Atlantis Highlights in Engineering (AHE), volume 2
International Conference on Industrial Enterprise and System Engineering (IcoIESE 2018)

Application of Risk IT Based on ISO 31000 Standards Process Capability Assessment Model Case Study : Andalas University

Mohammad Hafiz Hersyah[1], Kridanto Surendro[2]

1 Computer System Department, Information Technology Faculty, Andalas University
[2]School of Eectrical and Infromatics Engineering, Bandung Institute of Technology, ITB
Indonesia
mhafiz@fti.unand.ac.id

Abstract*— The fact given that capability function is to aim executed things works properly and effectively in organization business process could not running well without considering risk management aspects. Risk management overlay every event possibilities that able to either to hinder or accelerate organization business process in fullfilling organization's business objectives. In this thesis research, is presented with a proposed two dimensional conceptual mapping between capability dimension from ISO 15504 and risk management model from ISO 31000, where ISO 31000 model is adapted into application of risk IT process using COBIT 4.1 as a reference.

Keywords— ***ISO 15504* ; ISO 31000; Manajemen Risiko, Dimensi Kapabilitas, COBIT 4.1**

I. INTRODUCTION

Nowadays, risk management is considered as the main tool to reduce the risk of failure. At the moment where an organization could able to conduct prediction regarding something matter in the future, risk management can be adopted to find defect that placed in planning and executing direction to reduce the possibilities and effect that potentially will happen. Risk management means having executed preventive actions before the crisis taking place, that could increase the success possibilities and reduce the consequences from unavoidable risk. [1].

In the last decade, information technology (IT) has becoming one from the strongest factors in forming process and services on an organization. IT Capability has become either strategic and also operational in an organization. Fail to understanding, indentifying and managing risks often be as a main cause form IT matter. At the tome where IT projects has turn into analysis level in most of research regarding risk management, IT itself has becoming more realistic in the form of infrastructure, and because of that, there is a requirement of an ability to adapt IT risk strategies much more than IT project level strategies. [2] On reality also often found that the organization's commitment in form of the respond against IT risk are not yet perfect. There are bigger possibilities that the organization is running standard procedure such as *back up* to sore data much more than having a successful IT project. Project which possibly require a lot of fund and well managed organization's data is not automatically become most valuable and critical asset for organization. The risk in project selection is also high. The top management also seldom be equipped with good information to create decisions regarding this matter. IT has becoming an important part in organization's daily routine but the real problem occur when organization are not fully prepared to accept troubles which one of them is IT risk that able to occur anytime [2].

To be able to get IT risk well managed in an organization, as the first step, there are many methods that able to adapt to see whether an organization already take a good care its IT risk effectively in understanding, indetitying and managing IT risk that can be happened everytime, one of them is to applied ISO 31000 risk management standard which its capability level is being measured by using ISO 15504 standard. A high duration organization's environment such as academic institution also often characterized with product and service that able to e reviewed with an IT risk perceptive. In this case study, Andalas University (Unand) is being choosed as the analyzed institution. There is an immediate study regarding the ability of application of IT risk on current Unand organization body to assess and reflect the current state and promoting the improvement actions on the application of IT risk based on ISO 31000 standard.

The main problems that become focuss on this reserach are :

a. **What are the process from the application of IT risk on Unand that need to be assessed using ISO 31000 standard ?**
b. **How is the applied capability level design and the scale of capability measurement that can be eligble in assessment model ?**
c. **How is the form of the capability process assessment set in assessing the process of the Unand's application of IT risk and the proposed of application IT risk framework ?**

II. LIETRATURE REVIEW

The used literature review on this research are :

A. ISO 31000

On ISO 31000 standard, the risk management life cycle is diviede into three major parts [3]:

a. Principle
b. Framework
c. Process

Being described on the following illustration :

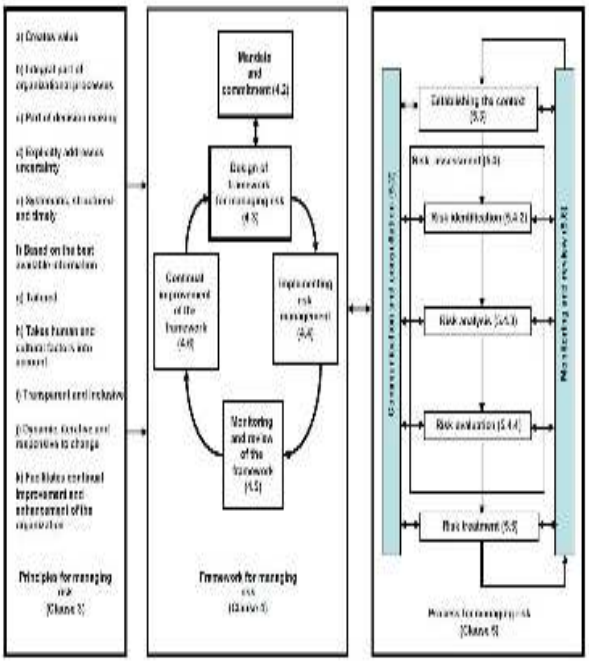

Fig 1 :ISO 31000 Risk Management Model

B. ISO/IEC 15504

On ISO/IEC 15504-4 documentation, Pada dokumentasi ISO/IEC 15504-2[4], define a measurement framework that provide a basis to conduct rating from capability process, based on the achievement from the attribute process that has been define. This documentation also define requirements to conducting an assessment and expressing a state where the assessment result is able to be compared.

Capability dimension depict the capability process measurement that relevant with the current organization's goals and future plans. Capability is being described with its relation against the process attributes that being grouped in capability levels. The levels of capability is determined based on the achievement of spesific process attribute that being assessed correspondingly with ISO 15505-2.

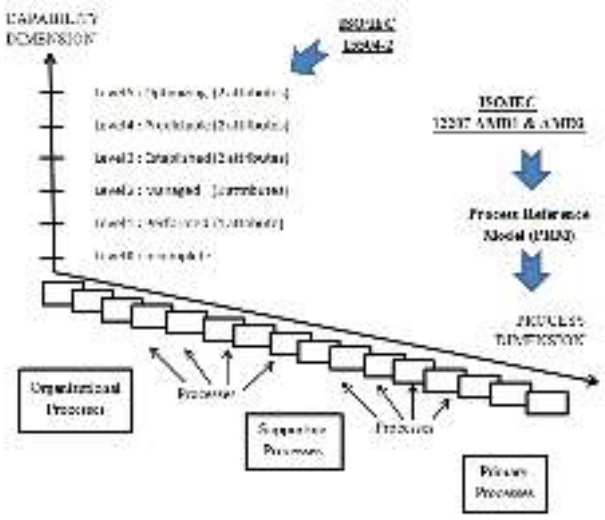

Fig 2 : Relationship between process refernce model and input

C. COBIT 4.1 PAM (Process Assessment Model)

COBIT 4.1 PAM is being designed based on COBIT 4.1 dan ISO/IEC 15504. Developed to placing requirements for a process assessment based on COBIT to increase the accuracy and robustness from IT process review. COBIT 4.1 PAM is a guidance that contain process assessment indicator and its output from 34 process on COBIT 4.1.(IT Governance Institute, 2011). PAM is build by using the ISO/IEC 15504 scale. On PAM, there are six process capability levels and nine process attribute. The process capability levels are :

0. *Incomplete Process :* The exsisting process is not yet being implemented or fail to achieve its process purpose. On this level, is being mark with a little or even no proves from sistematic achievemnt from process purpose.
1. *Perfomed Process :* The exsisting process is being implemented and able to fullfill its purpose.
2. *Managed Process :* The process that has been explained on previous level on this stage are being implemented on more manage fashion (planned, monitored, adjusted) and *work* product are relevantly established, controlled and maintained.
3. *Established Process:* The process achievement that has been explained before on this stage are being implemented by using a well defined process that able to achieve its desired process effect.
4. *Predictable Process :* The process achievement that has been achieved previously on this stage are being operated in define scope to obtain the effect of the process.
5. *Optimzing Process :* The achievement process that has been grabbed before on this stage continously improved to achieve the current business purpose and projected business purpose.

Nine process attributes that will become the assessment object on COBIT 4.1 PAM are :

0. Process Performance
1. Performance Management
2. Work Product Management
3. Process Definition
4. Process Deployment
5. Process Measurement
6. Proses Control
7. Process Innovation
8. Continous Optimization

Assessment indicators are being used to assess whether the process attribute has been achieved or not. There are two types from assessment indicator that are :

1. Capability Process Indicator. Is being applied on capability level 1 through 5.
2. Performance Process Indicator, only applied exslusively on capability level 1.

Performance process indicator(*Base Practice* dan *Work Product*) is a spesific for each process and being used to determine whether a process is on the capability level 1. On the other hand, capability process indicator is a generic for each process attribute for capability level 1 through 5. Being depict on illustration 3 [5].

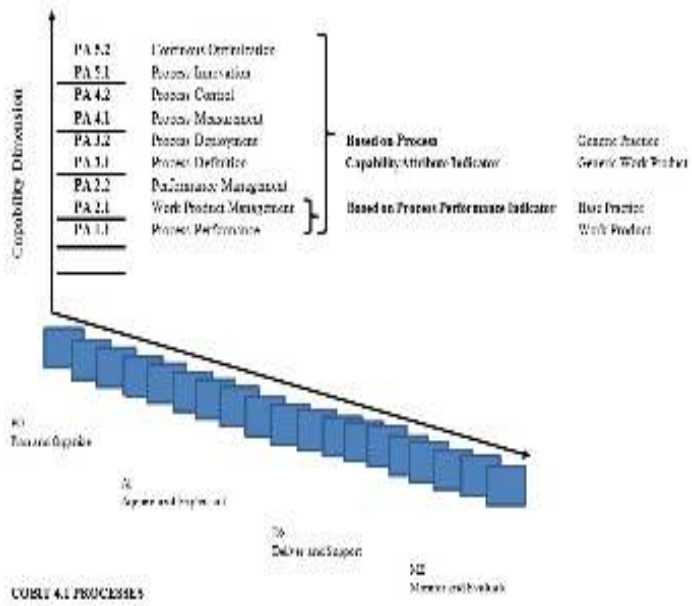

Fig 3 : Assessment Indicator (COBIT 4.1 PAM)

III. ANALYSIS AND DESIGN

On this chapter will explained regarding the adaptation of ISO 31000 risk management model into application of IT risk process with identifying the process and its derivative and alsi the measurement instrument of application of IT risk ISO 31000.

A. Adaptation ISO 31000 Model into Process

On the early stage of the proposed application of IT risk, is being held adaptation of ISO 31000 model into the proposed application of IT risk process by considering the relationship between ISO 31000 model, where principles of ISO 31000 risk management as the inisiation stage in form of commitment from top management that being translated into framework and process on ISO 31000.

The adaptation is continued by referencing to four domain of COBIT 4.1,that are :

1. *Plan and Organize (PO)*
2. *Acquire and Implement (AI)*
3. *Deliver and Support (DS)*
4. *Monitor and Evaluate (ME)*

As the basic reference to obtain proposed process that consists of :

1. Planning
2. Design
3. Operate
4. Evaluation

Where planning gives input on desin process regarding early inisiation of application of IT risk. The next step is the design process gives input in the form of design and framework implementation on operate process and on the last stage, evaluation is taking place regarding the overall process of the application of IT risk by giving feedback to each process as being depicted on illustration 4.

Fig 4. ISO 31000 adaptation into application of IT risk

B. *Process capability level mapping*

The mapping result between capability dimension and process dimension will be joined into a capability assessment process model of application of IT risk in illustration 5.

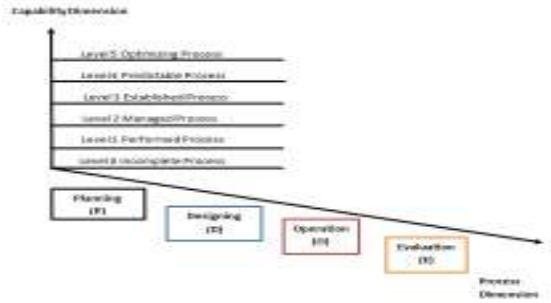

Fig 5. The proposed application of IT risk capability process assessment.

On illustration 5, the process dimension of the application of IT risk which divided into four process that are : planning (P), Designing (D), Operates (O) and evaluate (E) will posess it own *base* practice on each activities and producing *work* in the form of proves or artefak that able to become reference to other activities component either in the same process or even different, being mapped against the capability dimension assessment scales to assess the current level of capability and to promote regarding improvement of the capability level of the application of IT risk in the future.

IV. IMPLEMENTATION

On this chapter will discuss regarding the implementation of application of IT risk standard ISO 31000 process capability assessment with observing at the current condition (as is) and to do recommended improvement of capability level.

A. *The result of capability process assessement*

The result of assessment scale from *base practice* and *work product* which being tested on three different kind types of respodent. The result that be obatined is the lowest scale from the assessment scale detail of *base practice* and *work product*. Based on the level 1 assessment result of the application od IT risk, as being explained on table 1.

Table I Final recapitulation capability assessment level 1

Type of Respondent	List of Respondent	Level 1 Capability Assessment Scale	
		Base Practice	*Work Product*
University	Responden 1	L	L
	Responden 2	L	L
Faculty	Responden 3	L	L
	Responden 4	L	L
	Responden 5	F	F
	Responden 6	P	P
	Responden 7	P	P
	Responden 8	L	L
	Responden 9	L	L
Foundation	Responden 10	P	P
	Responden 11	P	L
Result		**P**	

Based on the result of level 1 capability level of application of IT risk, shown that not all of the component on faculty and foundation has translated the standarized activity of *base practice* and the prove of *work product* that come from the sequence of application of IT risk standard ISO 31000 that consist of three major group that are principle, framework and process. This matter has been prove with there are still several faculty and foundation that achieve the final score of P (*Partially Achieved),* which is mean the activities on *base practice* and *work product* that been produced still having low percentage scale that positioned between 15 until 50%. While other faculty are haveng the final result of L (*largely achieved)* which mean that the *base practice* and *work product* that produced already in the percentage scale between 50 until 85%.

The assessment could not be continued to the next level because of based on the final result, the application of IT risk process at Unand still on the level of zero. Aside from that, the final result still cant fullfill the requirement from the capability assessment level 1 due to less activities on *base practice* and *work product* that correspond as the proves of the activities that has been done to be called occupying the F scale (> 85% - 100%).

B. *The proposed of improvement of capability process level*

The assessment of application of IT risk on this research is a personal innisiative to find out the current state (as is) regarding the capability process level of application of IT risk on Unand. The result that obtained from the process assessment can be used as an input for Unand itself in managing and improving the application of IT risk process.

The proposed step of improvement regarding capability process level of application of IT risk is a suggestion improvement of capability level from 1 through 5. The general description can be viewed on illustration 6.

Fig 6 General description of the proposed improvement of capability process level

V. CONCLUSION

The conclusion that can be obtain from the research are, Application of IT risk based on ISO 31000 standard Process capability assessment model that has been produced on this research is refer to the rule that has been inferred on ISO 15504 and consist of two dimension that are capability dimension and the measured process dimension. On this reserach, already produced the assessment set start from the first level up to the fifth level of capability dimension of application of IT risk process at Unand.

Process dimension that will be measured consist of twelve process that being scattered into fout steps that are planning (P), Designing (D), Operates (O) and evaluate (E). Unand still postioned on the level of 0 on capability of application of IT risk process. This final result mean that there are unsufficient *base practice* and *work product* that has been executed and produced at Unand.

Base on the final result of the quesioner on the first level capability of application of IT risk, can be concluded that the IT risk still not yet being priority and still not yet being applied at Unand.

REFERENCES

[1] Liu Guling dan Zhang Xiaojuan (2011) : Research on the Risk Management of IT Project, International Conference on E-Business and E-Goverment, China.
[2] Jordan, Enrie dkk (2005) : Beating IT Risk, John Wiley & Sons, US.
[3] BS ISO 31000 : 2009 : Risk Management – Principles and Management., UK
[4] PD ISO/IEC TR 15504-2 (2003) : Information technology - Process assessment Part 2: Performing and Assessment. Switzerland.
[5] IT Governance Institute (2007) : COBIT Assessment Process (CAP) : Cobit 4.1 Process Assessment Model., US