Development of IT Risk Management Framework Using COBIT 4.1, Implementation In IT Governance For Support Business Strategy

Jarot S. Suroso
Bina Nusantara University
Jln. Kebon Jeruk Raya No. 27 Jakarta
Indonesia
jsembodo@binus.edu

Bayu Rahadi
Bina Nusantara University
Jln. Kebon Jeruk Raya No. 27 Jakarta
Indonesia
bayurahadi@live.com

ABSTRACT
Extensive use of information technology in companies put IT into a position which is of considerableconcern, especially in large companies that put IT becomes a strategic part of the company. The importanceof IT division, make the companies willing to pay big to get the benefits offered by IT itself, but on the otherhand appears disappointment incurred from investments are not comparable with the results obtained. Untilthe threat appear and disrupt the business of the company. By doing risk management using the IT risk management framework by Cobit 4.1, the combining between business strategy Goals and IT Goals can assist companies in identifying risks that might occur and Companies can design how to mitigate if risks occur. IT governance should be able to support the company's business strategy by managing and memange risks in order to avoid large financial losses to the company due to the lack of identifying and analyzing risks in the company.

CCS Concepts
• Information systems → Information systems applications → Enterprise information systems → Enterprise applications.

Keywords
Risk Management; Cobit 4.1; IT Risk Management Framework; Business Strategy; IT Governance.

1. INTRODUCTION
Extensive use of information technology in companies puts IT into a position which is of considerable concern, especially in large companies that puts IT into a strategic part of the company. Once the importance of IT, companies are willing to pay big to get the benefits offered by IT[1]. However, on the other hand, it appears disappointment incurred from investments that are not compatible with the results obtained. Top management has always wanted an investment that must be issued in accordance with the benefits, regardless of the risks, threats, and weaknesses in the company. Especially on things that are the responsibility of the IT division, which sometimes it is not realized, it will affect the performance of the company's business either directly or indirectly[2].

IT Governance will put the structure around how organizations align IT strategy with business strategy, and then make sure that companies stay on track to achieve their strategies conduct risk management for IT governance, risk identification and risk analysis used to determine the type of risk and the magnitude of the risk if it occurs.

The main objective of IT governance is to ensure that IT investments to support business strategies, but on the other hand can mitigate risks from its use. IT governance or governance of information technology (IT) is a part of corporate governance that focuses on the management of IT in the organization, including IT system performance and risk management. IT governance is the application of governance mechanisms: structure, roles, processes / procedures, and relational mechanisms to ensure that IT is managed in accordance with the needs and strategy of the organization[3].

XYZ is a life insurance company and of course the risk is important, companies should consider the possibility that the risk will occur which can degrade the performance of the company in case of problems in IT, which is currently IT is already used as the company's business strategy. Currently the governance of IT in PT XYZ is not align with Enterprise Risk Management, because it has not had a framework standards, IT governance and ERM still follow the rules of the regional, so the need for a framework that can help companies especially in IT governance to establish IT governance based analysis a strong risk, so that IT organizations can support the company's business strategy.

The company uses COBIT (Control Objectives for Information and Related Technology) version 4.1 for IT governance. COBIT provides a clear policy and good practice for IT governance, assisting senior management in understanding and managing the risks associated with IT. It provides the framework and control objectives detailed instructions to management, business process owners, users and auditors. It defines IT activities in a generic process model within four domains. It contains Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. They map to IT's traditional responsibility areas of plan, build, run and also monitor[4].

ICEMT '17, July 9–11, 2017, Singapore, Singapore

ACM ISBN 978-1-4503-5293-2/17/07…$15.00
https://doi.org/10.1145/3124116.3124134

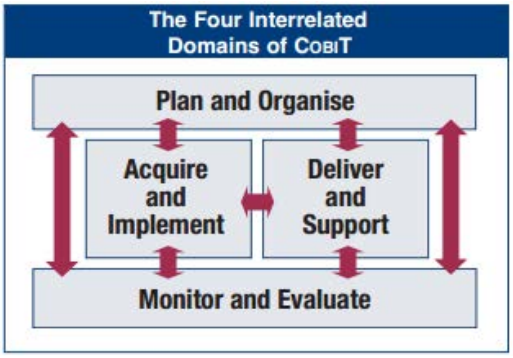


Figure 1. Four Domain of Cobit 4.1

The problems which are summarized in this study include two things. First, how the business dependence on IT, second, how is the implementation of IT Risk Management at PT xyz, third, how effective business strategy that is supported by the implementation of good IT Governance. The study contains theoretical basis related to IT risk management in the implementation of information technology by utilizing the COBIT 4.1 framework.

2. LITERATURE REVIEW

IT Governance is part of the management company and composed of the leaders, all members of the organizational structure and processes - processes yangmempunyai a view to ensuring that existing IT support and then help in achieving the organization's strategies and also its objectives[5].

COBIT has been developed by the IT Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA). COBIT is a set of documentation of best practices for the governance of IT that can help auditors, management and the user to bridge the gap between business risks, control needs technical issues. COBIT framework as we know, consists of 34 high-level control objectives and grouped into four domains, four domains are: Planning and Organization (10 processes), Acquisitionand Implementation (7 processes), Delivery and Support (13 processes), Monitoring and Evaluation (4 process).

Risk IT is a framework that based on a set of guiding principles for the effective IT Risk Management. Complement COBIT Framework, a comprehensive framework for the governance and control of IT-based business solutions and services[6].

Figure 2. Risk Hierarchy

Figure 3 is the risk it framework issued consists of three domains : risk governance, risk response and risk evaluation.
IT Risk Management is a framework based on a set of guiding principles for effective IT risk management. The framework complements COBIT, a comprehensive framework for the governance and control of business-driven, IT-based solutions and services[7].

IS strategy related to what should be done with the information, systems and technology, and how to manage applications from a business standpoint. IS strategy related to what should be done with the information, systems and technology, and how to manage applications from a business standpoint (Figure 4) [8].

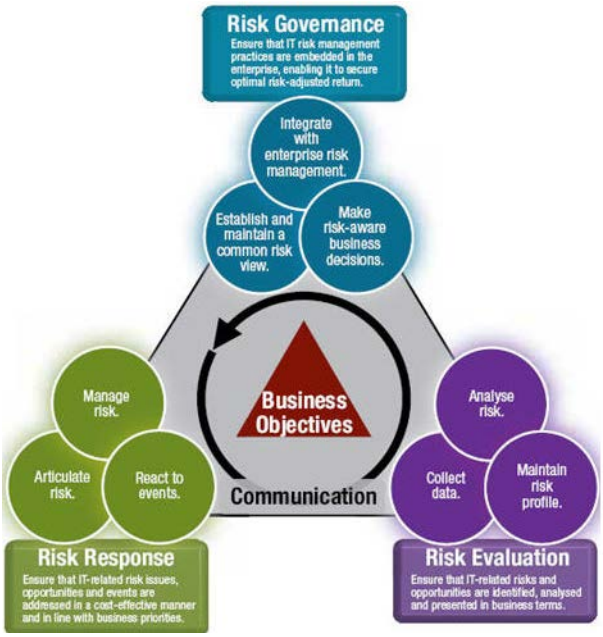


Figure 3. IT Risk Framework

3. METHOD

3.1 Methodology

The methodology used in the writing of this case study, the end result will be given on the application form of IT Risk Management by using COBIT 4.1 to endorse the company's business strategy. Here is a schematic framework of thinking that is used in case study research in PT XYZ. The study was conducted by interview and observation. Interviews were conducted to the managerial IT regarding the company's business processes and risk management[9].

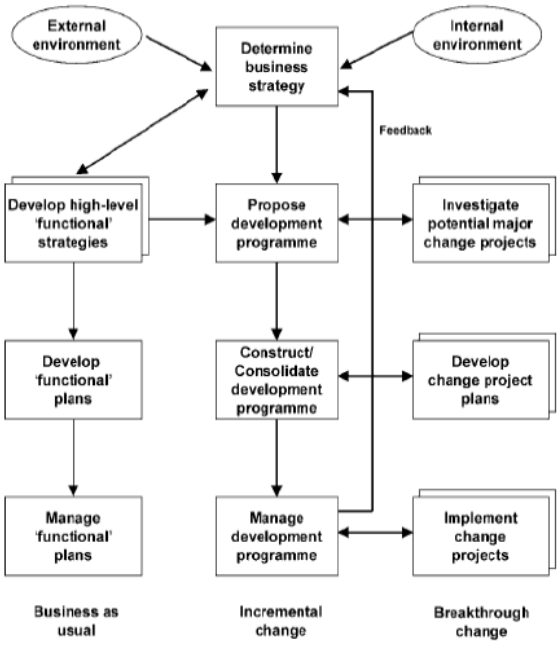


Figure 4. Integrated Business Strategy Framework.

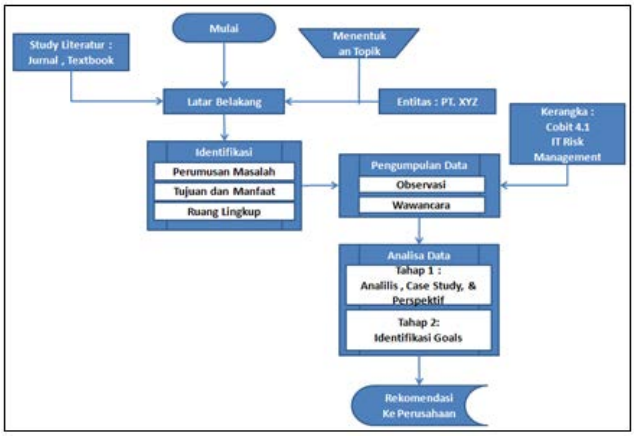


Figure 5. Methodology

The issues to be researched, authors collected data relating to ongoing business processes, control has been done, and best practices in the company that is PT.XYZ. The collected data was collected based on interviews, observations, and supporting data obtained from the original company. and in the analysis based on the COBIT 4.1 framework and IT Risk Management[10].

The above picture is the mind map in this case study, linking business strategy with IT governance is then connected also with IT risk management framework that the result is to give recommendations to XYZ about IT risk management framwork by COBIT[11].

3.2 Mindmap

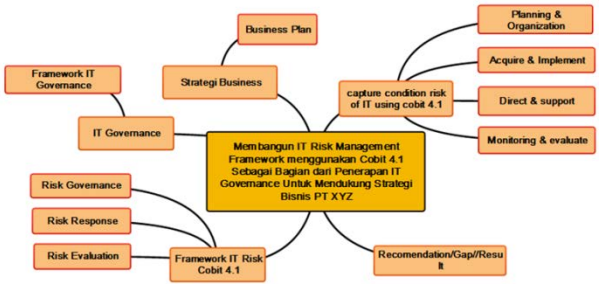


Figure 6. Mind Map

4. RESULT AND DICUSSION

First we will describe comparison among risk management, octave, fair dan NIST. Risk management of IT within COBIT is a framework that is based on a set of guiding principles for the effective management of IT risk. Complement COBIT Framework, a comprehensive framework for the governance and control of IT-based business solutions and services[12].

The Factor Analysis of Information Risk (FAIR), these methods apply: (i) a classification of risk factors to compile information; (Ii) a method to measure the factors that increase the risk of information, including the frequency of occurrence of threats, vulnerabilities and disadvantages. This methodology consists of four components: threats, assets, organization and external environment. Thus, the scenario assessment is classified into one category or the factors that have contributed positively or negatively to the risk[13].

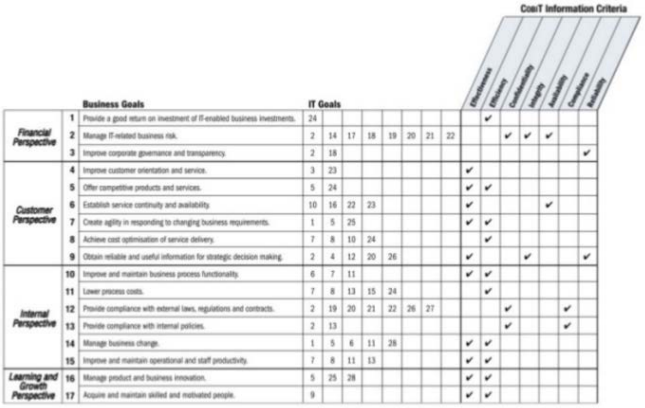
The Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Allegro is a methodology to streamline and optimize the process of assessing information security risks so that the organization can obtain enough results with the investment of time pliers short, people and resources are limited in relation to the information, services and business process. This methodology differs from other approaches because its main focus is on asset information is used, in which information is stored, transported and processed, and how the information has an impact on threats, vulnerabilities and disruptions[14].

The National Institute of Standards and Technology (NIST), aims to provide guidance in assessing risks to information systems. This method provides guidelines for conducting the risk assessment process step by step, starting from the preparation of the evaluation, risk assessment, reporting the results of the evaluation and maintenance in the review and how the risk assessment as well as other complementary processes provide each other with each other[15].

Table 1. Comparison in IT Risk Management methods

Attribute, characteristic	Octave	Fair	NIST	IT Risk COBIT
Focus	Assement dan risk majemen	Risk assess ment	Not applicable	Risk governance, evaluation and response
Identification risk	Medium	Mediu m	High	High
Risk Analysis	Medium	High	Hiht	High

In this study conducted a risk assessment in accordance with IT risk management framework and based on the data-data that have been obtained from the interview. Before performing the risk assessment information system, the first thing to do is to define the company's business goals and objectives of IT to do an interview to the parties concerned, namely Head of IT Department, Head of IT Governance, IT Risk Management, IT Security, IT Compliance, IT Policy and procedure IT BA, IT Developement, IT Services, IT infastructure. Interviews were conducted to determine the business strategy and IT strategy, then do the assessment of the risks that might occur by searching the risk impact, critical information assets of IT and business, container risk, the risk that potentially occur (area of concern) and the consequences of those risks.



Companies are already having an especially IT procedures service level agreement (SLA) that are listed in the document. The management should be communicated effectively to all stakeholders. IT departments in this regard has been made SLA on any problems and always strive to maintain the quality of service of each of its service.

Figure 7. Service Level Agreement [16]

Automated tools and techniques with the knowledge base already done centralized. Each helpdesk staff can interact so that the solution can be done quickly. Responsible for the team was also able to clearly monitor effectively[17]. The procedure for communicating to resolve incidents are defined and communicated by implementing Help Desk System.

Type	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Incident	6	8	8	48	74	378	1279	1688	1429	1539	1362	1404	9223
Service Request	0	0	0	0	0	0	0	563	1177	1532	2566	2106	7944

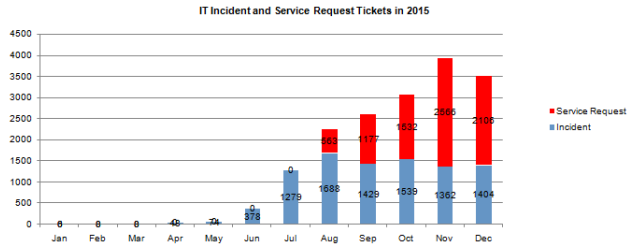


Figure 8. IT Incident and Ticketing System

There is now a special section that handles the incident so that the existing problems can soon look for a solution and looks already implemented and tried to consistently implement effective problem management, where each issue received identified the root cause and then formulated to address the problem.

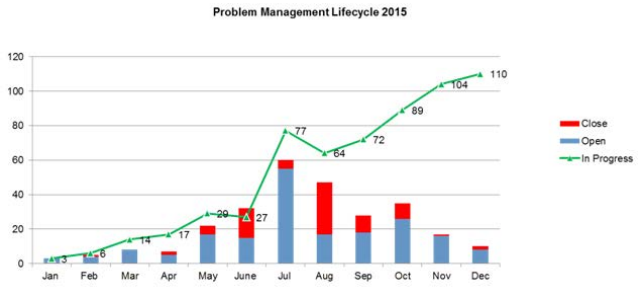


Figure 9. Problem Management Lifecycle

Every project that has been implemented will be monitoring, monitoring in detail about what needs to be repaired or to be evaluated for the system to support the company. Currently the IT performance monitoring and evaluation has been carried out properly, so the entire system can be managed properly

ALL YEAR INCIDENT 2015						
	P1	P2	P3	P4	P5	SLA Breached
Jan	3	3				1
Feb	6	2				0
Mar	3	5				2
Apr	1	4	14	24	5	8
May	0	3	22	23	26	3
Jun	2	2	32	145	197	8
Jul	0	9	25	38	1207	173
Aug	0	7	71	33	1577	117
Sept	0	9	50	18	1352	57
Oct	0	7	54	29	1449	75
Nov	0	6	40	31	1290	105
Dec	1	5	54	35	1309	79

ALL YEAR Service Request 2015						
	P1	P2	P3	P4	P5	SLA Breached
Jan						
Feb						
Mar						
Apr						
May						
Jun						
Jul						
Aug	0	0	2	2	559	22
Sept	0	0	35	0	1142	55
Oct	4	10	14	0	1504	68
Nov	2	11	21	6	2526	78
Dec	2	3	12	3	2086	29

Figure 10. Monitoring system.

5. CONCLUSIONS

According to the previous explanation, it can be summed up as follows:

1. Standard IT Governance using COBIT, results of mapping between the existing process showed that there are 21domain COBIT that can be mapped into

the business and IT Goals to harmonize between business strategy with IT strategy.

2. Risk communication has been defined based on the framework by mapping each stakeholder into the COBIT 4.1 framework of risk communication.

Goals of key risk activity already are managed and grouped based on the criteria of IT risk management to monitor, evaluate and manage risk. (RG, RE and RR).

6. REFERENCES

[1] Alberts, C., & Dorofee, A. (2003). Introduction to the OCTAVE Approach. … , *PA*, *Carnegie Mellon* …, (August), 1–37.

[2] Alberts, C. J., & Dorofee, a J. (2002). Managing Information Security Risks: The OCTAVE Approach.

[3] Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process, (May), 154.

[4] Haes, S. De. (2006). Information Technology Governance Best Practices in Belgian Organisations, *00*(C), 1–9.

[5] ISACA. (2007). CoBIT 4.1. *IT Governance Institute*, 1–29.

[6] ISACA. (2013). COBIT ® Process Assessment Model (PAM): Using COBIT ® 5.

[7] Jordan, E., & Silcock, L. (2005). Beating IT Risks, 292.

[8] Kouns, J., & Minoli, D. (2010). Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and A Practical Guide to Risk Management Teams.

[9] Larsen, M. H., Pedersen, M. K., & Andersen, K. V. (2006). IT Governance: Reviewing 17 IT Governance tools and analysing the case of Novozymes A/S. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *8*(C), 1–11. http://doi.org/10.1109/HICSS.2006.234

[10] Laudon, K., & Laudon, J. P. (2013). *Management Information Systems, Global Edition*. http://doi.org/0-273-78997-X

[11] Mechanism, I. T. G. (2008). C OBI T as an IT Governance Mechanism, 1–32.

[12] Mintzberg, H. (1987). the Strategy Concept .1. 5 Ps for Strategy. *California Management Review*, *30*, 11–24.

[13] Neely, M. P. (2008). Accounting Information Systems: A Business Process Approach, Second Edition. *Issues in Accounting Education*, *23*(3), 495–496.

[14] Planas, E., Ronza, A., & Casal, J. (2004). *The Risk IT Framework*.

[15] Turban, E., McLean, E., & Wetherbe, J. (2001). Information Technology for Management. *Improving Quality and Productivity*.

[16] Van Grembergen, W. (2003). Strategies for Information Technology Governance.

[17] Ward, J. L., & Peppard, J. (2002). *Strategic planning for information systems* (Vol. 28).