Volume. 19 Issue 3 (2022) Pages 508-521
AKUNTABEL: Jurnal Akuntansi dan Keuangan
ISSN: 0216-7743 (Print) 2528-1135 (Online)

Operational risk analysis with approach enterprise risk management

Dewi Cahyani Pangestuti[1]✉, Heni Nastiti[2], Renny Husniati[3]
Fakultas Ekonomi dan Bisnis Universitas Pembangunan Nasional Veteran, Jakarta.

Abstract

The more risk management is used in a company, the more it will increase the value of the company and also affect how much money the company makes. Risk management, carried out by company managers, is the company's way of anticipating the risks that occur. The purpose of this study is to recognize, identify, assess, and control operational risks of PT. Indosat Ooredoo Tbk. in the Network Operation Center division. The research method used is risk analysis with Enterprise Risk Management. The conclusions in this study are that 49 risks have been identified, including 10 risks that include acceptable or acceptable risk criteria, 32 risks that include supplementary issue risk criteria or risks that require action if the company's resources are available, and 7 risks that include risk issues or risk criteria that immediately need to be managed and reduced. Operational risks to PT. Indosat Ooredoo, like the risk of thuggery in the Regional Operation department, have a big effect and are likely to happen. Meanwhile, the risk is the least in the Partner Management department.

Key words: Enterprise risk management; risk operational

✉ Corresponding Author
Email Address: dewichepe@upnvj.ac.id
DOI: 10.29264/jakt.v19i3.11795

INTRODUCTION

The amount to which a company's corporate strategy results differ from those defined in its corporate objectives, or the extent to which they fail to reach these objectives (using a "downside risk" measure), is referred to as enterprise risk. The strategy adopted to attain these business goals has a risk profile that stems from the numerous elements that may have an impact on the actions, procedures, and resources used to implement the strategy. A variety of external and internal circumstances might cause a company's actions to produce results that differ from those outlined in its corporate objectives. Some external factors are related to those in the market where a company competes, such as new entrants, changing consumer tastes, or new product innovations. Other external factors, like changes in the economy, capital, and financial markets, as well as changes in the political, legal, technological, demographic, and other contexts, emerge from a larger context. Although active managers perceive the risk profile of a specific strategy to be excessively high, most of these factors are beyond management's control (Callahan, 2017; ERM, 2004; Pangestuti & Hunah, 2021).

The Sarbanes-Oxley Act of 2002 (SOX), for example, is frequently cited as having had a substantial impact on transforming the face of risk management (Beasley et al., 2005; Pagach & Warr, 2010). Rating agencies have also aided in bringing ERM to light; in May 2008, Standard & Poor's (S&P, 2008) Ratings Services announced its intention to integrate ERM assessment in non-financial firm ratings. And, since corporations face a greater range of risks as a result of globalization, industry consolidation, and deregulation (Hoyt & Liebenberg, 2011),ERM has emerged as a coping mechanism for the constraints imposed on businesses to be more efficient. Despite its growing popularity, ERM knowledge is riddled with discrepancies and uncertainties. As the importance of ERM grew, several frameworks arose to assist businesses in implementing ERM. The large number of frameworks established contributes to a general lack of clarity about the key elements of ERM. While the core notions of ERM are similar, there is evident discontent with existing ERM guidelines. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM framework, according to Beasley, Branson, and Hancock (2010), is one of the most mentioned ERM frameworks (ERM, 2004).
The risks arising in the company both externally and internally come from the movement of the mobile industry and the increasing number of competitors. The way a company prepares for risks is through risk management, which is done by company managers. Risk management is a method or system of managing risk and protecting the company's property, property rights, and profits carried out based on the possibility of a loss due to risk. Risk management in the company is carried out with several activities, namely: recognizing and identifying risks, measuring risks, mapping risks in harmony with the magnitude or absence of potential risks and impacts caused, controlling risks, identifying risks that are and will be faced by the company, and finally monitoring risks in every business activity or activity (Jankensgrd 2016; Pangestuti & Hunah, 2021).

The more risk management is used in a company by managing the risks, the more valuable the company will be and the more the company will make. PT. Indosat is also one of the companies that are very concerned about the company's risks , (Chaidir et al., 2020). This is evidenced by the existence of divisions that control management risk. Management or control of risk is needed so that these risks can have a positive impact, which can satisfy the company's consumers, because the risks arising in this company can have a positive impact on the level of quality of service provided to consumers, especially in network systems. The purpose and focus of this study are to recognize and analyze operational risk factors, identify operational risk factors, and handle or control risk factors on an ongoing basis at PT. Indosat to provide a better quality of service to consumers in terms of networking systems.

The main goal of every company that produces goods and services is to prosper so that its stakeholders will be happy. The same goes for other companies. PT. Indosat Tbk, engaged in telecommunications, has a large capital base to carry out its business activities in the field of telecommunications and digital. PT. Indosat is committed to providing the best possible service for its stakeholders, especially shareholders, which is the main goal of PT. Indosat. As is the case with other companies, Indosat also always controls the risks in its business so as not to cause large losses for the company. However, in reality, not a few employees of PT. Indosat do not obey and follow standards of procedure (SOP) while working, so this has the potential to cause losses for the company. Losses above $5 billion have been experienced by Indosat, specifically in 2014 because of Indosat's network problems for almost one day, and this caused customers to feel the impact of complaining to Indosat Ooredoo.

Then, after the problem was evaluated, analyzed, and identified, the root cause was found, namely that there were Indosat Ooredoo employees who violated the SOP. For violations that have been committed, the employee was sanctioned with a warning letter, and some of them were also given verbal reprimands. Therefore, so that the problem does not reoccur, PT. Indosat Ooredoo anticipates improvements to the SOP and continues to increase supervision of every business activity. PT Indosat Ooredoo also mitigates by asking for input or advice from internal and external parties (indosatooredo.com). Based on the above problems, the recommendation of this study is to identify, assess, and control operational risks of PT. Indosat Ooredoo Tbk. in the Network Operation Center division using the enterprise risk management method.

METHOD

Based on the purpose of this study, which is to identify, assess, and control operational risks of PT. Indosat Ooredoo Tbk. in the Network Operation Center division, The research method used is qualitative. This study was conducted in the year 2020. The method of collecting data in this study is through questionnaires, interviews, and focus group discussion (FGD). The questionnaire method is a data collection technique that involves asking questions to competent employees in the Network Operation Center division. The interview method is a data collection technique that involves getting information from question-and-answer activities and giving it directly to Network Operation Center employees. While FGD is a technique of collecting data through the formation of groups in each department to know the magnitude of the effect or impact and any possible risks that may occur, As for the stages in the analysis with Enterprise Risk Management on the operational risks of PT. Indosat Ooredoo Tbk., in the Network Operation Center division, it is carried out as follows:

Risk Identification

Risk identification is the activity of recognizing and identifying events that are considered to hinder the achievement of company goals or objectives (Roy, 2020). This risk identification process is carried out systematically and structured, analyzed in depth, and must be able to reach all risks that are within the control of the Network Operation Center Division of PT. Indosat Ooredoo Tbk. Brainstorming is a tool used to identify risks by asking every employee in each related department to record the risks that have occurred and those that will occur. Then there is also the risk breakdown structure (RBS), which directs employees to arrange in order the most important risk factors and their consequences or impacts, from the largest to the smallest.

Measuring Risk

To know how likely or possible the risk is and the impact of the risk, all risks in each department will be measured. In the measurement of risk, things that need to be agreed upon in advance are the conversion of the size of the likelihood (probability) and the impact of the risk to be used. The likelihood of such a risk is expressed in percentage form (Tarigan et al., 2020). Then, the likelihood measurement is converted to a quantitative level scale, which is from 1 to 5. Here is a table of likelihood sizes:

Table 1.
Probability Level

Incident	Likelihood of Occurrence (%)	Event information in 1 year
Seldom	Possibility to occur when conditions are not normal, it's possible≤ 20	1 - 2 times
Chances of Happening	Likely to happen at some time, likely$20 \leq X \leq 40$	3 - 4 times
Medium Chance	Could happen at some time, maybe $40 \leq X \leq 60$	5 - 6 times
Big opportunities	In many circumstances it will be possible, the possibility $60 \leq X \leq 80$	7 - 8 times
Almost Sure	Can happen in many situations or circumstances, the possibility is $80 \leq X \leq 100$	> 8 times

How big is the impact caused by the event (if it occurs) on the company's goals or objectives, meaning that the impact is related to the target? Therefore, the magnitude of the impact must be stated using the same measure. The Likert scale is used to measure the instrument by giving a score in 5 categories, namely:

Table 2.
Impact Level

Result Score	Financial Consequences	Consequences on Work Safety	Consequences on Company Image
1= Not Significant	Very small loss	Accidents at work without a doctor's help	Image bad for employees' internal environment
2= Small	Minor loss	Accidents at work assisted by a general practitioner	Image bad for the owner
3= Medium	Medium loss	Work accidents assisted by specialist doctors	Image bad on local media
4= Big	Big loss	Work accidents assisted by specialist doctors as well as hospitalization	Image bad on national media
5= Very Big	Huge loss	A very serious work accident and can be life-threatening	Image bad on international media

Therefore, the multiplication of opportunities and the consequences or impacts of an event is a way to measure and manage unwanted risks. The formula is as follows: P: Possibility, D: Impact or effect

$$\boldsymbol{L = p\ x\ D}$$

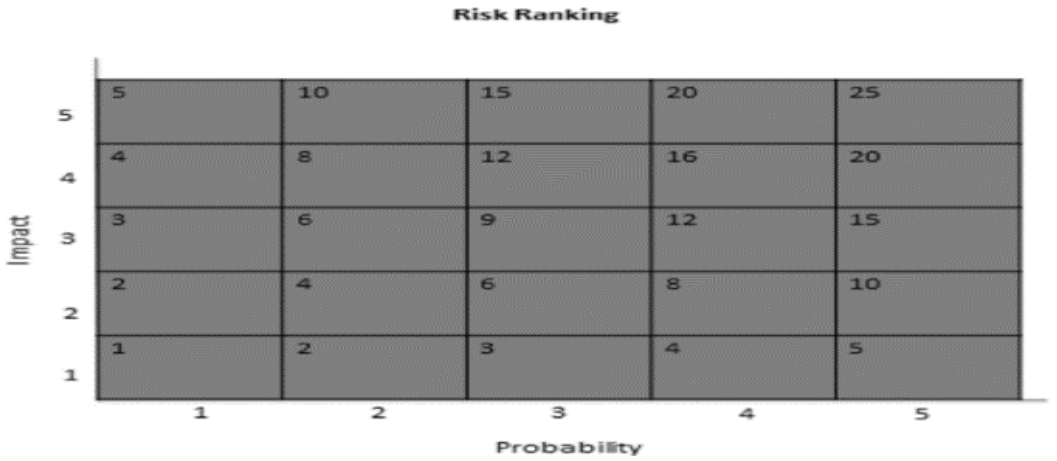

Figure 1.
Classification of Risk Measures

Risk Analysis

Analyzing the consequences and possibilities of all risks that can interfere with the realization of goals or objectives in the Network Operation Center Division of PT. Indosat Ooredoo Tbk and also providing data to help evaluate and know how to treat risk is the purpose of risk analysis. Risk analysis includes considering and combining estimates of consequences and likelihood (likelihood of occurring). Risk analysis depends on the availability of risk information and data. This analysis can be semi-quantitative, quantitative (specific indications of risk levels), qualitative (general indications of risk levels), or a combination of the three (Afefy, 2015).

Risk Evaluation

Comparing the level of risk obtained during the analysis process with predetermined risk standards or criteria is an activity to evaluate risk. After evaluating the risk, a priority list of risks is obtained for further action. Furthermore, the results of the risk analysis will be validated by the highest authority as the risk manager, (Malhotra, 2015). The results of the validation will then be used as the basis for determining the plan for the stages of the control method to minimize the possibility of risk occurrence and reduce the impact caused by the risk. The following is a classification of risk categories:

Table 3.
Risk Category Classification

Category Tiers	Score	Information
Low	$X.Y \leq 4$	No action required (Acceptable)
Currently	$4 < X.Y. \leq 8$	If company resources are available, it is recommended to take action (Supplementary Issue)
Tall	$8 < X.Y. \leq 12$	Action is needed to manage risk (Issue)
Extreme	$12 < X.Y. \leq 25$	Urgently needed to manage risk (Unacceptable)

RESULT AND DISCUSSION

Risk Identification

The process of operational risk identification has been carried out through the dissemination of questionnaires and interviews at every department in the company, PT. Indosat Ooredoo Tbk. The recruitment of informants in each department is done by taking as many as 6 respondents who are representatives of each department to fill out a risk identification questionnaire owned by each department. The sampling technique used is convenience sampling, which is the filling out of questionnaires by employees who are willing to volunteer. Based on the answers to the different questionnaires, the characteristics of the people who filled them out are split into several groups. These groups are based on their position, the amount of training they've had, how long they've been working, and what they've studied.

Table 4.
Operational Risk Identification of PT. Indosat Ooredoo Tbk

Risk Type	Risk
Consumer Front Office	Submitting customer profile information to unauthorized parties Travel risks for teams of shift employees who come home late Employees often share usernames & passwords with inappropriate employees The problem alarm was notified late due to the technician falling asleep Wrong explanation of root cause information from technical department to CCS
Regional Operation (EJBN Operation, CJWJ Operation, Jabodetabek Operation, Kalisula and Papua Operation, and Sumatra Operation)	The lack of technical human resources causes BTS not to be controlled and handled properly Complaints from customers due to bad signal There is the theft of generators, batteries, and antennas so that service to consumers is hampered and the signal is bad There is no vehicle for operations resulting in delays in resolving complaints from customers The resolution of complaints from customers is slow There is thuggery The unavailability of stock modules/devices causes the BTS and MSC (Mobile Switching Center) devices to be unable to repair Natural disasters
Transmission Operation	Marine cable break Fiber optic cable broke due to hoeing Broken coaxial cable due to flood The loss of the satellite from orbit, lightning struck the VSAT link and bad weather caused slow access to ATMs at banks Lightning strikes the VSAT link and bad weather causes slow ATM access at the bank
Internet Protocol/Multi Packet Label System Operation	Destination IP error committed by Indosat vendors in their work on the MPLS system of the Indosat network so that Indosat's data access is down

Risk Type	Risk
	Error in changing the network layer so that the MPLS network suddenly goes down
	Employee errors in routing and layer settings on the network cause data network disconnection
	Network backbone Indosat international down causes access difficulties for customers
	Indosat network disconnection due to employee error
Access Operation	Lack of human resources as equipment and technology increase
	Work environment security must be considered because laptops/cellphones are often lost
	Lack of operational vehicles
	The lack of computers/laptops for outsourced employees causes sluggish performance
	It is necessary to pay attention to the risk of Human Error and Employee Accident
Civil, Maintenance, and Electrical Operation	The frequent shutdown of PLN causes the BTS and BSC devices to go down
	Late check of generator
	Damage to the AC for the inner site (MSC, BSC, and BTS)
	There is still a lack of employee skills regarding air conditioning, generators, and batteries
	Land lease contract for tower placement is not extended
	To turn on the generator must be manual because it does not turn on automatically
Core Operation	Incorrect configuration on PC, CS, and IN-VAS systems
	When onsite work to MSC there is a hardware action error
	Giving users to outsourced employees does not match the level
	Still lack control over vendors
	Provision of SMS and customer voice by employees is done without permission from the company and the police
Configuration Management	Server devise disconnect
	The server has a virus
	The bad or broken server
	Distributing the server admin password to irresponsible parties
	It takes a long time because the server modules and spare parts come from abroad
Partner Management	The approach taken by Indosat vendors to employees is through gifts to facilitate collaboration
	Cooperation between employees and vendors to facilitate maintenance reports
	Penalty to undisciplined vendors reduced by employees
	Employees are not objective in determining the winning vendor
	Employees get vendor prizes for winning contract tenders

Measurement or Risk Assessment

A risk measurement or assessment is an activity that measures or assesses the level of likelihood and magnitude of the impact of risk. Because of the different types of work and responsibilities owned

by each department, risk measurements are carried out differently according to their respective departments. Based on table 1, we are informed about events, the likelihood of events, and how many occur in a year. Then, the data will reveal what the odds score is. So, based on the results of the processed data, a risk assessment can be given in each department.

Recapitulation of measurement results or operational risk assessment of PT. Indosat Ooredoo is as follows:

Table 5.
Recapitulation of Measurement Results or Operational Risk Assessment Indosat Ooredoo

Risk Type	Risk	Impact	Possibility
	Submitting customer profile information to unauthorized parties	Big	Seldom
	Travel risks for teams of shift employees who come home late	Currently	Medium chance
Front Office	Employees often share users and passwords with inappropriate employees	Small	Big opportunities
	The problem alarm was notified late due to the technician falling asleep	Small	Big opportunities
	Mistakes in explaining root cause information from technical department to CCS	Small	Medium chance
	Lack of technical human resources	Currently	Medium chance
	Complaints from customers due to bad signal	Big	Medium chance
	The theft of generators, batteries, and antennas	Big	Seldom
	There are no vehicles for operation	Small	Medium chance
Regional Operation	The resolution of complaints from customers is slow	Big	Medium chance
	There is thuggery	Currently	Almost sure
	The unavailability of stock modules or devices causes BTS and MSC devices to not be repaired	Big	Likelihood of happening
	Natural disasters	Very large	Seldom
	Marine cable break	Big	Likelihood of happening
	Fiber optic cable broke due to hoeing	Big	Likelihood of happening
Transmission Operation	Broken coaxial cable due to flood	Big	Likelihood of happening
	Missing satellite from orbit	Very large	Seldom
	Lightning strikes the VSAT link and bad weather causes slow ATM access at the bank	Currently	Likelihood of happening
	Destination IP error committed by Indosat vendors in their work on the MPLS system of the Indosat network so that Indosat's data access is down	Big	Likelihood of happening
	Error in changing the network layer so that the MPLS network suddenly goes down	Big	Likelihood of happening
	Employee errors in routing and layer settings on the network cause data network disconnection	Big	Likelihood of happening
Internet Protocols/	Network backbone Indosat international down causes access difficulties for customers	Big	Seldom
Multi Packet Label System	Indosat network disconnection due to employee error	Very large	Seldom
	Lack of human resources as equipment and technology increase	Currently	Big opportunities
	Work environment security must be considered because laptops/cellphones are often lost	Small	Big opportunities

Risk Type	Risk	Impact	Possibility
	Lack of operational vehicles	Small	Medium chance
Access Operation	The lack of computers/laptops for outsourced employees causes sluggish performance	Small	Big opportunities
	It is necessary to pay attention to Human Error and Employee Accident	Small	Big opportunities
Civil	The frequent shutdown of PLN causes the BTS and BSC devices to go down	Currently	Big opportunities
Maintenance, & Electrical Operation	Late check of generator	Small	Medium chance
	Damage to the AC for the inner site (MSC, BSC, and BTS)	Currently	Likelihood of happening
	There is still a lack of employee skills regarding air conditioning, generators, and batteries	Currently	Likelihood of happening
	Land lease contract for tower placement is not extended	Currently	Likelihood of happening
	To turn on the generator must be manual because it does not turn on automatically	Currently	Likelihood of happening
	Incorrect configuration on PC, CS, and IN-VAS systems	Small	Medium chance
	When onsite work to MSC there is a hardware action error	Currently	Likelihood of happening
	Giving users to outsourced employees does not match the level	Big	Likelihood of happening
Core Operation	Still lack control over vendors	Small	Medium chance
	The provision of SMS and customer voice by employees is carried out without the permission of the company and the police	Big	Seldom
	Server device disconnect	Small	Medium chance
	The server has a virus	Small	Likelihood of happening
Configuration-on Management	The bad or broken server	Currently	Likelihood of happening
	Distributing the server admin password to irresponsible parties	Big	Seldom
	It takes a long time because the server modules and spare parts come from abroad	Big	Likelihood of happening
	The approach taken by Indosat vendors to employees is through gifts to facilitate cooperation	Big	Seldom
	Cooperation between employees and vendors to facilitate maintenance reports	Currently	Likelihood of happening
	Penalty to undisciplined vendors reduced by employees	Big	Seldom
	Employees are not objective in determining the winning vendor	Big	Seldom
	Employees get vendor prizes for winning contract tenders	Big	Seldom

Table 6.
Operational Risk Priority Level PT. Indosat Ooredoo Tbk

Priority Level	Risk	Risk Type
Level I (Extreme)	The existence of thuggery	Regional Operation
Level II (Tall)	Travel risks for teams of shift employees who come home late	Front Office
	Lack of technical human resources	Regional Operation
	Complaints from customers due to bad signal	
	The resolution of complaints from customers is slow	
	Lack of human resources as equipment and technology increase	Access Operation
	The frequent shutdown of PLN causes the BTS and BSC devices to go down	Civil, Maintenance, and Electrical Operation
Level III (Currently)	Employees often share users and passwords with inappropriate employees	Front Office
	The problem alarm was notified late due to the technician falling asleep	
	Mistakes in explaining root cause information from technical department to CCS	
	There are no vehicles for operation	
	The unavailability of stock modules or devices causes BTS and MSC devices to not be repaired	Regional Operation
	Natural disasters	
	Marine cable break	
	Fiber optic cable broke due to hoeing	
	Broken coaxial cable due to flood	
	Missing satellite from orbit	Transmission Operation
	Lightning strikes the VSAT link and bad weather causes slow ATM access at the bank	
	Destination IP error committed by Indosat vendors in their work on the MPLS system of the Indosat network so that Indosat's data access is down	Internet Protocols/ Multi Packet Label System
	Error in changing the network layer so that the MPLS network suddenly goes down	
	Employee errors in routing and layer settings on the network cause data network disconnection	
	Indosat network disconnection due to employee error	
	Work environment security must be considered because laptops/cellphones are often lost	
	Lack of operational vehicles	
	The lack of computers/laptops for outsourced employees causes sluggish performance	
	It is necessary to pay attention to Human Error and Employee Accident	Access Operation
	Late check of generator	
	Damage to the AC for the inner site (MSC, BSC, and BTS)	
	There is still a lack of employee skills regarding air conditioning, generators, and batteries	
	Land lease contract for tower placement is not extended	
	To turn on the generator must be manual because it does not turn on automatically	Civil, Maintenance, and Electrical Operation
	Incorrect configuration on PC, CS, and IN-VAS systems	
	When onsite work to MSC there is a hardware action error	
	Giving users to outsourced employees does not match the level	
	Still lack control over vendors	Core Operation
	Server device disconnect	Configuration Management
	The bad or broken server	
	It takes a long time because the server modules and spare parts come from abroad	

Priority Level	Risk	Risk Type
	Cooperation between employees and vendors to facilitate maintenance reports	Partner Management
Level IV (low)	Submitting customer profile information to unauthorized parties	Front Office
	The theft of generators, batteries, and antennas	Regional Operation
	Network backbone Indosat international down causes access difficulties for customers	Internet Protocols/Multi Packet Label System
	The provision of SMS and customer voice by employees is carried out without the permission of the company and the police	The Core Operation
	Servers got a virus	Configuration Management
	Distributing the server admin password to irresponsible parties	
	The approach taken by Indosat vendors to employees is through gifts to facilitate cooperation	
	Penalty to undisciplined vendors reduced by employees	
	Employees are not objective in determining the winning vendor	
	Employees get vendor prizes for winning contract tenders	Partner Management

Handing and Controlling Risk

After handling risk, the risk evaluation stage is carried out in each department in the network operation section of PT Indosat Ooredoo Tbk. Using a number of factors, including interviews with managers and supervisors in each department, an evaluation is made of the risk of problem categories and additional problems, such as the following:

Front Office

Travel risks for a team of shift employees who go home at night Handling this risk is done by providing instructions, directions, and decisions for employees who get shift 2 (14:00 to 22:00) and who return home at night if conditions or situations such as the weather do not allow them to keep working until shift 3 (22:00 to 06:00) replaces employees who get shift 3. The next day, the replaced employee will work two shifts, so the risk can be avoided.

The alarm problem was detected too late, due to the technician's sleeping. To address this risk, instructions or work guidelines are developed that penalize those who sleep in the workplace both during working hours and when not working (off).

Employees frequently share user names and passwords with coworkers. Handling this risk entails developing regulations and SOPs in the relevant departments that require employees not to share users and passwords carelessly with other employees. There are also consequences for those who violate or reprimand those who do it once, as well as sanctions with a warning letter (SP) for those who do it repeatedly.

Error in the explanation of root cause information from the technical section to CCS. This risk handling is done by creating a facility or two weekly meetings with the CCS team (Customer Contact Services) to be able to solve problems arising from customer complaints in the network division and identify root cause information with simple methods to facilitate the understanding of the CCS team. The CCS team also compiled a report on customer complaints about technical teams both in writing and orally so that there is synchronization between both parties, and the CCS team also provides knowledge sharing.

Regional Operation

Customer complaints due to bad signals. Handling this risk is done with several things, namely:
In densely populated areas, urban technical teams will test signal strength with BER TEST tools and data performance with Oklahoma Speed Test, and may recommend the installation of repeaters or signal amplifiers;
If there is a bad signal in the building, it will be given the addition of a repeater or indoor BTS; and
The addition of BTS is done so that the planning team and project can add BTS and outdoor BTS in small urban areas that, from the business side, are found by potential customers.

There's thuggery. Handling this risk is done in several ways, namely:
Work with the police to monitor, control, and take action if thugs try to extort money from you;

Approach groups that affect the area to work together to maintain the safety and comfort of employees; Provide an opportunity for thugs there to become security officers in the region.

The resolution of complaints from customers has been slow. Handling this risk is done by creating a rapid reaction team. If there are complaints from customers, especially those who are close to the office, they will be immediately addressed.

Lack of HR technicians Handling this risk is done by providing training and sharing knowledge with the team to handle technical problems or by preparing a new employee's additional budget.

There are no vehicles for operation. Handling this risk is done by maximizing existing operational cars for distant areas. As for the area where the employee's motorcycle is most often used, the company can claim the costs.

The inability to obtain module or device stock results in irreparable BTS and MSC devices. This risk handling is done by providing the indicated information to the division and department to immediately order the module to the vendor as specified so that the device can be repaired.

Natural disasters. Handling this risk is done by preparing spare parts at the head office so that when there is a natural disaster, they can immediately make a change of parts.

Transmission Operation

Fiber optic cables are broken due to being hoed. Handling this risk is done through cooperation between the transmission operation department of PT. Indosat, the PU office in the province or city, and PDAM, with the aim of having information submitted to the Indosat team when there is a soil or road excavation.

Breaking of the Sea Cable Line Handling this risk is done through cooperation between PT. Indosat Ooredoo Tbk, TNI AL, and Polair with the aim of monitoring, controlling, and inspecting the sea cable line owned by PT. Indosat with TNI AL and Polair.

the breakup of the coaxial cable due to flooding. Handling this risk is done in the form of cooperation between the departments related to the SAR team of PT. Indosat, with the aim that when there is a coaxial cable that breaks, it can be immediately handled.

loss of a satellite from its orbit. Handling this risk is done by transferring the potential losses of the company to insurance companies, commonly referred to as "risk transfer methods."

Lightning struck the VSAT link, and the bad weather caused slow ATM access at the bank. Handling this risk is done by adding anti-lightning devices in every building that has VSAT wiring.

IP/MPLS Operation

Indosat vendors make IP destination errors while working on the Indosat network's MPLS system, causing Indosat data access to fail. Handling this risk is done by showing the SOP and providing information about the impact that can occur before the vendor does his work. Also, the technical party must keep an eye on the vendor while it works, and when it's done, the vendor must check to see if there was any damage to the network or data.

Employee errors in routing settings and network layers cause the data network to disconnect. Handling this risk is done by creating an SOP for each employee, and if there are new employees, they must be guided and supervised by senior employees.

an error in changing the network layer so that the MPLS network goes down suddenly. This risk handler is done by creating an SOP for each employee, and if there are new employees, they must be guided and supervised by senior employees.

The breakup of Indosat's network was due to employee error. Handling this risk is done by creating an SOP for each employee, and if there are new employees, they must be guided and supervised by senior employees.

Access Operation

Lack of human resources while increasing devices and technology. Handling this risk is done by providing training and sharing knowledge with the team to handle technical problems and cooperate with regional teams so that problems in the region can be directly addressed by regional teams. Then it was also mentioned that the division prepares a budget for the addition of new employees.

The safety of the work environment must be considered because laptops and mobile phones are often lost. To deal with this risk, employees are told that ID cards can't be lent to anyone and that they need to follow the rules. Employees are also told to keep their personal items, like laptops and cellphones,

safe, especially when there are meetings or activities outside of the office, and suspicious people, let alone unknown people, are kept an eye on.

It is important to consider human error and employee accidents. Handling this risk is done by organizing training, sharing knowledge, refreshing through family gatherings and other equality events, and specifically for accident employees, forming a team in collaboration with Indosat's K3 team to provide warnings to comply with applicable SOPs so that work accidents can be avoided.

Lack of operational vehicles. The best way to deal with this risk is to use as many operational vehicles as possible and use the remote when work isn't urgent.

The lack of computers or laptops for outsourced employees leads to sluggish performance. Handling this risk is done by trying to get every OS employee to receive a new or used computer and enter into the division budget for laptop procurement.

Civil, Maintenance, and Electrical (CME) Operation

PLN's frequent outages cause problems with both BTS and BSC devices. Handling this risk is done through a form of cooperation between PT. Indosat and PLN. When there is a power outage plan or when doing power plant work, PLN will immediately inform Indosat to prepare alternative tools.

late checking the generator. This risk handling is done by making SOPs for all technical teams, where the technical team must always check the availability of generator sets and batteries.

To turn on the generator requires a manual because it does not automatically turn on. This risk handling is done by making SOPs for all technical teams, where the technical team must always check the availability of generators and batteries and ensure the generator can be used automatically.

There is still a lack of employee capabilities regarding air conditioning, generator sets, and batteries. Handling this risk is done by providing training and knowledge sharing to all employees to be able to overcome existing problems either with senior employees or in collaboration with vendors.

The ground lease contract for the tower placement was not renewed. Handling this risk is done in the form of cooperation between the division team with the planning team and management partners to negotiate with landowners. In addition, the planning team and CME also need to prepare a budget and prepare to look for new land to rent.

The Core Operation

Incorrect configuration on PC, CS, and IN-VAS systems. This risk handling is done by creating SOPs for all employees and vendors. Provide training and knowledge-sharing to all employees to be able to overcome problems and know how to configure the core system.

When doing onsite work at MSC, there is a hardware action error. This risk handling is done by creating SOPs for all technical teams and providing training and knowledge sharing to all employees to be able to overcome problems and be able to fix hardware.

There is still a lack of control over vendors. To handle this risk, the SOP must be made clear to all employees. The work must be supervised while the vendor is working, and once the vendor is done, the employee and vendor must figure out if there is a bad effect on the network or system or not.

Giving users who are not at the level of outsourced employees Handling this risk is done through the supervision of user and password usage by managers and supervisors. There are consequences or sanctions for employees who violate them.

Configuration Management

Disconnect the server device. Handling this risk is done by affirming the SOP to employees and checking the server at the beginning of work and before returning from work.

Disconnect the server device. Handling this risk is done by affirming the SOP to employees and checking the server at the beginning of work and before returning from work.

It takes a long time because the modules and spare parts of the server come from abroad. Handling this risk is done by preparing the right time and specifications by ordering modules and spare parts of the server from 6 to 1 year in advance, in collaboration with the partner management department.

Partner Management

Cooperation between employees and vendors to facilitate maintenance reports. Handling this risk is done by enforcing and clarifying the SOP to all employees about sanctions or consequences for employees who let vendors work on maintenance and make maintenance reports.

CONCLUSION

Based on the results of the collection, analysis, processing, and evaluation of risk data above, it can be concluded that several things, namely: operational risks in the Network Operation Center division at PT. Indosat Ooredoo Tbk include 49 risks, representing 9 types of risks in each department. Operational risks to PT. Indosat Ooredoo have a high impact and possibility of occurrence, namely the risk of thuggery in the Regional Operation Department. Meanwhile, the risk is the least in the partner management department. Of the 49 risks identified, 10 include acceptable or acceptable risk criteria, 32 include supplementary issue risk criteria or risks that require action when the company's resources are available, and 7 include risk issues or risk criteria that immediately need to be managed and mitigated. Risk criteria are used in the handling and control of risks so that they know which risks are a priority for handling. And risk management is also tailored to the source of the problem. It is expected that with the continuous control of risk factors, PT. Indosat Ooredoo Tbk. can provide a better quality of service to consumers in terms of networking systems. The company must be stricter in monitoring the company's operations by observing the risks in the field and looking for information related to the risks and problems that occur to reduce the risks that occur. And subsequent research is better at measuring financial losses from risks that arise.

REFERENCES

Afefy, I. H. (2015). Hazard Analysis and Risk Assessments for Industrial Processes Using FMEA and Bow-Tie Methodologies. Industrial Engineering and Management Systems. https://www.koreascience.or.kr/article/JAKO201503340570366.page

Alaoui, Y. L., & Tkiouat, M. (2017). Managing operational risk related to microfinance lending process using fuzzy inference system based on the FMEA method: Moroccan case study. Scientific Annals of Economics and Business. https://www.ceeol.com/search/article-detail?id=874397

Beasley, M. S., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. Journal of Accounting and Public …. https://www.sciencedirect.com/science/article/pii/S0278425405000566

Bhuana, E. B., Sumartini, S., & Sofia, A. (2017). Analisis Manajemen Risiko Operasional dalam Merencanakan Strategi Operasional (Studi Kasus pada Unit Pelaksana Teknis Pengujian Kendaraan Bermotor Dinas Perhubungan Kota Cimahi). Jurnal Ilmu Manajemen Dan Bisnis, 8(2), 1. https://doi.org/10.17509/jimb.v8i2.12660

Callahan, C. (2017). Does Enterprise risk management enhance operating performance? Advances in Accounting, 37, 122–139. https://doi.org/10.1016/j.adiac.2017.01.001

Chaidir, R. R., Fauzi, R., & Mulyana, R. (2020). Perancangan Manajemen Risiko Operasional Spbe/e-gov Pada Kategori Sumber Daya Manusia, Keamanan Dan Bencana Alam Berdasarkan Permen Panrb No. 5 Tahun 2020: Studi Kasus Di Pemerintah Kota Bandung. EProceedings of Engineering, 7(2).

ERM. (2004). COSO. In Enterprise Risk Management – Integrated Framework. https://doi.org/10.1504/IJISM.2007.013372

Goldberg, M., & Pleune, T. (2008). Enterprise Risk Management-Identifying, Measuring, and Managing Model Risk-Model risk has emerged as a new field, rife with its own specific …. In RMA Journal.

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. Journal of Risk and Insurance. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6975.2011.01413.x

Hunah, G. R., Pangestuti, D. C., & Sugianto, S. (2021). Analisis Risk Management Disclosure Pada Bank Umum Konvensional Yang Terdaftar Di Bursa Efek Indonesia. Konferensi Riset Nasional Ekonomi Manajemen Dan Akuntansi, 2(1), 1042–1056.

Jankensggrd, Hh. (2016). A Theory of Enterprise Risk Management. In SSRN Electronic Journal. Elsevier BV. https://doi.org/10.2139/ssrn.2753106

Malhotra, Y. (2015). Toward Integrated Enterprise Risk Management, Model Risk Management & Cyber-Finance Risk Management: Bridging Networks, Systems and Controls Frameworks. In SSRN Electronic Journal. Elsevier BV. https://doi.org/10.2139/ssrn.2792629

Marginingsih, R. (2017). Tata Kelola Manajemen Risiko Pada PT Unilever Indonesia , Tbk. Jurnal Cakrawala, 17(2), 156–164.

Pagach, D. P., & Warr, R. S. (2010). The effects of enterprise risk management on firm value. In Journal of Finance.

Pangestuti, D. C., & Hunah, G. R. (2021). An Exploratory Study On R{\i}sk Management D{\i}sclosure On Convent{\i}onal Commerc{\i}al Banks In Indones{\i}a. APMBA (Asia Pacific Management and Business Application), 10(2), 145–158.

Pangestuti, D. C., Nastiti, H., & Husniaty, R. (2021). Failure mode and effect analysis (FMEA) for mitigation of operational risk. INOVASI, 17(3), 593–602.

Pangestuti, D. C., & Tindangen, A. M. L. (2020). The Influence of Internal and External Factors on Firm Value. European Journal of Business and Management Research, 5(5).

Roy, S. (2020). Concept of risk identification, analysis, retention and application of enterprise risk management with reference to indian industries. … International Journal of Multidisciplinary Research. https://www.indianjournals.com/ijor.aspx?target=ijor:zijmr&volume=10&issue=4&article=001

Septi, H. D. (2018). Evaluasi Peran Enterprise Risk Management Dalam Upaya Pengelolaan Risiko Operasional Pada Usaha Percetakan Kedai Digital Di Tanjungpinang, Journal of Chemical Information and Modeling, 2(1), 15–27.

Sudaryono, B. (2012). Analisis Manajemen Risiko Perusahaan Dan Kepatuhan Terhadap Kinerja Perusahaan. In Media Riset Bisnis & Manajemen (Vol. 12, Issue 3, pp. 180–198).

Tandiawan, V. (2020). Journal of Tompotika : Social , Economics , and Education Science (JTSEES). 01(01), 105–126.

Tarigan, R. E. B., Soekarno, P., STr, M., & ... (2020). Analisa Risiko Operasional Di Divisi Network Operation Center (Noc) Pada Pt. Indosat Ooredoo. Manajemen Risiko, 1–40.

Tjaja, A., Sekartyasto, D., & Imran, A. (2019). Meminimasi Risiko pada Rantai Pasok Menggunakan Kerangka Kerja Suplly Chain Risk Management di PT Adhi Chandara Dwiutama. 3(1), 29–40.

Wiryono, S. (2008). Analisis Risiko Operasional Di PT TELKOM Dengan Pendekatan Metode ERM. Journal of Technology Management, 7(1).

Wulandari, R., & Susanto, R. (2019). Penerapan Manajemen Risiko Operasional Pada Unit Teller Pada PT. Bank Pembangunan Daerah Sumatera Barat Cabang Lubuk Alung. 1–10. https://doi.org/10.31219/osf.io/pjgch