RISK MANAGEMENT OF TELECOMMUNICATION DEVICES TESTING LABORATORY (A CASE STUDY OF TELKOM INFRASTRUCTURE ASSURANCE UNIT BANDUNG)

Fajar Rahmat Sentiko* **and Taufik Faturohman**
School of Business and Management, Institut Teknologi Bandung, Indonesia
Email: fajar_sentiko@sbm-itb.ac.id

Abstract .*Telkom Indonesia, precisely Infrastructure Assurance (IAS) unit has role in the development of infrastructure that supports industrial revolution 4.0 precisely in the telecommunication sector. To maintain service quality and customer satisfaction, companies must follow ISO 17025:2017 which contains General Requirements for Competence in Testing and Calibration Laboratories with a risk-based thinking approach. IAS unit must implement risk management to anticipate risks that can disrupt the stability of business. The concept used is the adoption of ISO 31000:2009. Risk identification process is carried out from SWOT Analysis, Brainstorming, and other research. Risk analysis using AHP is done using BPMSG Software which then searches for their respective weights, and then obtaining the results of risk evaluation by mapping the risks. The final step is make the risk mitigation. Based the risk analysis, there are 29 risk factors from 7 different types of risks. Risks that have a critical level of risk are 1 risk, risks that have a high risk level are 15 risks, and risks that have a moderate risk level of 8 risks and those with a low risk level are 5 risks. These risks that has a level of critical and high risk become priority for mitigation plan.*

Keywords: *Risk Management, ISO 17025:2017, Analytical Hierarchy Process (AHP), Telecommunication Device Testing, BPMSG Online Software*

INTRODUCTION

The Infrastructure Assurance Unit (IAS) Telkom Bandung is a telecommunication equipment testing laboratory owned by PT Telkom Indonesia. This unit is the main laboratory used by Telkom for testing, even the Ministry of Communication and Information appoints the IAS unit as the main test center for testing and certification of telecommunications equipment because it has a good source of experts and the most complete facilities in Indonesia. To maintain the service quality and customer satisfaction of the company adhering to the International Organization for Standardization (ISO), IAS units as Testing and Calibration Laboratories must refer to ISO 17025: 2005, but in 2017 there was the development of ISO 17025: 2017 which has important changes that must be owned by IAS. Accreditation from KAN is very important for the company to continue to run its business, because if it fails, the company cannot operate for the time being. To be able to pass the Audit from the National Accreditation Committee (KAN), IAS must follow the developments of the ISO changes, one of which is the use of risk based thinking in planning and implementing actions. Therefore, according to the results of the brainstorming and interviewing from the experts, the risk assessment and implementation of risk management in the work environment of the IAS unit was considered appropriate to overcome the above problems. This research has an objective to identification the possible risk, the risk analysis and also analyze the mitigation of the risk of telecommunication-equipment test laboratory.

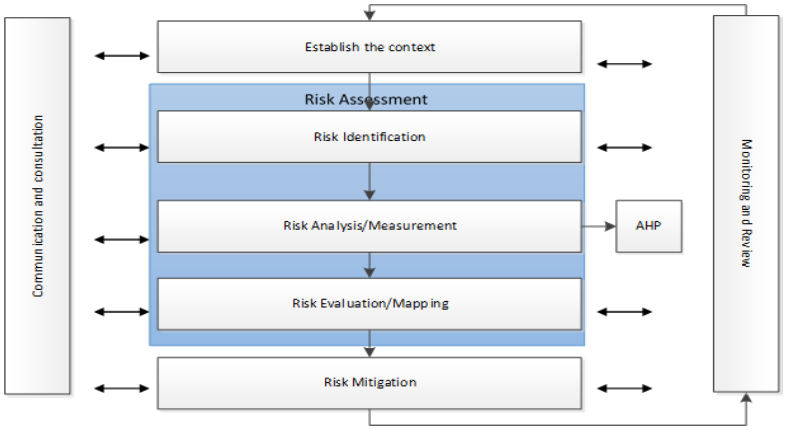

Figure 1. Conceptual Framework: ISO 31000:2009

To make risk management in telecommunication equipment testing laboratories, the above steps are needed to be able to improve performance and anticipate risks that can disrupt the stability of the company's business. The concept used is the adoption of the risk management process issued by ISO 31000: 2009 which contains the scope, definition, principles, framework, and also the process of risk management. in this study, the tools used in risk analysis are Analytical Hierarchy Process. Risk identification got from the results of observations of the possible risks that could occur as well as the results of expert interviews in the related laboratories, Risk identification process is carried out from SWOT Analysis, Brainstorming, and other research. Then the risk analysis/risk measurement uses measurement through the Analytical Hierarchy Process (AHP) approach and is measured based on its likelihood and impact, the next step is risk evaluation which contains the mapping and grouping of risks, and finally the risk treatment / mitigation stage that is making mitigation risk based on 4 methods. The methods are Avoidance, Reduction/Control, Transfer, and Acceptance. After that the next step is to analyze and make an implementation plan

LITERATURE REVIEW

According to Olsson (2002), risk is the possibility of adverse consequences of happening and risk is the uncertainty of future outcomes. In Olsson, the risk management process is discussed starting from monitoring the problem, then collecting the risks that are found in the company, then measuring the risk to the risk list, and then entering the evaluation stage whether managing, accepting, mitigating, and refusing risk, then formulating a method for monitoring the risk.

Quoted from COSO (2004), Risk management is a process carried out by corporate entities such as the board of director, management, and other personnel, in an applied in strategy setting and across the enterprise, events that may affect the entity, and manage risks to be within its risk appetite, assurance regarding the achievement of entity objectives. Risk management important to deal effectively with potential future events that create uncertainty and Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

Based on ISO 31000:2009, explains the application of risk which consists of three elements: principle, framework, and process. The principle of risk management is the basis of the risk management practice or philosophy. The framework is the arrangement of a risk management system in a structured and systematic manner throughout the organization. Process is a sequential and interrelated risk management activity. The process of the Analytical Hierarchy Process (AHP), was first developed by Thomas L. Saaty, a mathematician from the University of Pittsburg, United States in the 1970s. The use of AHP in this study is intended to calculate risk analysis. According to Saaty (2008), AHP is a method for making alternative sequences of decisions and choosing the best alternative when decision makers with multiple objectives or criteria for making certain decisions. The most important thing in AHP is the functional hierarchy with the main input of human perception which is an expert (expert judgment). With hierarchy, a complex and unstructured problem can be solved into groups, then the groups are organized into a hierarchical form. The pairwise comparison assessment procedure in AHP, refers to the assessment score that has been developed by Thomas L Saaty. The score is as follows:

Table 1. AHP Scoring

Intensity of Importance	*Definition*	*Explanation*
1	Equal Importance	Two activities contribute equally to the objective
2	Weak or slight	
3	Moderate importance	Experience and judgement slightly favour one activity over another
4	Moderate plus	
5	Strong importance	Experience and judgement strongly favour one activity over another
6	Strong plus	
7	Very strong or demonstrated importance	An activity is favoured very strongly over another; its dominance demonstrated in practice
8	Very, very strong	
9	Extreme importance	The evidence favouring one activity over another is of the highest possible order of affirmation

Reference: Saaty (2008)

Next is the preparation of paired matrices to normalize the importance of each element in each hierarchy. previously the consistency test was carried out first. The consistency test is carried out on each questionnaire / expert who assesses or gives weighting, the benchmark used is the Consistency ratio (CR) <10%. If the CR has fulfilled the requirements, then the priority is in each hierarchy which is then ended by drawing conclusions.

ISBN: *978-623-92201-0-5*

METHODOLOGY

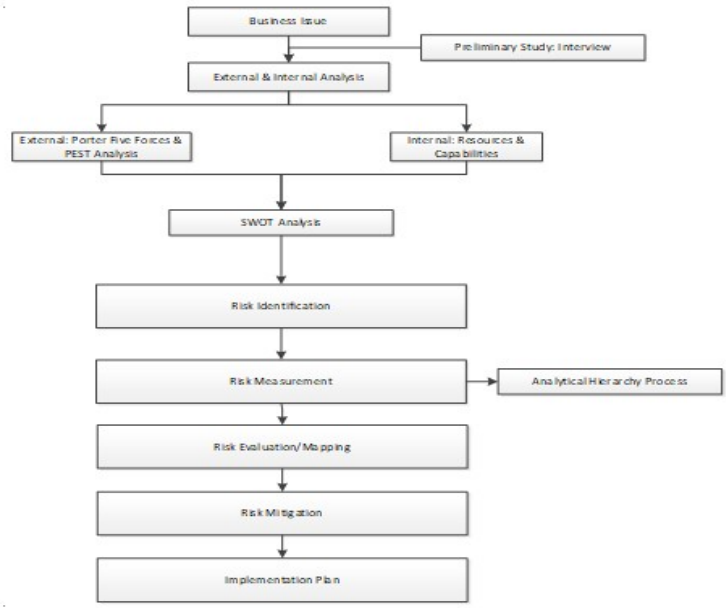

Figure 2. Research Methodology

On this project, to compile the research began from collecting and describing business problems that exist in the company, the initial process used was interviews with laboratory managers examining telecommunications equipment to develop environmental conditions and laboratories, testing processes, and analyzing both the external environment also internally from the IAS division. The external analysis used is Porter five strengths, because the author wants to know the state of the industry and competitors in the IAS Telkom environmental division. then internal analysis is carried out by searching for resources and capabilities to study the internal conditions experienced by Telkom's current IAS division. After obtaining external and internal analysis, then summarized into a SWOT analysis. This was done to find out the location of the advantages, weaknesses possessed by IAS Telkom, and the opportunities and threats possessed by the Telkom IAS division. it is useful to help writers find solutions that they have.

Next, the process of risk management process that starts with making risks collected at IAS Telkom. after that, it enters the risk management process that starts with making risk identification which contains various risks that can occur in the Telkom IAS division. basically risk identification comes from the results of internal and external analysis and the results of brainstorming with IAS laboratory managers. After the list of risk identification is formed, the next step is to create a risk measurement that uses tools AHP to determine the degree of the identified risk owned by the company. After that go to the risk evaluation stage to then mapping the risk and evaluate the level of risk contained in the risk mitigation. The last stage is making an implementation plan for the company to implement the risk management that has been made.

FINDINGS AND ARGUMENT

The findings and arguments of the work should be explicitely described and illustrated. Supporting figures, tables and images of the results (no more than two figures and two tables) may be included in the extended abstract.

Risk Identification

Based on ISO 31000:2009, Risk identification is identifying sources of risk, areas of impacts, events and their causes/consequences. , Risk identification process is carried out from SWOT Analysis, Brainstorming, and other research

Table 2. Risk Identification (Example)

No.	Risk Type	Risk Code	Risk Factor	Risk Description	Cause of Risk	Risk Impact	Source
1	Business Risk	B1	Price Competition	There is an indication of competition Price with a similar Test Lab	There is no standard tariff for testing, the Lab has the right to set their respective prices	The decline in demand testing, the transfer of Loyal Customer to a similar Test Lab, decreased revenue.	SWOT Analysis, Olsson (2002), Interview and Brainstorming with Expert, Telkom Annual Report 2018, Wiryono (2008)
2	Environmental Risk	E1	Robbery	The emergence of irresponsible outsiders taking / stealing testing devices	Lack of security or security of assets, especially outside the building	Material, data / information losses	Olsson (2002), Interview and Brainstorming with Expert, Wiryono (2008)
3	Financial Risk	F1	Late Payment	The risk of late payment being deposited by the customer	The customer pays the payment bill not according to the set time	The process of issuing a test order (SPK) to the Lab is too late so that the Lab has not been able to do the testing	Interview and Brainstorming with Expert, Mike Ogbalu III (2016)
4	Legal/Regulatory Risk	L1	International guideline rules	Guidelines for testing rules from the international world globally that make the test / system running now become obsolete	International rules or testing standards that continue to grow	Dissolution of the QA Test Lab and cessation of test services, the measuring instrument can become obsolete if the rules change	Olsson (2002), Interview and Brainstorming with Expert, Wiryono (2008), Telkom Annual Report 2018, SWOT Analysis
5	Market Risk	M1	Interest rate risk	Risks that arise when there are fluctuations in interest rates	Volatile interest rate	Fluctuating interest costs make the money issued uncertain	Olsson (2002), Telkom Annual Report 2018
6	Operational Risk	O2	Non-Compliance with SOP	The non-compliance of staff in undergoing SOPs is valid for various reasons	Lack of awareness of staff and punishment that is less strict	Overlapping the sequence of processes that confuse data recording by other staff	Olsson (2002), Interview and Brainstorming with Expert,Wiryono (2008), SWOT Analysis
7	Reputational Risk	R2	Customer Complaints	Customer complaints are due to measurement accuracy and the progress obtained by the customer is very minimal or due to late testing	There is no 2-way monitoring system from the customers and testers, so customers do not know the testing progress and the number of queues that must be waited for	Laboratory credibility has dropped	Olsson (2002), Interview and Brainstorming with Expert, Mike Ogbalu III (2016), Wiryono (2008)

From the analysis of risk identification, IAS has 29 risk factors. Risks are obtained from observations, brainstorming with laboratory managers, interviews, SWOT analysis, and other research. of these risks, we found 7 risk types including Business risk, Environmental Risk, Financial Risk, Market Risk, Operational Risk, Reputational Risk, and Legal / Regulatory Risk.

Risk Analysis

Based on ISO 31000: 2009, after identifying risks, the next step is risk analysis / measurement. In this study, AHP was used as a tool to make measurements of the risk identification that had been made. the study uses online software assistance from Business Performance Management Singapore (BPMSG).

Table 2. Risk Analysis (Example)

Risk Category		Risk Factor			Likelihood Level		Impact Level	
Business Risk	0,156	Price Competition	**B1**	0,013	0,007	Low	0,007	Moderate
		New Competitor	**B2**	0,029	0,018	Moderate	0,014	High
		Revenue Target	**B3**	0,114	0,052	Moderate	0,064	High
Environmental Risk	0,030	Robbery	**E1**	0,005	0,002	Low	0,003	Very Low
		Potential Disaster	**E2**	0,006	0,002	Very Low	0,003	Low
		Waste Problem	**E3**	0,019	0,010	Moderate	0,007	Low
Financial Risk	0,104	Late Payment	**F1**	0,078	0,036	High	0,037	Moderate
		Limitations of Funding	**F2**	0,026	0,012	High	0,013	Moderate
Legal/Regulatory Risk	0,349	International guideline rules	**L1**	0,087	0,039	Low	0,038	Very High
		KEMENKOMINFO testing guideline rules	**L2**	0,262	0,119	Low	0,137	Very High
Market Risk	0,021	Interest rate risk	**M1**	0,007	0,003	Very Low	0,003	Very Low
		Foreign Exchange Risk	**M2**	0,014	0,007	Low	0,006	Low
Reputational Risk	0,280	Quality of Service	**R1**	0,070	0,035	High	0,033	High
		Customer Complaints	**R2**	0,210	0,107	Moderate	0,103	Very High
Operational Risk	0,060	Low rejuvenation of tools	**O1**	0,001	0,001	High	0,001	Low

Based on risk analysis from Business risk, the biggest risk factor is the target revenue; for the biggest environmental risk is the problem; then for financial risk the largest weight is on the late payment; Legal / Regulatory risk, the greatest weight in the guidelines; then for the risk market; for the biggest weighted reputation risk in customer complaints; and for operational risk is under performance assessment. Risk analysis and measurement is carried out by calculating the Analytical Hierarchy Process (AHP) using BPMSG Online Software.

Risk Eevaluation

According to ISO 31000, risk evaluation is a process to help decision making based on the results of risk analysis and measurement. This process helps in classifying which risks require the highest priority to solve the problem. This process is carried out by comparing the level of risk that has been done in the previous process, then mapped.

ISBN: *978-623-92201-0-5*

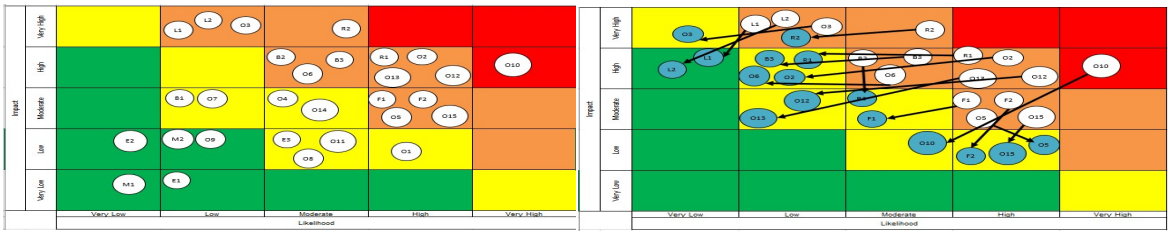

Figure 2. Risk Mappig and Mitigation

Based on the results of risk mapping, the risk that has a risk level that is critical amounts to 1 risk, then the risk that has a high risk level is 15, then the risk has a moderate risk level of 8. Finally, the one who has a risk level low is 5 risks. From the 29 risk factors that are owned, the risks made by further mitigation plans are 16 risks which got critical and high risk (marked in red and brown). Critical is Delay testing, High risks are Non Compliance with SOP, Website system down, data inconsistency, Quality of Service, Late Payment, Limitation of Funding, Rapid Development in Technology, New types in device testing, customer complaints, new competitor, revenue target, HSE, under performance assessment, international guideline rules, Kominfo guideline rules.

Risk Treatment/Mitigation

According to ISO 31000, risk evaluation is a process to help decision making based on the results of risk analysis and measurement. This process helps in classifying which risks require the highest priority to solve the problem. This process is carried out by comparing the level of risk that has been done in the previous process, then mapped. The next step is treatment / mitigation of risks that have been classified. Based to COSO (2004) there are four methods of risk mitigation which, such as:

- Accept = accepting a risk by not taking significant action that requires large resources.
- Avoid = eliminate (get out of situation)
- Reduce = minimize risk as optimally as possible without eliminating the company's opportunity to gain profits, done by reducing likelihood or impact
- Share/Transfer = partner with someone to overcome the risk

Table 3. Risk Mitigation (Example)

Level of Risk		Risk Level	Risk Code	Risk Factor	Risk Mitigation	Description
Likelihood	Impact					
Very High	High	Critical	O10	Delay Testing	Reduce	Monitoring is strictly through the OTR website and ensures the SOP is running, customer education
High	High	High	O2	Non-Compliance with SOP	Reduce	Briefing, Training and affirmation of rules with reward and punishment
			O12	Website System Down	Transfer	The appointment of the Task Force (Satgas) in website area
			O13	Data inconsistency	Reduce	TTH and OTR website integration. TTH-OTR synchronization and monitoring according to SOP
			R1	Quality of Service	Reduce	Maintain customer satisfaction, increase customer experience
High	Moderate	High	F1	Late Payment	Reduce	Customer Education, applies late penalties
			F2	Limitations of Funding	Reduce	Optimization of existing equipment
			O5	Rapid Development in Technology	Reduce	Assessment Technology, Vendor Update, and Strengthen Collaboration with IRS (Infrastructure Research)
			O15	New types in device testing	Reduce	Establishment of a research and development team to keep up with developments in technology in telecommunications
Moderate	Very High	High	R2	Customer Complaints	Reduce	Improve customer service, communicate two-way progress testing
Moderate	High	High	B2	New Competitor	Reduce	Collaboration with the Allied Test Lab and the establishment of a Test Lab association
			B3	Revenue Target	Reduce	Increased testing rates that have not been revised since 2016
			O6	Health Safety Environment	Transfer	Implementation of K3 and Security Hardening

CONCLUSIONS

From the results of observations and interviews, the Telkom Bandung IAS work unit still has many potential risks and requires good and well implemented risk management. Although it is the market leader with the most complete customer base and facilities and is directly appointed by the government, this unit must improve its services and maintain its quality to increase the performance and sustainability of business. The following is the solution to this research. From risk identification process, The IAS Telkom Bandung work unit has 29 risk factors. Risks are obtained from observations, brainstorming with laboratory managers, interviews, SWOT analysis, and other research. of these risks, we found 7 risk types including Business risk, Environmental Risk,

Financial Risk, Market Risk, Operational Risk, Reputational Risk, and Legal / Regulatory Risk. Based on the results of risk analysis, the risk that has a risk level that is critical amounts to 1 risk, then the risk that has a high level is 15, then the risk has a moderate risk level of 8. Lastly, the risk with risk level low is 5 risks. Risk mitigation is classified into 4 groups, namely avoid, reduce, transfer, and accept. From the 29 risk factors that are owned, the risks made by further mitigation plans are 16 risks. These risks are 1 risk that has a critical risk level, and 15 risk that has a high risk.

REFERENCES

COSO. 2004. Enterprise Risk Management - Integrated Framework (Executive Summary andFramework). New Jersey: Committee of Sponsoring Organization of the Treadway Commission

ISO.2009.31000:2009 Risk Management-Principles and Guideline. Geneva, Switzerland: International Organization for Standardization

Mike Ogbalu III. Inherent Risk in Global Remittances. West African Institute for Financial and Economic Management(WAIFEM)

Olsson Carl .2002. Ebook Risk Management in Emerging Market. Great Britain. Financial Time Prentice Hall

Saaty, T.L.2008. Decision Making with The Analytic Hierarchy Process. Int. J. Services Science, Vol. 1, No. 1, pp 83-98