Measurement of IT Risk Management Maturity Level in CEC Using IT Domain Risk Governance Framework

Annas Iswahyudi[1*]

[1]Graduate Student of Master Information Technology Program, Swiss German University, Tangerang 15143, Indonesia
*Corresponding author: annasipteknet@gmail.com

Abstract. IT Risk Management has long been adopted and implemented in CEC. This is inseparable from the high need for reliable and trusted information technology services at CEC as a government institution that has primary task for eradicating corruption. With a good IT risk management is expected to reduce the impact if the IT risk occurs and impacted to overall business process in CEC. However, up to 15 years after the implementation of IT risk management has never been measured how the level of IT maturity risk management. In this research, Author will use the IT Risk Framework with the risk governance domain approach as a standard IT risk management framework to evaluate the implementation of IT risk management in CEC. The process of evaluating the level of IT maturity is based on the maturity model that has been defined in the IT risk framework.

Keyword: IT Risk Management, IT maturity, risk governance domain

1. Introduction

CEC was established in 2002 to address against corruption in Indonesia. Become super body Institution, CEC has main duty to eradicate corruption as the extraordinary crime in Indonesia CEC was established to revitalize national anti-corruption efforts. CEC has adopted ISO / IEC, ISO / DIS 31000, Risk Management Standard since 2008 in the IT Department, which is reviewed annually by independent auditors (CEC Enterprise Architecture Review, 2014). In carrying out its role information technology risk management has been works very well because it is able to provide added value in order to achieve organizational goals, possible risks to technology information that can cause failure in running the information system function so that it can causing the impact of loss and reputation risk for the organization. IT Risk Framework provides a framework comprehensive to control and manage business based information Technology. Risk IT provides a framework to assist organizations in identifying, determine, and manage information technology risks. Therefore an analysis of risk management in CEC uses the risk domain IT Risk domain framework Governance.

2. Materials and Methods

2.1 Literature Study

2.1.1 Risk IT Framework

The IT Risk framework is used to help implementing information technology governance, and company which COBIT has adopted as a governance framework information technology used by Risk IT for improve risk management (Kulkarni, n.d.). Processes must be combined between internal interests and external organization. Internal matters include incidents in IT operations, failures in projects, and the replacement of an IT strategy. External things itself can include changes in circumstances that exist in the market, the existence of new technology and cause regulation on IT. IT risk itself can be said is a business risk where business risks cover in users, owners, ways operate, involvement, influence and adoption of IT in the organization (Alex Pasquini, 2013). The process model in the IT Risk framework has three the domain of Risk Evaluation (RE), Risk Governance (RG) and Risk Response (RR) as described in **Figure 1**

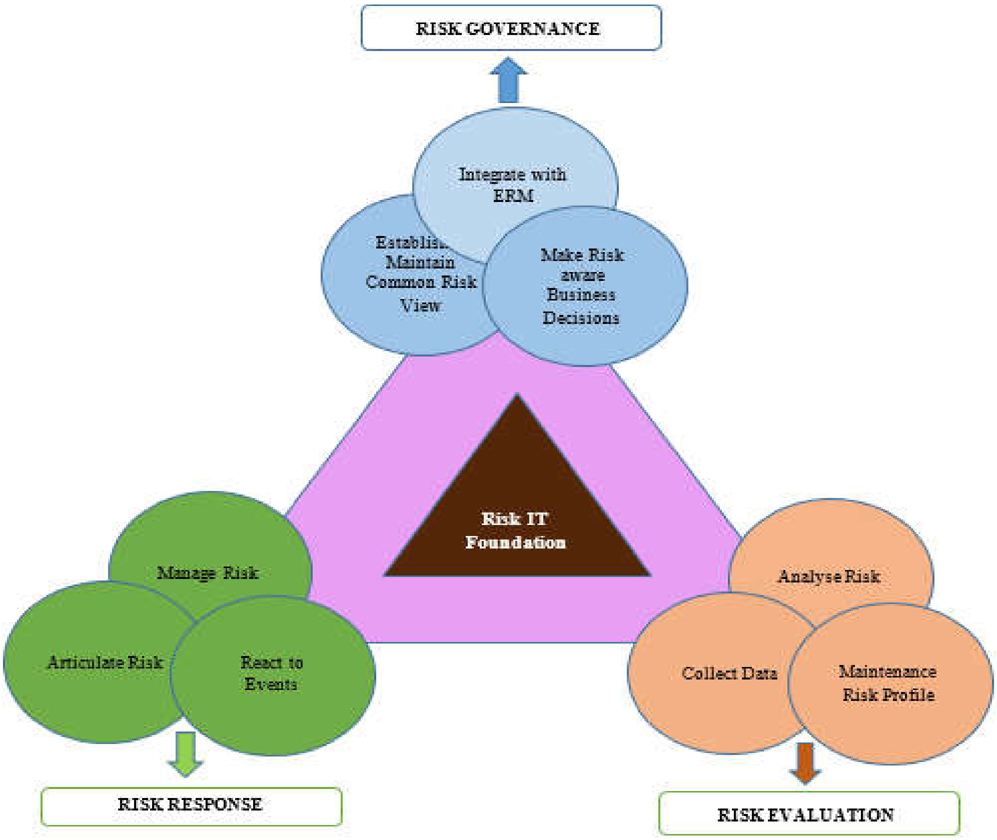

Figure 1. IT Risk Framework (Information Systems Audit and Control Association, 2009)

2.1.2 Risk Governance

At this stage, management practices must be ensured IT risks have been conveyed within the company, for allows for optimal risk adjustment. Risk Governance consists of three processes namely:

1. RG1 Establish and maintain a common risk view
2. RG2 Integrate with ERM
3. RG3 Make risk-aware business decisions

a. RG1 Establish and maintain a common risk view

Ensuring that risk management activities are aligned with the capacity of the company's goals relating to IT losses and leadership has a subjective tolerance for it. Following are the key activities of RG1:

- RG1.1 Perform enterprise IT risk assessment
- RG1.2 Propose IT risk tolerance thresholds
- RG1.3 Approve IT risk tolerance
- RG1.4 Align IT risk policy
- RG1.5 Promote IT risk-aware culture
- RG1.6 Encourage effective communication of IT risk

b. RG2 Integrate with ERM (enterprise risk management)

Integrate IT and operations risk strategies with business strategy risk decisions that have been made. Following are key activities RG2:

- RG2.1 Establish and maintain accountability for IT risk management
- RG2.2 Co-ordinate IT risk strategy and business risk strategy
- RG2.3 Adapt IT risk practices to enterprise risk practice

- RG2.4 Provide adequate resources for IT risk management
- RG2.5 Provide independent assurance over IT risk management

c. RG3 Make risk-aware business decisions

Ensuring that decision making by companies based on opportunities and consequences. Following are the key activities of RG3:

- RG3.1 Gain management buy-in for the IT risk analysis approach
- RG3.2 Approve IT risk analysis
- RG3.3 Embed IT risk considerations in strategic business decision making
- RG3.4 Accept IT risk
- RG3.5 Priorities IT risk response activities

2.1.3 The Risk Maturity Model

COBIT 5 is also designed to be a tool that can solve problems in IT governance in understanding and managing risks and the benefits associated with corporate information resources. In addition, COBIT 5 is also designed to be a tool that can solve problems in IT governance in understanding and managing risks and the benefits associated with corporate information resources. Therefore, a maturity model method is needed to measure the level of process management development, the extent of the management capability. How well development or management capabilities depend on achieving COBIT goals 5 (Arief and Wahab, 2016).

In this way, the maturity models are designed to enable management to focus on key areas needing attention, rather than on trying to get all processes stabilized at one level before moving to the next. The maturity model scales can help management understand where weaknesses exist and set targets for where they need to be (Behara and Palli, 2013) . The most suitable maturity level for an enterprise will be influenced by the enterprise's business objectives, the operating environment and industry practices (Nurpulaela, 2016). Specifically, the level of IT risk management maturity will depend on the enterprise's dependence on IT, its technological sophistication and, most important, the future role its executives and management foresee for information technology (Pasquini and Galiè, 2013). To create the results easily usable in management meetings—where they should be presented as a means to support the case for future plans to improve risk governance, evaluation and response, a graphical presentation model might need provided as follows in **Figure 2**:

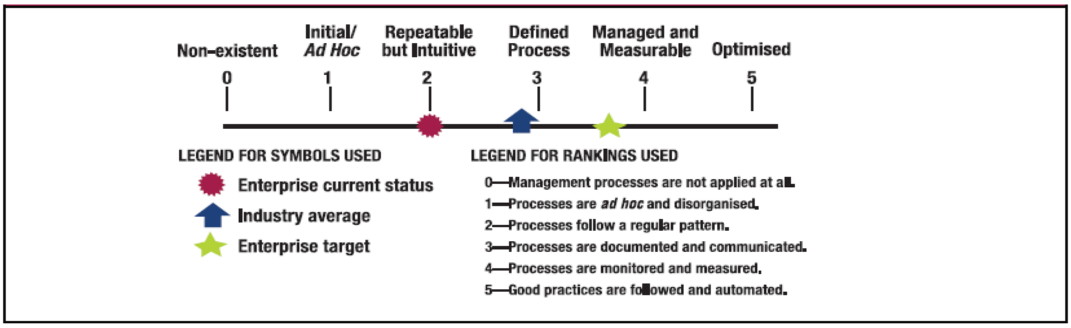
Non-existent
Initial/ Ad Hoc
Repeatable but Intuitive
Defined Process
Managed and Measurable
Optimised
0
1
2
3
4
5
LEGEND FOR SYMBOLS USED
Enterprise current status
Industry average
Enterprise target
LEGEND FOR RANKINGS USED
0—Management processes are not applied at all.
1—Processes are ad hoc and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

Figure 2. Maturity Model (ISACA, 2012)

There are five levels of application of risk management that can be defined in a series of models according to ISACA as shown in **Figure 2** above , including: 1. Initial: is the starting point for the use of a new or undocumented repetition process; 2. Repeatable: the process is at least adequately documented so that repeated attempts at the same steps can be carried out; 3. Defined: a process defined / confirmed as a standard business process; 4. Managed and Measurable: this process is managed quantitatively according to agreed metrics; 5. Optimized: process management includes intentional optimization / improvement of processes.

2.2 Methods

Analysis of the maturity level of IT risk management governance in CEC by collecting data through:

1. Observation
   Observations aims to understand the scope of the implementation of IT Risk management in related business processes with the CEC IT department.
2. Interview
   In this study, the objects and materials research are employees with 4 type of employee levels: a. middle management level is IT director or at same level, b. IT governance division head, c. IT risk officer and Staff. With various background level through the composite of different sources to get whole point of view, range of respondent are decided because various range consideration determined accuracy of result
3. Document review
   Documents collected are documents that related to IT risk management activities, i.e. IT risk management organizational structure, duties & authorities of the risk management division, IT Risk Register, Risk Profile and Appetite, IT risk policies and controls, guidelines the application of IT risk management. The documents used are limited to the last 3-year version (2014, 2015, 2016) of the document officially designated as a reference document.
4. Develop maturity assessment tool
   The rating scale used is 1 to 5. Results from these 6 variables are averaged to obtain the final score. The image above is an example of the tools developed in this research. After observation, interviews and document review, the process of measuring the maturity level of Risk Governance is carried out using a tool to determine the scores for each of the key activities. To assess key activities in the Risk Governance domain, a tool is used to conduct scoring using 6 (six) parameter as follows:
   1. Awareness & Communication: is the level of concern of all stakeholders about IT risks and how to communicate in treating these risks
   2. Responsibility & Accountability: is the adequacy of the division of tasks, responsibility and audit of each risk charged to each PIC (person in charge) that has been assigned
   3. Goal Setting & Measurement: Determination of the final destination and how to measure each risk control that has been set
   4. Policies, Standards & Procedures: the adequacy of policies, implementation standards and procedures for IT risks that have been determined
   5. Skills & Expertise: quality of human resource management and risk management
   6. Tools & Automation: Software, Hardware and other devices used to control IT risks

   See detail maturity assessment tool as shown in **Table 1** below:

Table 1. Maturity assessment tool

No.	Key Activities		Maturity Rank Model			Final Score
			Variabel 1	Variable 2	V3…n	
	Process Goals :					AVG(Score 1…n)
1	RG1.1	Perform enterprise IT risk assessment				Score 1
2	RG1.2	Propose IT risk tolerance tresholds				….
3	RG1.3….n					….
4	RG2.1….n					….
5	RG3.1….n					Score n

3. Results and Discussion

3.1 Resume of Result

Detailed scores for all key activities as shown in the following **Table 2**:

Table 2. Results score key activities

RG1	**3.21**
RG1.1	3.72
RG1.2	3.75
RG1.3	3.83
RG1.4	2.88
RG1.5	2.86
RG1.6	2.25
RG2	**2.99**
RG2.1	3.27
RG2.2	3.00
RG2.3	3.17
RG2.4	2.50
RG2.5	3.00
RG3	**3.00**
RG3.1	3.33
RG3.2	2.80
RG3.3	2.80
RG3.4	3.17
RG3.5	2.83
Average Risk Governance Score	**3.06**

The results in **Table 2** can be explained as follows.

a. RG1 Establish and maintain a common risk view

In this process the CEC already has risk management activities where there has been a workshop on existing IT risk assessment but it has not been followed by all areas in the CEC has also made risk tolerance and policies for IT risk at the CEC have also conducted training for related business units to raise awareness about risk, but for the IT risk discussion activity itself orally is explained to be done if the risk occurs at that time, there is no special planning carried out every periodically to discuss the risk. Existing program activities are still only followed by manager-level positions, not all parties related to the business.

The level of maturity of the RG1 process is Level 3 **Defined Process**, because there is already organizational awareness in discussing and communicating IT risks in the company but the risk tolerance discussed is still only based on technological developments, needs, and skills needed in the company today and there is no regular planning for communication activities that discuss IT risks at CEC.

b. RG2 Integrate with ERM (enterprise risk management)

In this process the CEC has specified responsibility for existing IT risk management in the organization and has considered the effect of IT risk on existing business strategies and has used methods to deal with existing risks using ISO27001, and has a monitoring website that monitors activities on the business, but the related business units do not have risk measurement documents that should be reported to those who handle risk management, namely the risk management division and good corporate governance, because at the time of the incident the related business unit can sometimes solve existing problems. For problems or events that occur also verbally explained is the responsibility of the parties concerned.

The level of maturity of the RG2 process is Level 3 **Defined Process**, because there is already a section that handles IT risk in the organization and the organization's risk management committee that provides risk management guidelines and resources to deal with IT risk but IT risk is still focused on existing risk issues the organization and the IT risk department are not yet fully engaged with the risk management committee in the Organization.

c. RG3 Make risk-aware business decisions

In this process the CEC has conducted trainings on the importance of IT risk analysis but has not been fully attended by all existing leaders and staff, the existing leader assigns tasks to the IT security and quality assurance department at the IT Directorate to consider risk activities. The maturity level of the RG3 process is Level 3 **Defined Process**, because the CEC has considered the effects of IT risks and determined the actions that must be taken in addressing IT risks but for discussion in conducting risk analysis it is still left to the IT department in the organization and consideration of existing risks still based on existing risk issues and only those that occur most frequently in the organization.

3.2 Gap Analysis

Table 3. Standard Deviation Risk Governance Domain

No.	Risk Governance Domain	Standard Deviation
1.	RG1. Establish and maintain a common risk view	0.591
2.	RG2. Integrate with ERM	0.265
3.	RG3. Make risk-aware business decisions	0.221

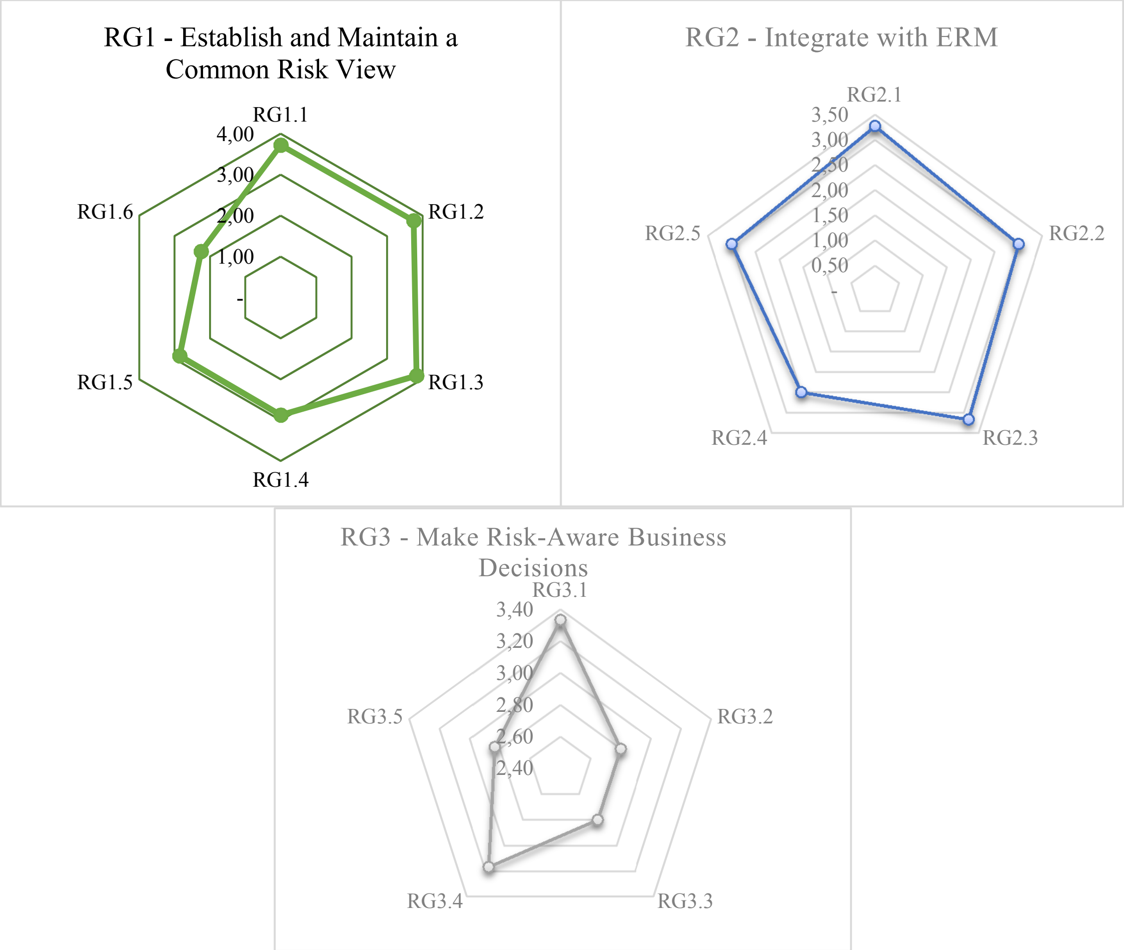

Figure 3. Curve radar comparison RG1, RG2, RG3

Using standard deviation calculations (see **Table 3**) and curve radar comparisons (see **Figure 3**) it can be seen the implementation gap between key activities in the domain of risk governance. From the table xx and xx figures it can be seen that the RG1 domain has the largest standard deviation of 0.591, while the RG3 domain has the smallest standard deviation of 0.221. This indicates that the key activities in RG1 do not yet have an even distribution of maturity values or have a large gap between the high measurement value and the lowest value. Conversely, in RG3 the distribution of key activity measurement values has a low gap. The lowest value in RG1 is key activities RG1.6 Encourage effective communication of IT risk with a score of 2.25. While the highest score is RG1.3 Approve IT risk tolerance with a score of 23.83.

4. Conclusion

From results and analysis above we conclude that:

1. Based on the results of measurements on IT risk management in CEC using the IT Risk Framework, especially for the domain of Risk Governance, the answers are obtained from the problem formulation that the maturity level of the RG1 Establish and Maintain a Common Risk View, RG2 Integrate With ERM and RG3 Make Risk-aware Business Decisions are level **3 Defined Process.** Level 3 is still in line with the average level in industry or organization best practices that adopt IT risk management.
2. All CEC stakeholders, especially leaders and officials in the IT department need to improve the management process of several key activities that still exist in level 2 and increase even higher levels that already exist in 3 so that in the future it is expected to be at the managed and measurable level (level 4) even if possible achieved at Optimized (level 5). This is necessary considering that CEC is an institution that has a very important task in this country and has a good reputation so IT risk management must be as much as possible.

References

Alex Pasquini, 2013. COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process.

Arief, A., Wahab, I.H.A., 2016. Information technology audit for management evaluation using COBIT and IT security (Case study on Dishubkominfo of North Maluku Provincial Government, Indonesia), in: Information Technology, Computer, and Electrical Engineering (ICITACEE), 2016 3rd International Conference On. IEEE, pp. 388–392.

Behara, G.K., Palli, P., 2013. Maturity Assessment for Enterprise Architecture.

CEC Enterprise Architecture Review 2014-2016.

Information Systems Audit and Control Association, 2009. The risk IT framework. ISACA, Rolling Meadows, IL.

ISACA, 2012. COBIT5-Implementation.

Kulkarni, G., n.d. Applying the Goals Cascade to the COBIT 5 Principle Meeting Stakeholder Needs 10.

Nurpulaela, L., 2016. Evaluation of IT governance to support IT operation excellent based on COBIT 4.1 at the PT Timah Tbk, in: Information Technology, Computer, and Electrical Engineering (ICITACEE), 2016 3rd International Conference On. IEEE, pp. 336–339.

Pasquini, A., Galiè, E., 2013. COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process. Proc. FIKUSZ 13, 67–76.