KSA proficiency level condition of the Pentesters. The result is shown this table 4 below.

Table 4 is taken from documents containing the results of mapping the knowledge, skills and abilities of the pentester. This document was created by the researcher based on the mapping of work roles from the NICE Framework tool provided by NIST (NICE Framework Owner). The Proficiency level filled by interviewing Principals using references from the CIISec Framework and the whole results are validated again by Principals. The results of the mapping so far have been quite satisfactory for the company after the results were presented to Management. Especially for principals, it is considered sufficient to guide Pentesters whose KSA level is below them. Given that one work role in a company is a combination of 2 work roles in the NICE Framework.

2. Action Plan for KSA Proficiency Level Improvement

There is some action planning recommended by researcher. The first recommendation is to start standard cyber security workforce for work roles in the company. The other is to maintain and upgrade KSA Proficiency level to deal with future trends of the cybersecurity industry, and promote more Junior pen-testers to become pen-testers and senior pen-testers. Currently, only Pentesters, Senior Pentesters and Principals Mondays can be sold to the clients when conducting projects. Junior pen-testers only work as an assistant for roles above them.

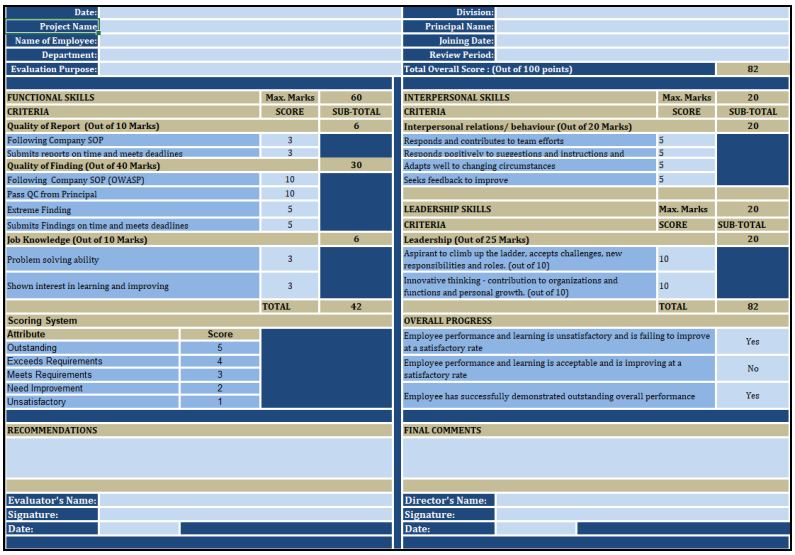
To do that Researcher has recommend a performance review to XYZ Company. Reviewers consist of the Project Manager, their Supervisor and the H.R. team. The performance of Penetration testing consultants will be measured based on their achievement in each project using a scorecard.

To measure the score of each project, we create a Microsoft Excel (Picture 4.1) file that consists of measurement on technical skills and soft skills. List of measurement items made based on input from Project Manager, Principal Level Consultants and H.R.

The score is divided into five criteria:

1. Quality of finding (technical skills)
2. Quality of report (technical skills)
3. Job knowledge (technical skills)

4. Interpersonal (soft skills)
5. Leadership (soft skills).



Date:			Division:		
Project Name:			Principal Name:		
Name of Employee:			Joining Date:		
Department:			Review Period:		
Evaluation Purpose:			Total Overall Score : (Out of 100 points)		82
FUNCTIONAL SKILLS	Max. Marks	60	INTERPERSONAL SKILLS	Max. Marks	20
CRITERIA	SCORE	SUB-TOTAL	CRITERIA	SCORE	SUB-TOTAL
Quality of Report (Out of 10 Marks)		6	Interpersonal relations/ behaviour (Out of 20 Marks)		20
Following Company SOP	3		Responds and contributes to team efforts	5	
Submits reports on time and meets deadlines	3		Responds positively to suggestions and instructions and	5	
Quality of Finding (Out of 40 Marks)		30	Adapts well to changing circumstances	5	
Following Company SOP (OWASP)	10		Seeks feedback to improve	5	
Pass QC from Principal	10				
Extreme Finding	5		LEADERSHIP SKILLS	Max. Marks	20
Submits Findings on time and meets deadlines	5		CRITERIA	SCORE	SUB-TOTAL
Job Knowledge (Out of 10 Marks)		6	Leadership (Out of 25 Marks)		20
Problem solving ability	3		Aspirant to climb up the ladder, accepts challenges, new responsibilities and roles. (out of 10)	10	
Shown interest in learning and improving	3		Innovative thinking - contribution to organizations and functions and personal growth. (out of 10)	10	
	TOTAL	42		TOTAL	82
Scoring System			OVERALL PROGRESS		
Attribute	Score		Employee performance and learning is unsatisfactory and is failing to improve at a satisfactory rate		Yes
Outstanding	5		Employee performance and learning is acceptable and is improving at a satisfactory rate		No
Exceeds Requirements	4		Employee has successfully demonstrated outstanding overall performance		Yes
Meets Requirements	3				
Need Improvement	2				
Unsatisfactory	1				
RECOMMENDATIONS			FINAL COMMENTS		
Evaluator's Name:			Director's Name:		
Signature:			Signature:		
Date:			Date:		

Figure 5
Scoring Card

Every time a project closes, Principals, together with the project manager and H.R., will give a score for every team member based on their performance when involved in the I.T. Security Projects. H.R. Team will collect the score.

The Researcher also proposed and discussed with the H.R. department to have rewards based on scores collected using the scoring card, and the result is shown in table 5.

Table 5
Scoring references for reward

Current Level	Next Level	Point	Time Duration
Junior Consultant	Consultant	Min 6500 24 Project a year with average score per project 90	3 years
Consultant	Sr. Consultant	Min 11000	5 years
Sr. Consultant	Principal	Min 15000	7 years

3. Self-Assessment Result for APO07 Manage Human Resources

The process of managing human resources focuses on ensuring the arrangement, optimal placement, decision, and human resource skills. The result for Self-assessment showed in figure 4.2 after being filled by Management Representative (The Self-assessment form result is available in the appendix A).

Process Name	APO007 - Manage Human Resources									
Description	Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people.									
Purpose	Optimise human resources capabilities to meet enterprise objectives.									
Level	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
Process Attribute		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA5.2
Process by Percentage		100%	95%	90%	5%	5%	5%	5%	5%	5%
Rating by Criteria		F	F	F						
Capability Level Achieved				2						

Figure 6
APO07 Achievement Level

Based on the data on the achievement of the level of each process, the calculation of the average capability levels is as follows.

$$\text{Capability Level} : \frac{\frac{(0*1)+(1*0)+(2*2)+(3*0)+(4*0)+(5*0)}{2}}{2} : \frac{4}{2}$$

$$\text{Capability Level} : 2$$

Level 2 means that XYX Company Process Capability level is managed. The performed process is now organised (planned, monitored and adjusted), and its work products are appropriately established, controlled and maintained.

XYZ company have not set the capability level target for APO07 yet since this research is the first assessment for it. Since COBIT® 5 have level 5 as the highest capability, if we compare with current achievement, the gap will be 3 (Figure 4.3).

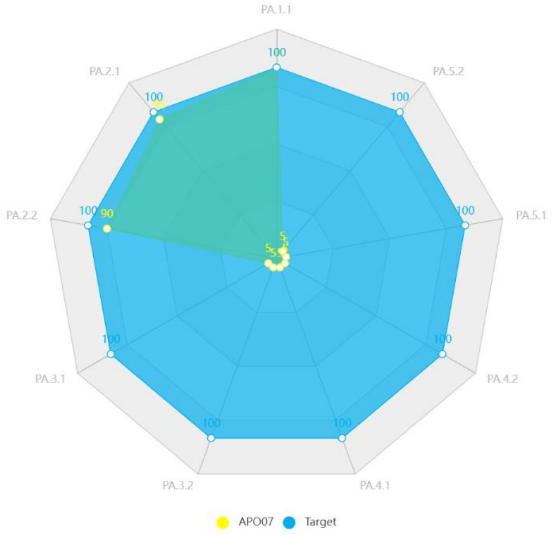


Figure 7
Gap Capability analysis for APO07

4. Self-Assessment Result for BAI08 Manage Knowledge

The Manage Knowledge process focuses on maintaining the availability of relevant, current, and validated Knowledge that can be trusted to support all process activities and facilitate decision making. The total result for Self-assessment showed in figure 4.4 after being filled by Management Representative (The Self-assessment form result is available in the appendix B).

Process Name	**BAI08 - Manage Knowledge**									
Description	aintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making. Plan for the identification, gathering, organising, maintaining, use and retirement of knowledge.									
Purpose	Provide the knowledge required to support all staff in their work activities and for informed decision making and enhanced productivity.									
Level	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
Process Attribute		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA5.2
Rating by Precentage		100%	95%	95%	5%	5%	5%	5%	5%	5%
Rating by Criteria		F	F	F						
Capability Level Achieved				2						

Figure 8
PA 2.2 Summary of Capability level Assessment of BAI08

Based on the data on the achievement of the level of each process, the calculation of the average capability levels is as follows.

$$\text{Capability Level} : \frac{(0*1)+(1*0)+(2*2)+(3*0)+(4*0)+(5*0)}{2} : \frac{4}{2}$$

Capability Level : 2

Level 2 means that XYX Company Process Capability level is managed. The performed process is now organised (planned, monitored and adjusted), and its work products are appropriately established, controlled and maintained.

XYZ company have not set the capability level target for BAI08 yet since this research is the first assessment for it. Since COBIT® 5 have level 5 as the highest capability, if we compare with current achievement, the gap will be 3 (Figure 4.5).

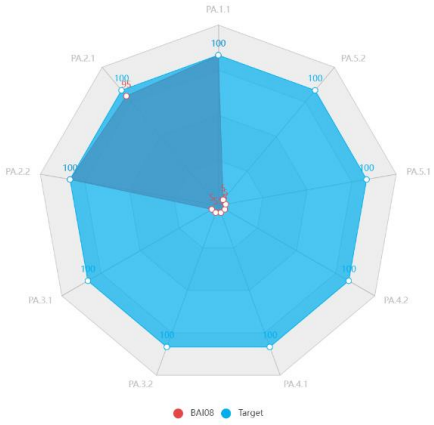


Figure 9
Gap Capability analysis for BAI08

5. Action Plan for Knowledge Management Process (APO07 and BAI08) Improvement

The resulting research from the assessment has been gathered and informed to the XYZ Company Management. The meeting is conducted to discuss the result and the action plan based on COBIT®5 Self-Assessment guidance. The main result is the management focus will not set target level or level up the current Capability Level but more to focus on improvement where investment for the action plan can be measured. Both actions for processes are shown in table 4.6 and table 4.7.

The Management also conduct some action as response of the result, which are:

- Establish Internal Academy as Knowledge sharing center that act as internal training center to prepare internship employees, new hire employees and current employees to learn a lot of knowledge in IT Security that will be mentored by Principals and Senior Pentester. This is as additional to current Confluence® to improve current Knowledge Management Process (BAI08).
- Hire talent manager and Human Capital expert for planning Human Capital development for XYC Company to improve current Human Resources Management (APO07).

6. Validating

Validity is used as a measure of the quality of a study. The study is considered objective if someone comes to the same analysis using the same working method. The validity of the survey indicates the extent to which the level of interpretation and concept obtained has appropriate implications between the Researcher and the participants.

a. Expert Validation with COBIT®5 Certified Consultant

Based on discussions with Siti Kamila (COBIT®5 Certified number:04023484-01-PXG4) and XYZ Company IT Governance Team. The result is also presented to the Top Management.

it can be summarized as follows:

- The Assessment of Processes (APO07 & BAI08) in the research framework providing a good view of Capability Level assessment since the guidance from COBIT®5 is followed.
- The data obtained and analysed using COBIT®5 can provide a picture of the current Capability Level of Knowledge Management.
- The questionnaire was filled correctly using Self-Assessment tool provided by ISACA.
- The result based on judgment by Management Representative (Top Management, H.R Head, Confluence Manager, and IT Governance).
- The Top Management has received the result and use it as feedback and have plan to conduct the assessment as annual activity that need to be conducted by IT Governance team although the assessment only for Pentesters not all IT Security workforce of the company.

b. Expert Validation with H.R Head and Internal CPHCM consultant

Based on discussions with Donny Silangit (H.R. Head of XYZ Company) and Robby Anzil Firdaus (CPHCM Certified) and presented to the top Management, their opinion on the research result is as follows:

- The research framework can provide an overview of the current KSA Proficiency Level of the Pentesters, which Management needs. And their Feedback: It should be conducted to other consultants like I.T. Governance, Forensics, Threat Hunting, and Fraud Intelligent team.
- The work roles result mapping from NICE Framework can represent the current work roles condition in the Company.
- The Proficiency Level can describe the competencies of the Pentesters team where the team competencies for IT. Pentest Projects suits the client requirement.
- The result has received by Top Management as feedback for future improvement

7. Observation

In this thesis, the researcher immerses himself in the setting where the respondent is, while taking notes, because the researcher is the Project Manager who sees, supervises and lead the Pentesters directly in the implementation of the IT Security project. As part of the company with 4 years of experience is used to help map out work roles and directly involved in daily process of Knowledge Management within the company has given the researcher enough information for conduct capability assessment. The research is going well in terms of data collection, interview process and presentation process, because this research is supported by XYZ Company Management since the beginning. A lot of companies do not agree and support their employees' competencies capability measured and published as thesis, since the employee competencies sometimes are compared against other companies to have winner in the bidding process where the winner will get the

project. This information is used to be kept confidentially . The company accepts research results with open arms as part of improvement feedback for the company.

Conclusion

Work roles in the XYZ Company can be mapped using NICE Framework, Proficiency level of each work roles can be measured using CIISec Framework, The results of COBIT® 5 Self-Assessment for the Capability level of Knowledge Management is in level 2 (Managed service), If work roles and proficiency level are using standard frameworks, it can be measured its capability and its improvement using any frameworks, Although COBIT 5 Self-assessment is a precursor to more rigorous, evidence-based assessment but enough to assess the capability level for a system, so that the company can take further action, and COBIT® 5 have limitation for providing processes on how to measure costs and time to level up Capability level of Knowledge Management.

BIBLIOGRAFI

Assidiq, Hasbi, and Armelia Syafira. (2020). *Qualifying Cyber Crime as a Crime of Aggression in International Law*. Google Scholar

"CIISec Skills Framework." (2019). *CIISec Skills Framework*. Google Scholar

Cybersecurity, I S C, and Workforce Study. (2021). *A Resilient Cybersecurity Profession Charts the Path Forward*. Google Scholar

Frian, Antonio, and Fransiska Mulyani. (2018). *Millenials Employee Turnover Intention In Indonesia*. *11*(3). Google Scholar

ISACA 2013b. (2013). *COBIT Self-Assessment Guide: Using COBIT 5*. Google Scholar

Jakartapost.com. (2021). *Cyberattacks Crippling Indonesian SMEs: Study*. Google Scholar

Joseph Marks. (2021). *The Cybersecurity 202: The Government's Facing a Severe Shortage of Cyber Workers When It Needs Them the Most*. Google Scholar

Liputab6.com. (2021). *13,7 Juta UMKM Indonesia Telah Gunakan Platform Digital Untuk Berjualan*. Google Scholar

NIST. (2021). *NICE Framework Competencies : Assessing Learners for Cybersecurity Work*. Google Scholar

Prayoga, Fadel. (2020). Indonesia Jadi Target Pasar Ekonomi Digital Terbesar di Asia Tenggara. Google Scholar

Suhartadi, Imam. (2016). *Indonesia Kekurangan Bakat Cyber Security*. Google Scholar