ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 136

1st Annual Management, Business and Economic Conference (AMBEC 2019)

Operational Risk Analysis in Department of Enterprise Risk Management of PT. XYZ Based on ISO 31000: 2018 Framework

Lucyana Dewi*, Mandra Lazuardi Kitri
School of Business and Management
Institut Teknologi Bandung
Bandung, Indonesia
*lucyana.dewi@sbm-itb.ac.id, m.lazuardi@sbm-itb.ac.id

***Abstract*—PT. XYZ is a manufacturing company whose risk management practice is still categorized as an inefficient one which indicates the failure in the operations of the Enterprise Risk Management Department. Recently, there is no previous risk management research carried out on the implementation of risk management itself or which in this research explained as an operational risk at Department of Enterprise Risk Management in PT. XYZ. The aim of this research is to do risk analysis within the operations of the Enterprise Risk Management Department in PT. XYZ. Risk analysis was carried out using the ISO 31000: 2018 framework with qualitative approach which is only limited to the process of risk identification, risk analysis, risk evaluation, and risk treatment option selection. According to the analysis that has been carried out, 17 risks have been identified with 3 different types of operational risks, namely process, system, and people. From the assessment for each risk, the result shows that 9 risks are high risk, 7 are moderate risks, and 1 low risk which means that there is a need for mitigation actions for most operational risks that have been identified to reduce the level of likelihood and consequence of those risks.**

Keywords: risk, operational risk, risk management, ISO 31000: 2018

I. INTRODUCTION

PT. XYZ is a manufacturing company core competencies in specified product with the service of design and development, structure manufacturing, production, and other services that related to that specified product. It has been established since 1976 and the company has experienced several challenges in its business where it even had temporarily closed down during the 1998 crisis.

After years, in 2002, to face new global market system, the company has a changing phase which focusing on applying a new strategy to fulfill the current situation with a new structure. The restructuring program covers business re-orientation, justify and arrange human resources with available workloads, and strong capitalization based on the market which market-focused and concentrated business mission. PT. XYZ also changed the name of the company at that time.

One of the results of the changing phase was the establishment of Department of Enterprise Risk Management under the Division of Corporate Planning in 2003, which aimed to meet several manufacturing company standards which the implementation of risk management system for the whole company to overcome the negative risks that might occur in its business is needed. In implementing risk management, PT. XYZ currently refers to ISO 31000: 2018 Standards where ISO/TR 31004: 2016 and ISO/IEC 31010: 2016 serve as

guidelines for the implementation and techniques that should be used in risk management following the framework, principles, and processes described [1].

However, even though the Department of Enterprise Risk Management has been established, the company still faces some challenges within its business until today. For instance, some challenges are ineffective supply chain management practice, non-optimal human capital management, unrealized target sales, etc. As a result, the business has difficulty in gaining positive net income for years. For the past ten years, from 2010-2018, the business has faced losses on its financial statement for years except in 2014 and 2017.

The Manager of Department of Enterprise Risk Management in PT. XYZ [2] states that the implementation of enterprise risk management within this company is still can be categorized as an ineffective practice. It is proven by the losses and problems faced by this company for years, whether from financial, human capital, operational, or other aspects. This is the indication that the implementation of risk management at PT. XYZ is not optimal because risk management procedures have been carried out to deal with these issues from the process of risk identification to the risk treatment. However, in reality, these risks still occur and become a problem which is certainly being a challenge for the company.

Some proofs showing that inefficiency of risk management is causing the problem is that some parties within company still has "silo mentality" character in the implementation of risk management, which is defined by the Manager of Department of Enterprise Risk Management in PT. XYZ [2] as "a mindset present when certain departments or sectors do not wish to share information with others in the same company." Besides, some parties just provide risk analysis to fulfill the standard, but not implement it for the business practice. Those are an example of factors why all of those negative risk impacts such as losses and problems related to supply chain management

and human capital have still occurred even though risk management for the company's business process has been implemented.

However, ensuring the successful implementation of risk management in the company is the responsibility of the Enterprise Risk Management Department. The manager believes that this failure can occur as a result of an error either in the process, people, or other factors in Department of Enterprise Risk Management which certainly can disrupt the efficiency of the risk management process at PT. XYZ. The inefficient practice of risk management indicates the failure in the operations, where all readiness and resources already exist, but failure arises when the execution of the plan has been built. Where according to Oxford Dictionary [3], the inefficient condition is defined as "not achieving maximum productivity; wasting or failing to make the best use of time or resources."

To find out earlier about the risks that might arise in Department of Enterprise Risk Management of PT. XYZ, the analysis of operational risk for its Department of Enterprise Risk Management is needed to be carried out. The aims of the analysis consist of several processes which cover risk identification, risk analysis, risk evaluation, and risk treatment option selection.

II. METHODS

In conducting this research, the risk management process is limited by risk assessment (risk identification, risk analysis, and risk evaluation) and risk treatment option selection. The type of this research is a case study with qualitative method due to some considerations such as qualitative analysis is needed to understand the condition of the company and its risk management practice comprehensively and qualitative analysis is needed to uncover perspective from stakeholder who best understands the situation of the problem.

A. Data Source

Primary data includes general description of company, general description of Department of Enterprise Risk Management and its risk management practice, minor and major problems faced by Department of Enterprise Risk Management, current development program for risk management practice, general and qualitative likelihood and consequence risk criteria standard, level of likelihood and consequence for each risk identified, consequence/probability matrix standard, and risk category standard.

B. Data Collection

1) Interview, Interview is used to gain all of primary data needed to formulate risk identification. It is prepared with the question lists for related stakeholder which provided in Appendix A. The stakeholder that will be interviewed is Manager of Department of Enterprise Risk Management of PT. XYZ. After gaining answers from interviews, researcher will formulate risk identification that will be validated and discussed further with other stakeholders. The output from this interview is the lists of operational risks identified. Identified risks are used for the next step according to this research framework.

2) Focus Group Discussion, Focus group discussion is conducted to validate the results of previous interviews operational risks that have been identified and also to identify causes of appearance of risks in the Department of Enterprise Risk Management with the help of Fishbone / Ishikawa Diagram method. Focus group discussion will be held with stakeholders in the department, totaling four people and carried out directly at PT. XYZ.

3) Questionnaire, The questionnaire is used to asses each risk based on level of likelihood and consequence to obtain the total score of each risk. The results of the assessment will be used for the next process which is risk evaluation. The questionnaire will be filled by stakeholders in the Department of Enterprise Risk Management who have participated in focus group discussions which consist of four people.

C. Data Processing

To analyze collected data for this qualitative research, below are the lists of chosen tools for this research. Following methods are in accordance with the techniques of identification, assessment, and analysis in accordance with guidance from ISO/IEC 31010: 2016 Technique Implementation to analyze operational risk in Department of Enterprise Risk Management of PT. XYZ related to risk management practice at PT. XYZ.

1) Fishbone or Ishikawa Diagram, Fishbone or Ishikawa diagram is used to fulfill risk identification step. It is used to identify causes of risk so that the management understand the root cause of that identified risk. Causes of the risk are identified from the stakeholder perspective regarding the cause of the risk itself because the stakeholder most understands the conditions of these risks, where the stakeholder consists of four people from Department of Enterprise Risk Management. Fishbone or Ishikawa diagram for this research refers to Figure 1.

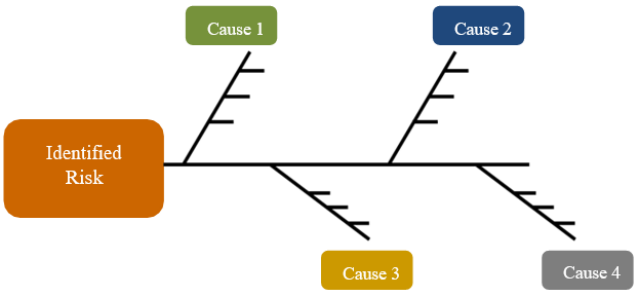

Fig. 1. Fishbone or Ishikawa diagram design for risk identification.

2) Consequence / probability Matrix, Consequence / probability matrix is used to fulfill risk analysis and risk evaluation process. The output is a rating for each risk or a ranked list of risk with significance levels defined. Before gaining ranked list of risk, researcher is going to determine the level of consequence and likelihood of each risk which each

level has been measured under explained condition. Below are standards for both level of consequence and likelihood, and consequence/probability matrix that refers to PT. XYZ [4] which has been revised to adjust this research. Table 1 and 2 explain measurement for level of each likelihood and consequence of risk for this research, and consequence/probability matrix for this research refers to Figure 2. After each risk has been ranked based on its level of likelihood and consequence, and classified into consequence/probability matrix, Table 3 shows what action should be taken based on each risk category.

TABLE I. GENERAL AND QUALITATIVE LIKELIHOOD RISK CRITERIA

Level	Term	Description	Probability
1	Rare	Rarely / almost never occurs, even if it occurs only in abnormal or certain situations	≤ 1%
2	Unlikely	Rarely happens or can happen but at certain times, in the right atmosphere / situation	1% < X ≤ 15%
3	Possible	Sometimes it happens, it can happen at certain times, in a normal atmosphere	15% < X ≤ 50%
4	Likely	It often occurs in every situation, or it is likely that it will occur in a normal atmosphere.	50% < X ≤ 70%
5	Almost Certain	Almost certain / often occurs in every situation or certainly will occur in any atmosphere	70% < X < 100%

Source: PT. XYZ Terms of Implementation - Risk Management (2016).

TABLE II. GENERAL AND QUALITATIVE CONSEQUENCE RISK CRITERIA

Level	Term	Description
1	Insignificant	• Small impacts on targets, can be ignored • Financial losses are very small or there are almost no financial losses at all • Does not interfere with the operation of the organization / project / program • It is enough to handle the internal company / organization
2	Minor	• Small damage and easy to repair • Small-to-medium financial losses • It is enough to handle the internal company / organization
3	Moderate	• Affects the achievement of several goals • Medium-large financial losses • The handling does not need assistance from outside the company
4	Major	• Important goals cannot be achieved • Loss of production capability • Big financial loss • Serious threat to the organization / project / program • The handling needs help from outside the company, but does not cause damage
5	Catastrophic	• A catastrophe / big disaster, all targets cannot be achieved • Financial losses are enormous or extraordinary • Very dangerous to the organization / project / program • The handling needs help from outside the • company and causes total damage is not acceptable

Source: PT. XYZ Terms of Implementation - Risk Management (2016).

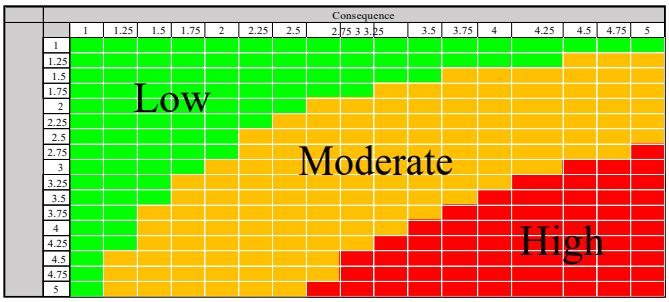

Fig. 2. Risk evaluation standard for this research.

TABLE III. RISK CATEGORY STANDARD FOR THIS RESEARCH

Risk Category	Score	Action	Need Mitigation Plan
Low	1 ≤ x < 5.5	Can be ignored, handled through routine procedures.	No
Moderate	5.5 ≤ x < 13.5	Action is needed to eliminate risks to control adequate risks.	Yes
High	13.5 ≤ x < 25	Serious attention is needed from management. Cannot be tolerated and immediate treatment is required.	Yes

III. RESULTS AND DISCUSSION

A. Risk Identification

Identification of possible risks that will occur in the operations of the Department of Enterprise Risk Management at PT. XYZ is conducted by analyzing the results of interviews. From the result of the interviews, risks are identified by researcher by processing the interview result and some information gained from articles related to risk management challenges. Those identified risks are validated by conducting focus group discussion along with using Fishbone / Ishikawa Diagram. The following Table 4 are the results of identification of operational risk in the Department of Enterprise Risk Management of PT. XYZ along with each type.

TABLE IV. RISK IDENTIFICATION RESULT

Type of Operational Risk	Code	Risk	Description
Processes	A1	Inaccurate risk analysis process	Failure in assess risk regarding to level of likelihood and consequence due to misunderstanding about risk condition and assessment guideline
	A2	The risk analysis process is not in accordance with company procedures	Risk analysis implemented not along with company's procedures related to risk management (certain process or principle is not well-implemented)

Table 4. Cont.

Processes	A3	Non-optimal risk mitigation process	Mitigation plan has not created or has created but not well-implemented even abandoned
	A4	Lack of information sharing from all parties in the risk management process (silo mentality)	Risk management is carried out unilaterally by each department, division, or unit and with certain parties only
	A5	Delay in the risk management process	Risk management is carried out late so that it cannot be implemented properly or cannot even be implemented at all in practice
	A6	Unwell managed administration and documentation for risk management	Proof of administration and documentation are not arranged in one place and are difficult to find
	A7	Unwell communicated risk analysis results	The risk analysis that has been made does not reach stakeholders in a timely manner or delivered but with limited understanding
Systems	B1	Non-optimal information system	Information related to risk management is difficult for all stakeholders to access
	B2	Inadequate procedures for certain situations and conditions	There is no SOP that is good for certain situations and conditions that are rare in the company
	B3	Unsuccessful project on risk management portals update	The risk management portal development program in the company is not in accordance with the plans that have been made
	B4	Loss of data related to risk management	Data loss due to a system that is too difficult to operate to store data or system hardware that has passed its lifetime
	B5	Incompleteness and inaccuracy of the information database	Sources of information related to risk management are incomplete or come from untrusted sources
People	C1	Incompetent employees within the department	Employees do not acquired the concept of risk management properly
People	C2	Lack of risk management knowledge for all stakeholders	Stakeholders in each area of risk management (related departments, divisions, units, projects, etc.) do not master acquired the concept of risk management properly
	C3	Conflict of interest in risk management implementation	The emergence of differences in goals, values, and interests in the implementation of risk management among stakeholders
	C4	Undisciplined and inconsistent people in risk management practice	Stakeholders do not follow the risk management SOP properly and consistently
	C5	Negligence in carrying out risk management by certain parties	The tendency of people to underestimate a problem, condition, and risk in the risk management process

B. Risk Analysis

Risk analysis is carried out to get each risk assessment with a predetermined level of possibilities and consequences. This assessment is done using questionnaire to stakeholders in the Department of Enterprise Risk Management which consists of four people. The following Table 5 is the result of the analysis of each risk.

TABLE V. RISK ANALYSIS RESULT

Type of Operational Risk	Code	Risk	L*)	C*)
Processes	A1	Inaccurate risk analysis process	3	3.75
	A2	The risk analysis process is not in accordancewith company procedures	2.25	3.5
	A3	Non-optimal risk mitigation process	4.25	4.25
	A4	Lack of information sharing from all parties in the risk management process (silo mentality)	4	4.75
	A5	Delay in the risk management process	4.25	3.75
	A6	Unwell managed administration and documentation for risk management	3	3
	A7	Unwell communicated risk analysis results	4	3.75
Systems	B1	Non-optimal information system	3	2.75
	B2	Inadequate procedures for certain situations and conditions	2.75	3
	B3	Unsuccessful project on risk management portals update	2.5	2.5
	B4	Loss of data related to risk management	1.5	3
	B5	Incompleteness and inaccuracy of the information database	4	3.75
People	C1	Incompetent employees within the department	2.5	3.25
	C2	Lack of risk management knowledge for all stakeholders	4.25	4.5
	C3	Conflict of interest in risk management implementation	4.5	4.75
	C4	Undisciplined and inconsistent people in risk management practice	4.25	4.25
	C5	Negligence in carrying out risk management by certain parties	4.25	4.25

*) Note:

L = Level of Likelihood

C = Level of Consequence

C. Risk Evaluation

Risk evaluation is used to determine what actions should be taken on each risk. In obtaining these results, we need the results from the previous stage which is risk analysis and put in the consequence/probability matrix. Figure 3 shows the result of risk evaluation for each identified risk using consequence/probability matrix.

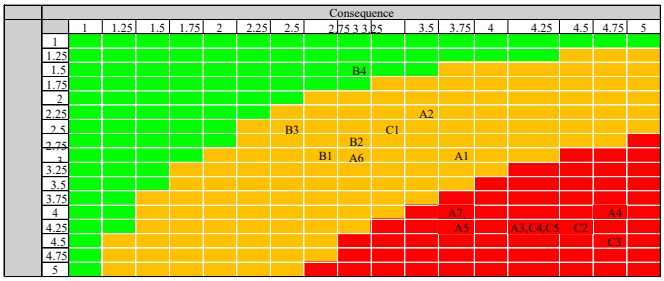

Fig. 3. Risk evaluation result.

From the result of consequence/probability matrix above, risk can be categorized based on the result of each score by multiplying likelihood with the consequence. Table 6 shows each risk category based on its score.

TABLE VI. RISK CATEGORIZATION RESULT

Risk Category	Score	Code	Risk	Type of Operational Risk
High	21.38	C3	Conflict of interest in risk management implementation	People
	19.13	C2	Lack of risk management knowledge for all stakeholders	People
	19.00	A4	Lack of information sharing from all parties in the risk management process (silo mentality)	Process
	18.06	A3	Non-optimal risk mitigation process	Process
	18.06	C4	Undisciplined and inconsistent people in risk management practice	People
	18.06	C5	Negligence in carrying out risk management by certain parties	People
	15.94	A5	Delay in the risk management process	Process
	15.00	A7	Unwell communicated risk analysis results	Process
	15.00	B5	Incompleteness and inaccuracy of the information database	System
Moderate	11.25	A1	Inaccurate risk analysis process	Process
	9.00	A6	Unwell managed administration and documentation for risk management	Process
	8.25	B1	Non-optimal information system	System
	8.25	B2	Inadequate procedures for certain situations and conditions	System
	8.13	C1	Incompetent employees within the department	People
	7.88	A2	The risk analysis process is not in accordance with company procedures	Process
	6.25	B3	Unsuccessful project on risk management portals update	System
Low	4.50	B4	Loss of data related to risk management	System

D. Risk Treatment Option Selection

TABLE VII. RISK TREATMENT OPTION SELECTION

Risk Category	Code	Risk	Risk Treatment Option
High	C3	Conflict of interest in risk management implementation	Risk Mitigation
	C2	Lack of risk management knowledge for all stakeholders	Risk Mitigation
	A4	Lack of information sharing from all parties in the risk management process (silo mentality)	Risk Mitigation
	A3	Non-optimal risk mitigation process	Risk Mitigation
	C4	Undisciplined and inconsistent people in risk management practice	Risk Mitigation
	C5	Negligence in carrying out risk management by certain parties	Risk Mitigation
	A5	Delay in the risk management process	Risk Mitigation
	A7	Unwell communicated risk analysis results	Risk Mitigation
	B5	Incompleteness and inaccuracy of the information database	Risk Mitigation
Moderate	A1	Inaccurate risk analysis process	Risk Mitigation
	A6	Unwell managed administration and documentation for risk management	Risk Mitigation
	B1	Non-optimal information system	Risk Mitigation
	B2	Inadequate procedures for certain situations and conditions	Risk Mitigation
	C1	Incompetent employees within the department	Risk Mitigation
	A2	The risk analysis process is not in accordance with company procedures	Risk Mitigation
	B3	Unsuccessful project on risk management portals update	Risk Mitigation
Low	B4	Loss of data related to risk management	Risk Acceptance

After getting the results of the categories of each risk from the stage risk evaluation, risk treatment option selection has been done to understand what further treatment would be taken for each identified risk. Risk treatment option is selected by stakeholder of the department according to the situation, condition, and ability of the department to handle these risks. Table 7 above shows risk treatment option for each risk.

IV. CONCLUSION

From the results of the analysis, it has been identified that there are 17 risks with three different types of operational risks in the Department of Enterprise Risk Management at PT. XYZ. The score results of each risk referring to the level of likelihood and consequence (risk analysis) indicate that each risk has quite concerning score. The result of risk evaluation for each risk based on their level of priority (risk classification) shows that 9 risks belong to the category of "high", 7 includes of "moderate" risk, and 1 “low” risk which means that there is a need for mitigation actions for most operational risks that have been identified to reduce the level of likelihood and consequence of these risks. From these results, it was also found that the type of risk of "people", namely C3 risk (conflict of interest in risk

management implementation) is a risk with the highest likelihood and consequence level among other risks. Risk treatment that should be taken by management for all of risks are most risk mitigation actions except for a low risk, risk acceptance option is should be selected for that risk.

ACKNOWLEDGMENT

Warm thanks to Mr. Mandra Lazuardi Kitri, S.T., M.B.A., my extraordinary supervisor and interviewees from PT. XYZ who gave me a lot of help during this research.

REFERENCES

[1] International Organization for Standardization. "Risk management — Guidelines (ISO 31000:2018)". Geneva: International Organization for Standardization. 2018.

[2] Manager of Department of Enterprise Risk Management in PT. XYZ. "The Implementation of Risk Management in PT. XYZ [In person]." PT. XYZ, Bandung. 2019.

[3] Oxford Dictionary. Word Definition: System, Inefficient, External Events. [online] Available at: https://en.oxforddictionaries.com/definition/ [Accessed 2 June 2019]. 2019.

[4] PT. XYZ. Terms of Implementation – Risk Management (pp. 9- 14). Bandung: PT. XYZ. 2016.