Risk Management In Protecting Banking Sensitive Information at XYZ Bank Using COBIT5 Framework

Maulid Ibnu Adhi Purwoko[1]

[1]Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Article Information

Received:
Accepted:
Published:
DOI: 10.33555/ejaict.v…

Corresponding Author:

FirstName LastName
Email: email address

ISSN 2355-1771

ABSTRACT

POJK No.18 / POJK.03 / 2016 concerning the Implementation of Risk Management for Commercial Banks is addressed to the management and board of directors of Banks to improve provisions regarding compromised customer information disclosure to the public, and breaches of customer information have led to the need for risk management practices in the use of Information Technology (IT). Risk Control Assessment (RCA) is based on the COBIT 5 framework to assess risks associated with the use of Information Technology Asset in XYZ Bank. By mapping the RCA and the provisions of POJK No.18 / POJK.03 / 2016, it can help management obtain information on the level of compliance of the Bank with provisions relating to Banking sensitive information.

Keywords: *POJK, Risk Control Assessment, Banking Sensitive Information.*

1. Introduction

Bank XYZ is among the 10 largest banks in Indonesia, with assets of more than 160 trillion rupiah. As a bank that is transforming into a digital bank, various types of digital services for various lines of business segments are presented with various kinds of technological innovations by building digital infrastructure as a support. The application of technology plays an important role in the collection and processing of data and / or information, its availability for the right person / user in the right format and at the right time which can support business decisions and strategic thinking. And with this initiative, XYZ Bank management realizes the risks involved in every innovation presented to its customers. And with this initiative, XYZ Bank management realizes the risks involved in every innovation presented to its customers.

Risk is considered as something that might go wrong in an establishing process and also a combination of the likelihood of an event and its effects. There are three categories of risks on the enterprise which is projects risks, product risks and business risks [1]. The need for an effective framework in managing these risks, especially in safeguarding sensitive bank information. Hence the organization must learn to stabilize the possible negative effects of risk against the possible gains of its related opportunity.

In Indonesia, the Financial Services Authority (OJK) has regulated matters relating to risk management related to the use of information technology at commercial banks in POJK No.18 / POJK.03 / 2016. Therefore, it becomes a guide for Banks in managing Information Technology in the aspects of risk management. Thus, Banking Industry needs a comprehensive framework covering all aspects of risk management due to various reasons such as the need to create appropriate internal controls, and prevent issues related to software errors and sensitive data exsposure [2]. Control Objectives for Information and Related Technology (COBIT), a comprehensive framework for IT governance and risk measurement in an organization. COBIT can provide standard practices that can assist organizations in implementing various processes and procedures in terms of risk management aspects[3].

COBIT 5 provides a comprehensive framework that can assist companies in achieving their goals for corporate IT governance and management. And it can be said to help companies in creating optimal value from IT applications. By maintaining a balance between realizing benefits and optimizing the level of risk and use of resources.

2. Research Method

The methods used in this research include:

- Observing by conduct in-depth discussions with professional experts involved in the Risk work unit as well as IT Security and Governance
- Literacy Method; namely searching for journals related to the COBIT framework, especially those related to the subject matter of Risk Management, IT Security and Governance.
- Conceptual method; In COBIT 5 Framework based on APO, BAI and DSS
- Providing questionnaires (Risk Control Assessment) to the Head of the Information Security Risk Management Division and the Head of the IT Security Policy Unit. Where in the process it will ask different concerns from one another.

In conducting the research, we work based on the IPO (Input-Process-Output) technique. This is expected to be in accordance with the purpose of using the COBIT framework in validating qualities from an audit point of view. In accordance to [4] that in producing audit quality it can be seen from 3 points of view, namely: an input perspective, a process perspective and a results / output perspective. Where in its implementation can produce an ethical aspect that is useful for quality formation. Among the ethical aspects according to [4] are: integrity, objectivity and independence.

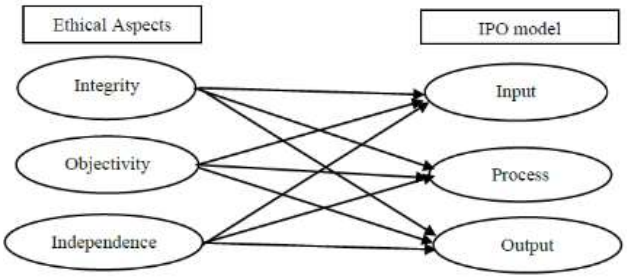

Figure 1. Ethical Aspect in IPO Model [4]

In the input process we ensure that by entering data according to other journal references so that it can be managed in the process of producing output in the form of a framework that can be used based on the COBIT framework, which is related to planning and organizing, development and implementation, and related to deliverable services.

The framework was created for the purpose of overcoming weaknesses in risk management and control that have been adopted by XYZ Bank, including:

• Maturity level, in how to assess and comply

• There is duplication of existing controls, thus making XYZ Bank lacking a single control repository.

• The need for clarity of processes and solutions for risk assessment

In the decision to use COBIT has been set by the team at XYZ Bank where a team is formed of governance experts in determining a basic risk management framework. The defined processes and templates to be used

are appointed by a team consisting of the IT security and risk management unit. There are 3 areas that underlie this, including:

• What form the conceptual framework will be used

• Identification of 'entity' standards for evaluating risks and controls

• Identification of how the process is in carrying out a Risk control assessment (RCA).

3. The Framework

The framework is defined by linking risks affecting technology and best control practices according to industry standards as defined in COBIT. Three goals have been set, among others :

1. Acting as a tool to facilitate risk assessment and effective control in technology.
2. Acting as a reporting framework to demonstrate how technology has met the requirements of reporting regulations, including the requirements contained in OJK regulations.
3. Acting as a means that can encourage assurance to management.

Following are the steps in implementing a framework using COBIT according to the expected outcome based on the risk rating [5], including :

• Risk identification level I (Severe) is defined based on information that has a financial or non-financial impact such as technology, business operations, people, law, regulatory, financial reports, financial crime and reputation.

• Risk identification level II (Major) is the main risk that is divided into 2 levels in terms of the impact that will be generated and its impact on business operations. At level II (Major) as related to the risks associated with IT technology as a supporting unit:

- Lack of IT support, especially in relation to the design and testing environment.

- IT systems that are not available as a support in a work unit

- Lack of awareness of the security of IT use

• On the identification of controlled objectivity; Where every risk that falls into the level II category can be identified with the use of COBIT. Table 1 shows the mapping of these risks in level II categories with controls identified for each risk of using technology[6] [7].

Table 1. Mapping Level Risk

Risk Control Assessment		
Adequate Design of IT System	**Availability of IT system**	**IT Security**
APO1 Define Information Architecture strategy	BAI2 Acquire application requirement software	APO1 Define Information Architecture strategy
APO3 Technology direction	BAI3 Acquire Technology solution	APO2 Define IT organization and relationship
APO8 Manage Quality Relationship	BAI5 Manage IT resources	APO9 Assess and Manage IT Risk
APO10 Manage Project Suppliers	DSS1 Devine and manage service level	BAI2 Acquire application requirement software
BAI1 Manage Programme for automated Solution	DSS3 Manage performance	DSS5 Ensure system Security
BAI2 Acquire application requirement software	DSS4 Ensure continuity service	DSS11 Manage Data
BAI3 Acquire Technology solution	DSS8 Manage Incident data	DSS12 Manage Phisical Environment
BAI6 Manage Changes	DSS3 Manage problem	
BAI7 Install and accredit solution changes	DSS11 Manage Data	
	DSS12 Manage Phisical Environment	
	DSS13 Manage Operation	

4. Identifying the Entities

In the design of IT systems, key entities related to model management are needed, where the model must be assessable and also to control risk. Logically this can be related to objectives related to reporting mechanisms and how to control support services on a technology platform [8].

In IT design, it can be defined in a model related to:

- **Person entity**: Where in this section there is certainty of duties and how it is correlated with social aspects (compliance, rules, work methods, culture, norms, personality, etc.) With the existence of an entity person is expected to be able to carry out risk assessment and control of the complete use of technology.
- **Process entity**: In providing support, control and governance in the IT environment, a process that can represent this is required.
- **Technology entity**: dealing with components in IT, such as: applications, servers, networks and firewalls.
- **Governance entity**: Relates to compliance with applicable and determined regulations, both from internal and regulatory agencies. And on this matter, it is recommended to know the control information and risks that may occur. Also important in meeting the target status for the development or change of a project before going live.

In determining IT services is one of the methods of this bank to fulfill the objectivity of the function of IT services. Identification of support services in a service scope consisting of the top types of services in a catalog that can be used as a reference. Service forms can be represented in the form of a support service map. The map consists of an explanation of the technology components in support of a quality form of end-to-end service. Each process entity and technology entity will differ greatly in linking to multiple support services. From this statement, it is expected that the results will be in accordance with the key management model of the key entities, so it can be said that a lot of flexibility can also be used as an expansion of IT services. In addition, it must also be adjusted to the needs of the organization today, tomorrow and in the future. Among these entities are interrelated and possibly useful in conducting risk assessments by means of developing and providing end-to-end service risk profiles in relation to overall management of the entity's management.

5. Implement and define the RCA Process

Figure 2 shows the process according to an overview that describes the risk assessment process in five steps [9]. Where the main task at each step should be identified. Process assistance in scope, schedule and how to carry out a risk assessment can be explained in detail.

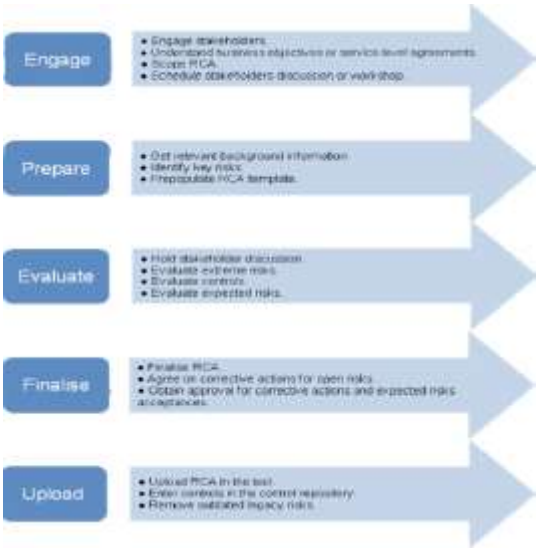

Figure 2. Risk and Control Assessment Process Step

The purpose of developing the RCA process is how to make certainty in the analysis and consistency of risk control involving a team. Excel templates can be used as a support tool to determine whether the available controls are feasible and can assist in determining risk. Templates are used by all entities defining all information assets. Templates are specified in capturing the following information:

- OJK control requirements and best practices
- Defining risk according to the level of potential risk
- Application according to the control process of COBIT
- Ownership of control
- Conduct an assessment of the available controls whether they are effective or not
- What actions will be taken to exercise control effectively
- The final stage of how the details of the action can be accommodated with data on the owner of the action and the target date for the action

In the template, complete information is carried out by the risk owner himself so that it can be reviewed and assessed by the integrated risk team. Then in the process of reporting open risks, it is entered into a risk management tool to record the closing actions taken. Consists of Tags :

- Entity owner: Risk Control Assessment (RCA) owner
- Risk owner: Who is responsible for the risk
- Owner of control: The owner who is responsible for maintaining the effectiveness of the control
- Owner of action: Which is determined due to ineffective controls

6. Result and Discussion

Based on the results of the observation and questionnaire on XYZ Bank. It can be concluded based on RCA step as follows :

- Adequate design of IT System.

APO1, related to the information architecture strategy, XYZ Bank is available and has implemented the Information Technology Strategic Plan (RSTI).

APO3, the direction of use and development of technology has also been well managed.

APO8, the quality management of the relationship between IT as a supporting unit and Line of Business (LOB) as a partner is quite good in providing technology application solutions. Although there are several GAPs, sometimes business initiatives for reasons of speed and accuracy often bypass IT and work directly with third parties.

APO10, collaboration with suppliers is inevitable, and potential risk factors are sometimes a second thing, so the business team often deviates from existing standards.
BAI1, the use of automated solutions has been widely implemented and has become a consideration for business units to be able to enhance systems / applications, especially those related to customer transactions.
BAI2, deals with build-in and in-house IT applications, where there is no ASR (Application Security Requirement) as a reference for security standards in IT applications.
BAI3, the latest technology solutions have been implemented and taken into consideration by management
BAI6, according to BAI3 which also has a correlation, it can also be explained that every change must be recorded properly. And the CCB (Change control board) mechanism which is held weekly with a permanent IT team.
BAI7, deals with the implementation of all change solutions related to technology use initiatives.

- Availability of IT System.

BAI2, It can be explained that every application at XYZ Bank must meet the minimum security requirements in accordance with IT Security standards.
BAI3, Obtaining Technology Solutions in accordance with the objectives and benefits of the Bank's business initiatives by always innovating in order to meet customer expectations by opening feedback channels for each service.
BAI5, Manage IT resources in a professional manner by consistently conducting continuous training, with centralized training facilities in Bogor by bringing in professional trainers from within and outside the country.
DSS1, Develop and manage service levels centrally by a Service Quality work unit.
DSS3, Manage performance by continuously updating information technology as a support.
DSS4, Ensuring service continuity by always innovating on digital products.
DSS8, Manage incident data well, because CSIRT rules are available as a standard reference for incident management.
DSS9, Managing problems has not been centrally still decentralized according to business units.
DSS11, Manages data fairly well, with tools namely DMS (Data Management System).
DSS12, Manage the physical environment fairly well and apply various kinds of the latest technologies such as Face Recognition Access.
DSS13, Managing operations towards office transformation to Digital Bank by implementing agile development.

- IT Security.

APO1, Information Architecture Strategy cannot be defined structured.
APO2, IT organizations are still not mature enough in terms of the types of work that are still overlapping.
APO9, Lack of risk management for IT, because the mainset of the IT team is only a support, not a bank-wide enabler.
BAI2, Rules for the use of software as security prerequisites have been set in IT security standards.
DSS5, System Security Standard is quite comprehensively regulated in the IT Security Standard provisions.
DSS11, In managing data related to security events, it is good because it has implemented SIEM.
DSS12, Physical Environment Management in terms of data security is good enough with the availability of capable data security mechanisms.

Regarding the training stages, there are generally many terms, using the RACI chart we can define each term into a task and function of each part such as the entity owner, risk owner, control owner and owner of the action. RACI itself is responsible, actionable, consulted and informed (see example in Figure 3[10]). Responsibilities can also be mapped into job descriptions with various performance evaluation criteria for each function or it could be the job level. And this arrangement will have an impact on employees.

RISK / Entity	CEO	COO	Integrated Risk	Facility Mgmt	IT Sec & Gov	Human Capital
Activity/Deliverables						
Manage Logical Security	I	I	C	C	R	C
Manage Physical Security	I	C	C	A	C	-
Reporting Security Incindent	I	A	I	I	R	I

Figure 3. RACI Chart example

Figure 3 can illustrate, where the facility management department is responsible for the continuous availability of physical security, while the chief operating officer (COO) is responsible for the incident reporting mechanism along with how to respond and the follow-up process. Meanwhile, every staff, both employees and vendors, in acting and working outside the office, it is in the attention of the HC team that they can be consulted regarding the logical security of the company's assets, namely the employees themselves and also be informed for the reporting.

The main challenge according to duties and responsibilities as in the example of the RACI matrix above is in explaining each process to stakeholders who have different backgrounds and understandings. This must be managed properly in order to be able to understand the risks where a training program is needed at various levels[11]. By involving more :

- In making adjustments to the training material delivered by the risk experts. Speaking of entity owners, there is a simple description of a process provided through a compulsory computer-based continuous training. As for risk and control owners, training details which include a sample and test, can then be delivered through classrooms in different locations or through web-based training sessions.
- By adjusting the training provided by risk experts to the audience. For entity owners, a simple process overview is provided through compulsory computer-based training. For risk and control owners, training is detailed and includes samples and tests, and delivered via classrooms at different locations or via web-based training sessions.
- Offering, as part of the mandatory training program, this awareness training session can be expected to explain the process by providing links and contacts to local risk experts within the organization with further guidance.
- By holding workshops it is hoped that we can disseminate relevant information to stakeholders, by starting the risk assessment process. Training resources were used to facilitate control self-assessment (CSA) at different locations.
- In the modification of the description, related to the role and how the performance evaluation process and real-time to be able to include specific tasks in risk and control.

7. Result and Discussion

The reporting process uses a simple spreadsheet which functions to maintain risk and control the repository for each entity. Within each entity, tools such as the Excel spreadsheet used to track risk can be used by members of the risk team, helping to determine actions to take and other matters. In the use of database repositories, generally serves to maintain risk over control within the organization[12]. Therefore, tools were developed to collect information about all entities. which will assist in :

- Centralized risk repository and information control

- In the process the RCA can help track all actions that have been determined and that have been approved
- Every service risk is Traceable
- Every closure action can be tracked
- Report to senior executives on risks based on requirements and levels of risk
- The basis for reporting on regulatory requirements is contained in a common risk and control database

8. Conclusion

In the development and implementation stage it took nearly two years. While the central team is responsible for developing the process, risk resources are work unit based, so it plays an important role in the implementation, training process, etc. Because the implementation is in different locations, it requires the involvement of several work functions in the team. Changes will make some work units resistant, with the feedback mechanism that the team uses to help in the process of aligning and correcting each change. This can help in increasing the maturity of the process. Other tangible benefits of this initiative :

- This exercise is very helpful for banks in managing risk and the control process according to best practice standards as well as from the regulator (OJK) and other regulatory processes. The spreadsheets in the RCA provide separate filters for implementation of compliance levels.
- Repository processes really help maintain consistency. This is done by creating a separate sub-unit within the risk team to ensure a quality check for each RCA prior to inclusion in the repository.
- The training package is generally seen as an important and valuable delivery by the risk team and is based on the needs of the participants. For example, a 15-minute training package for all entity owners was developed and implemented using an e-learning portal, while a detailed process training package was developed specifically for risk and control owners.

9. References

[1] R. Lock, T. Storer, I. Sommerville, and G. Baxter, "Responsibility modelling for risk analysis," *Reliability, Risk, and Safety*, no. September 2009, 2009.

[2] B. D. W. Hubbard, "Risk Management: A Very Short Introduction to Where We've Been and Where (We Think) We Are," *The Failure of Risk Management*, pp. 21–35, 2015.

[3] H. Haviluddin and A. Patricia, "Exploring COBIT Framework for Information Technology Governance (ITG) at Mulawarman University, Samarinda, East Kalimantan, Indonesia: A Descriptive Study," *Enhancing Sustainability, Competitiveness & Innovation*, no. 01, 2012.

[4] A. Agus and N. Aziza, "The effects of ethical factors in financial statement examination: Ethical framework of the input process output (IPO) model in auditing system basis," *International Journal of Financial Research*, vol. 11, no. 2, pp. 136–145, 2020.

[5] W. J. Fletcher, "The application of qualitative risk assessment methodology to prioritize issues for fisheries management," *ICES Journal of Marine Science*, vol. 62, no. 8, pp. 1576–1587, 2005.

[6] J. Barve, "COBIT Case Study: IT Risk Management in a Bank." [Online]. Available: https://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Study-IT-Risk-Management-in-a-Bank.aspx.

[7] M. Wolden, R. Valverde, and M. Talla, "The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system," *IFAC-PapersOnLine*, vol. 28, no. 3, pp. 1846–1852, 2015.

[8] R. D. S. De Haes, W. Van Grembergen, "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities," *COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities*, p. 25, 2013.

[9] B. W. Main, "Risk Assessment : A review of the fundamental principles," *Risk Management*, vol. 24, no. 4, pp. 1–7, 2008.

[10] S. Zhang and H. Le Fever, "An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-

BSC Model," *Journal of Economics, Business and Management*, vol. 1, no. 4, pp. 391–395, 2013.

[11] V. M. Sunder, "Lean six sigma project management - A stakeholder management perspective," *TQM Journal*, vol. 28, no. 1, pp. 132–150, 2016.

[12] U. Noor and A. Ghazanfar, "A survey revealing path towards service life cycle management in COBIT 5," *2016 11th International Conference on Digital Information Management, ICDIM 2016*, pp. 68–73, 2016.