Measuring The Implementation of IT Risk Analysis in Commercial Bank Based on Best Practice (a Case Study)

DEWI PUSPASARI, M. KASFU M. SATTAR, REIN NUSA
IT Governance Laboratory
University of Indonesia
Depok, Jakarta
INDONESIA
dewi.puspa00@gmail.com, kasfu@cs.ui.ac.id, m.sattar@gmail.com, rein.nusa@gmail.com

Abstract: - Risks faced by a bank increases with increasing number of users of electronic banking services. The threats not only bank robberies physically, but also the crime through a network of globally connected computer. Therefore, information technology risk management has become imperative for banks in Indonesia with the Regulation from Bank of Indonesia is increasingly tight. It is fully realized by the XYZ Bank that has started implementing IT risk management. However, because of limited time when they arranged an internal regulation of IT risk management, they have not yet do a thorough evaluation of their risk analysis methods compare with the existing best practices, such as IT Risk. In this study we evaluated the IT risk analysis has been done XYZ Bank. Though their time is limited and their personnel in the field of IT Risk is also not a lot, they have met almost all the essential of best practices, which have been tailored to their business needs.

Key-Words: - IT risk, risk analysis, best practices, IT Risk, regulation

1 Introduction

The rapid development of information technology requires a bank to continue to increase alertness. Moreover, with the increasingly widespread crime through electronics, such as falsification of the site of one leading bank in Indonesia some time ago and the break-through ATM machines are rife in 2010 [1].

If the bank's previous management familiar with market risk, credit, and legal, the bank now also need to consider other types of risks such as operational risks, some of which have to do with the use of information technology. The risks were not only stand alone but can also influence each other, such as the shift of customers who experienced break-ins money. In this case the operational risks affect the risk of reputation.

Risk cannot be separated with the assets owned an organization and the accompanying threats. These three things should be viewed comprehensively. If an organization's assets increase, then the list of threats needs to be evaluated, as well as risks. Because of that risk analysis is not something static but dynamic.

In the XYZ Bank's internal policies, listed IT risk analysis methods. However, until now the XYZ bank has not done a comprehensive evaluation of whether the method of risk analysis has met the essential of best practices. Gap analysis from the comparison can be input for improved methods of risk analysis in the future, so that IT risk management can be optimized.

2 IT Risk

According to ISO/IEC 27005:2008 IT risk is a potential that a particular threat will exploit vulnerabilities of assets or asset groups, thus causing losses to the organization [2]. This risk is measured by the probability of occurrence and its consequences.

To manage IT risk we need several steps to identify, analysis, and evaluation. The steps are called by IT risk management. The NIST 800-30 define IT risk management include three processes: risk assessment, risk mitigation, and evaluation [3]. There are many guideline and best practices to govern IT risk, such as COSO, COBIT, and IT Risk.

IT Risk is framework that launched by ISACA to identify, govern, and manage IT risk. It has principles to get optimize benefit from IT risk management. There are: must be connect to business objectives, align with overall ERM, balance the cost and benefits of managing IT risk, promote fair and open communication of IT risk, establish from the top management, also continuous process and part of daily activities.

IT Risk has three domains. Risk governance, risk evaluation, and risk response. Risk analysis is a part of risk evaluation domain.
Before we conduct risk analysis, organization need to determined universe risk and risk management scoping. The purpose of this stage is to identify and explain the environmental risks are related and determine the limits of IT risk management to be applied. And then define risk appetite and risk tolerance to determine the interest rate risk and an acceptable tolerance level for the company. IT Risk also suggest to include risk scenario to assist doing risk analysis. The purpose of risk scenario is to understand the risks associated with IT risk using scenario analysis.

The next stage is risk analyze. The purpose of this stage is defining the magnitude of risk caused by the impact of an IT incident. The quantity of risk is measured by the impact and occurrence frequency level. Then taking into account the level of risk tolerance, can be determined what level of risk exists, whether accepted or not, otherwise it will be risk mitigation measures.

There are two methods in risk analyze, quantitative and qualitative method [4]. Quantitative method use actual money amounts to provide a financially-based risk value. Qualitative method use scoring methods and the experience of employees and consultants to arrive at a risk score. The first is difficult but easy to understand by top management. The second is contrast with the earlier. Since limitation in each method, scientist combined two methods as semi qualitative method.

Risk analyze in IT Risk include risk response and prioritization. The purpose of this phase is to provide guidance on how to perform selection and prioritization of risk that will respond. The goal is to provide a response to the risks to match the tolerance limit of acceptable risk and has been set for the company. Four categories of risk responses that are commonly used are risk avoidance, risk mitigation, risk transfer, and risk acceptance.

3 RESEARCH METHODOLOGY

In this study we did several stages, beginning with define a research question, whether the implementation of risk analysis in XYZ Bank is met with best practices like IT Risk. We use IT Risk Practitioner Guides that contain practical and more detail guidance how do some of the activities described in the process model.

Next, we conducted deep interviews with key users, beside collect documents and internal regulations related to IT risk analysis. Then we reviewed of risk management, in particular stages of IT risk analyst.

Next, we compare the results of that analysis with best practices, IT Risk. From this comparison, the result is a gap list that could be a note of management for future enhancement.

4. Measuring Implementation of IT Risk

4.1 Existing Condition

XYZ bank has an internal regulation on Guidelines for Implementation of IT Risk Management BTN as a major reference in implementing IT risk management. This regulation includes an IT risk management cycle which divided into four major stages as shown in figure 3.
IT risk analyze as shown in figure 3 is next stage after asset criticality analyze. This stage aims to identify sources of risk that may occur following impact. The final goal of this stage is to determine the level of criticality of IT risk. There are four major activities undertaken at IT risk analysis stage: the identification of risks, identification of risk impact, the value of risk identification, risk and criticality analysis (figure 4). Explanations of each activity are as follows:

a. Risk identification
This activity aims to identify and classify risks into six risk groups: IT systems, information security, energy resources, human resources, networking and communications, also compliance. This activity not only records the risks list that might occur but that ever happened at XYZ Bank.

b. Risk impact identification
The purpose of activity to identify the likely magnitude of risk posed to the whole business on the XYZ Bank. Identify the impact of risk refers to Bank of Indonesia’s Regulation (PBI) No. 19/15/PBI/2007.

c. Risk value identification
Parameters that determine these values are: likelihood of risk (which used the same probability as measuring the threat likelihood) and impact.

d. Risk criticality analysis
Criticality level of risk is the product of the likelihood of risk by the impact of risk which is then mapped into a matrix of risk criticality. Criticality level of risk classification is as follows:
- High : between 60 to 100
- Medium : between 8 to 60
- Low : from 1 to 8

4.2 Gap Between Existing Condition and Best Practices

4.2.1 Risk Type
In conducting the risk analysis, Risk IT organizations require to determine the risk universe in order to do analysis of the impact of each type of risk category, and then make assessments on assets held to determine the level of asset criticality. This has been done by the XYZ Bank to define the risk universe which is divided into eight categories.

The type of risk defined has been adapted to the condition of the banking business and XYZ Bank as shown in table 2. Determination of risk type by XYZ Bank is quite appropriate, considers the risk universe of each companies is different, adjusted to actual conditions in the company. This is to ensure accurate data related to impact risk identification.

Criticality of assets has also been performed on stage before the risk analysis (figure 3), but unfortunately there is no necessary connection.
between stages of asset criticality and risk analysis. A result of asset criticality matrix (figure 5) does not become the input for risk analysis.

Table 2. Comparison of Risk Type of Risk IT with XYZ Bank

<table>
<thead>
<tr>
<th>Risk Type (Best Practice)</th>
<th>Risk Type of XYZ Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic risk</td>
<td>Strategic risk</td>
</tr>
<tr>
<td>Market risk</td>
<td>Market risk</td>
</tr>
<tr>
<td>Credit risk</td>
<td>Credit risk</td>
</tr>
<tr>
<td>Operational risk</td>
<td>Operational risk</td>
</tr>
<tr>
<td>Compliance risk</td>
<td>Compliance risk</td>
</tr>
<tr>
<td>Environmental risk</td>
<td>Reputation risk</td>
</tr>
</tbody>
</table>

4.2.2 Risk Map

Risk map determination in XYZ Bank based on risk criticality rate with criticality scale that had been determined in internal regulation (figure 6). It used semi-quantitative method from forum group discussion between IT risk staff and consultant.

From figure above, we can conclude that XYZ Bank had determined risk appetite that classified by three types, low, medium, and high. In contrast, risk tolerance had not been defined clearly. But from assessment result, for all high risk can’t be tolerated. Meanwhile, medium risk, some of them can be tolerated.

Risk appetite determination is static, no mechanism to review and update risk appetite and risk tolerance rate in XYZ Bank.

Magnitude of risk is also calculated based on estimated impacts and risks that ever happened before. The process of review of the risk analysis conducted regularly and has been documented in the SOP IT risk management. This is in accordance with the principles of IT risk is the risk analysis process carried out continuously.

![Fig 6. Risk Map XYZ Bank](image)

4.2.3 Risk Scenario

On IT Risk, risk analysis process gets input of risk scenarios. However, at XYZ Bank entered it in the next step, namely the mitigation of risk.

4.2.4 Risk Response and Prioritization

On IT Risk, risk analysis process, including the response in addressing the risks. However, at XYZ Bank entered it in the next step, namely the mitigation of risk.

4.2.5 Summary of Gap

A summary of the results of a comparative evaluation of the risk management framework is a framework that runs XYZ Bank current with best practice guide practitioners and IT Risk adjustment...
for the benefit of IT application development risk can be seen in the following table.

<table>
<thead>
<tr>
<th>No</th>
<th>Risk Guide</th>
<th>IT Practitioner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Risk Type</td>
<td>Tailored to the needs of the bank's business</td>
</tr>
<tr>
<td>2</td>
<td>Risk Map</td>
<td>Using semi quantitative methods</td>
</tr>
<tr>
<td>3</td>
<td>Risk Scenario</td>
<td>Not as input analyze risk.</td>
</tr>
<tr>
<td>4</td>
<td>Risk Response and Prioritization</td>
<td>The Next stage, not include with risk analyze</td>
</tr>
</tbody>
</table>

5 Conclusion

XYZ Bank has met some of the principles in conducting risk analysis. The difference between the steps in conducting a risk analysis of current conditions with best practices because of the adjustment of XYZ Bank to business needs and regulatory requirements from Bank of Indonesia. The note for XYZ Bank is integrating the asset criticality analysis with risk analysis so that both are one path, not stand apart.

References: