ISSN 2449-7479
eISSN 2543-8840
amme.wne.sggw.pl

Annals of Marketing Management & Economics
Vol. 4, No 1, 2018, 115–129
DOI 10.22630/AMME.2018.4.1.9

OPERATIONAL RISK ANALYSIS OF NETWORK OPERATION CENTER DIVISION PT. IO

Rindu Eka Bakti Tarigan, Ktut Silvanita Mangani
Universitas Kristen Indonesia – UKI, Indonesia

INTRODUCTION

Every company that produces goods and services has a goal to satisfy its customers. Similarly, PT. IO, a company engaged in telecommunications, is always striving to provide the best services to its customers. For that purpose PT. IO try to control the risks that occur in the company.

However, by year 2014 PT. IO incurred a loss of more than 10 billion INR (rupiah, ≈715 thousand EUR) caused by for one day error in data routing resulting in increased complaints from customers. In addition, in September 2016 when the sea cable broke for 2 days the company suffered a loss of 5 billion INR (358 thousand EUR). The results of the investigation indicated that there were employees identified as violating the Standard Operating Procedures (SOPS).

In the business world, companies anticipate risks that occur through risk management. The company's management continuously manages risks by conducting risk management activities, such as identifying, performing risk measurement, controlling, communicating, and monitoring the risks from each activity undertaken by the company. Risk management is a system of managing the risk and protection of property and corporate profits against possible loss due to risk.

Sunaryo [2007] defines risk as a loss due to unexpected events. While operational risk is defined as failure of internal processes, human resources, and failures in technology systems, as well as losses due to external events, and the consequences of violations of laws and regulations [Muslich 2007, Lam 2007, Hanafi 2009, Gunawan and Waluyo 2015]. Lam [2007] explained that effective operational risk management provide three

benefits such as minimizing daily losses while reducing the potential for large events, Improve the company's ability to achieve its business goals, as well as accounting of operational risks will strengthens the entire corporate risk management system. According to Sunaryo [2007] there are 3 stages in the risk management process: 1) risk identification, 2) risk Measurement, and 3) risk management/evaluation.

AIM AND METHOD

The objective of the research is to identify the operational risks faced by PT. IO; measure and evaluate the risks, as well as make control and response measures to operational risks in the Network Operation Center Division. The study was conducted from June to September 2016.

The sample selection was done by quota sampling followed by convenience sampling, i.e. by assigning every 5 employees from 8 departments and one region out of 13 departments and 5 regions of operation of PT. IO. Data collection technique uses questionnaires to the employees who have competence in network center operations and have had working experience of at least five years. Furthermore, FGD (Focus Group Discussion) is conducted to determine the magnitude of the impact and the probability of the risk occurring.

The data validity test is done by Triangulation Test, that is by comparing the interview result from the resources person.

RISK ANALYSIS AND MITIGATION

Risk identification can be done by identifying the event, cause, impact, and frequency and likelihood of occurrence. According to Mushlich [2007], there are several operational risk identification techniques such as Risk Self Assessment (RSA), Risk Mapping, Key Risk Indicator, Limit threshold and Scorecard. This study uses Risk Mapping, a process whereby the risks that occur and that may occur are mapped in each business unit or department.

Risk can be measured to determine the extent of likelihood and the impact. Likelihood risk is expressed by the percentage probability of risk occurrence [AS/NZ 2009]. The size of the likelihood was converted to a semi-quantitative size scale from 1 to 5. The size of the likelihood is described in Table 1.

Impact is the seriousness of the loss from the risk associated with the company's objectives, i.e. how much the impact may occur from the event (if it happens) on the target [AS/NZ 2009]. Impact is measured using a Likert scale with a score of 5 criteria, as described in Table 2.

TABLE 1. Likelihood Ratings

Score	Occurrence	Probability of Occurrence	Occurrence in a year
1	Rare	may occur only under abnormal conditions, probability ≤ 20	1–2 times
2	Unlikely	it may occur at some time, probability 20 ≤ p ≤ 40	3–4 times
3	Possible	it may happen at some time, probability 40 ≤ p ≤ 60	5–6 times
4	Likely	may occur in many circumstances, probability 60 ≤ p ≤ 80	7–8 times

Source: the authors elaboration of PT.IO based on Likelihood rating, based on AS/NZS 2009.

TABLE 2. Impact Ratings

Impact Score	Financial Impact	Occupational Safety Impacts	Corporate Image Impact
Score 1 (Insignificant)	Financial losses are very small	work accident without doctor's help	Bad image among internal employees
Score 2 (Minor)	Financial losses are small	work accident without the help of a general practitioner	Bad image among the owner's environment
Score 3 (Moderate)	Financial losses are moderate	work accident without the help of a specialist doctor	Bad image among the local media
Score 4 (Major)	Financial losses are big	work accident without the help of specialist doctor and hospitalization	Bad image among National media
Score 5 (Catastrophic)	Financial losses are very big	wound work injuries are very severe and result in death	Bad image among international media

Source: the authors elaboration of PT.IO based on impact rating based on AS/NZS 2009.

According to Sunaryo [2007], undesirable risk is measured and managed by using the multiplication value of the probability and impact of potential events, called level of risk, with the formula:

$$L = p \times I$$

where: L = level of risk,
p = probability,
I = impact.

Furthermore, the probability and risk impact tables are combined into a matrix. This matrix serves to map the risk and the level of risk. The risk level is divided into four and represented by four different colours, i.e. green for low risk, yellow for medium risk, orange for high risk, and red for extreme risk [Ristic 2013]. The risk level matrix is presented in Figure 1.

Risk evaluation is a comparison between the risk levels found during the analysis process with predefined risk criteria. In risk evaluation, risk levels and risk criteria are compared using the same basis. The result of a risk evaluation is a list of risk priorities for further action. An evaluation step is taken to ensure that not all identified risks require further control plans.

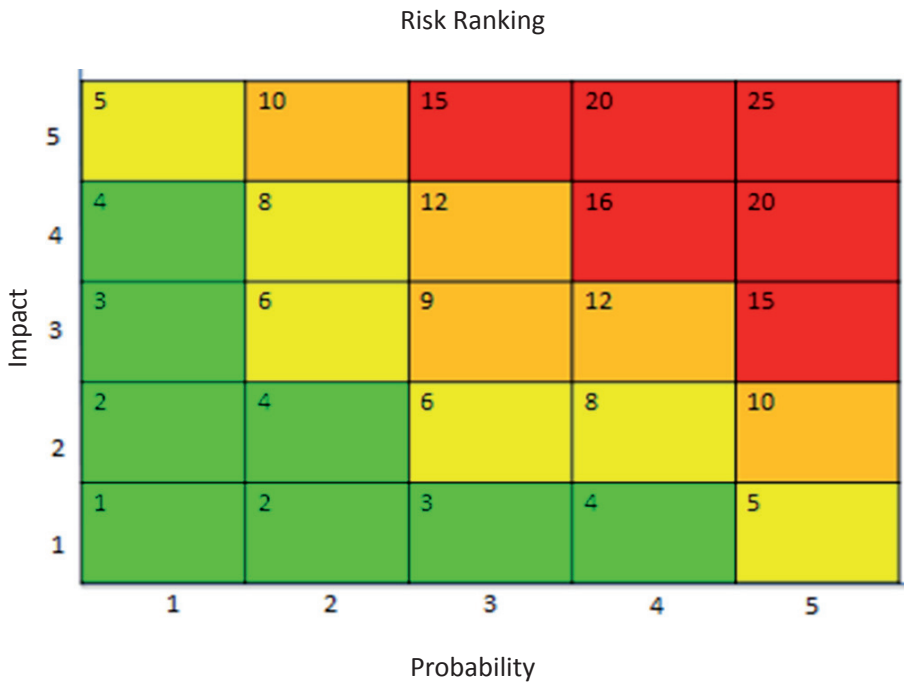

FIG. 1. Level of Risk
Source: the authors calculation based on formula $L = p \times I$.

The results of the risk analysis will be submitted to the highest responsible risk manager in the work unit for validation. Validation results will be used to establish a control system plan to reduce the likelihood or to reduce the impact of risk occurrence. The risk criteria are described in Table 3.

TABLE 3. Risk Criteria

Category Level	Score	Criteria and Explanation
Low	$L \leq 4$	Acceptable, no action is required
Moderate	$4 < L \leq 8$	Supplementary Issue, suggested action is taken if company resources are available
High	$8 < L \leq 12$	Issue, action required to manage risk
Extreme	$12 < L \leq 25$	Unacceptable, immediate action required to manage risk

Source: ISO 2009 version 2015, (Risk Management) [AS/NZ, 2009]

Risks that have been screened in the evaluation phase, then carried out the risk control plan. This step is called response to risk or risk mitigation. Risk mitigation involves identifying options to handle risks, assessing those options, setting up a risk treatment plan and implementing a risk treatment plan [Sunaryo 2007, see also: Darmawan 2011, Dewi 2012, 2010, Djohanputro 2004, Rosih 2015, Tisyana 2011, Wiryono ana Suharto 2008]. Risk mitigation is divided into two types: risk control and risk handling. Risk control is an attempt to avoid the risk. Examples of risk control can be in the form of procedures and work instructions, while the risk handling is the effort that will be done as a new step to treat the risk because the existing efforts are not yet adequate.

RISK IDENTIFICATION AND RISK MEASUREMENT

Risk identification and risk measurements were done at 8 departments and one region in the Network Operations Centre division, i.e. Front Office dept., Regional Operation Dept., Transmission Backbone Operation Dept., IP/MPLS Operation Dept., Access Operation Dept., CME Operation Dept., Core Operation Dept., Configuration Management, and Partner Management.

Risk measurement is performed prior to any action to change likelihood or risk impact, i.e. risk with conditions at the time of interview or mapping of the department. The risks that occur in each department may vary because of the differences in occupations and responsibilities. Risk measurements explain the incidence, probability of occurrence and frequency of occurrence in one year. Furthermore, risk measurement and risk criteria are determined. The summary of risk probability as well as the results of the measurement and risk criteria in each department of Network Operation Center are described in Table 4.

TABLE 4. Summary of Risk Results of the Network Operation Center Division

ti	Depart-ment		Description of Risk	Likelihood			Impact					Score Risk			Risk Criteria	Average Risk Score
				Occur in Year	Occurance	Score	Financial	Work Safety	Image	Impact Size	Score	Impact Score	Likelihood Score	Risk Score		
1	Front Office	1	Customer profile information to unauthori-zed parties	1	Rare	1	Ignored	Ignored	Affected	Major	4	4	1	4	Acceptable	(4 + 9 + 8 + 8 + 6) : 5 = 35 : 5 = 7
		2	Travel risk for employees on right shift	6	Possible	3	Ignored	Affected	Ignored	Moderate	3	3	3	9	Issue	
		3	Technicians fell asleep so shift alarm become late	5	Possible	4	Ignored	Ignored	Affected	Minor	2	2	4	8	Supplementary Issue	
		4	Employees provide their usernames and password to unauthorized	8	Likely	4	Ignored	Ignored	Affected	Minor	2	2	4	8	Supplementary Issue	
		5	Error in describing technical root cause by Customer Contact Services (CCS)	4	Unlikely	3	Ignored	Ignored	Affected	Minor	2	2	3	6	Supplementary Issue	
2	Regional Operation	1	Lack of Technicians	6	Possible	3	Affected	Ignored	Ignored	Moderate	3	3	3	9	Issue	(9 + 12 + 6 + 12 + 4 + 12 + 8 + 5) : 8 = 68 : 8 = 8,5
		2	Customer complaints against bad signal	6	Possible	3	Ignored	Ignored	Affected	Major	4	4	3	12	Issue	
		3	Lack of Operational vehicles	6	Possible	3	Affected	Ignored	Ignored	Minor	2	2	3	6	Supplementary Issue	
		4	Complaint handling is slow	6	Possible	3	Ignored	Ignored	Ignored	Major	4	4	3	12	Issue	
		5	Theft of Battery, Genset and Antenna	1	Rare	1	Affected	Ignored	Ignored	Major	4	4	1	4	Acceptable	
		6	Hoodium, the person who impersonates as youth organization request security money	8	Likely	4	Affected	Ignored	Ignored	Moderate	3	3	4	12	Issue	
		7	Limited Stock of Modules/Devices, affect BTS and MSC that need to repaired	3	Unlikely	2	Affected	Ignored	Ignored	Major	4	4	2	8	Supplementary Issue	
		8	Natural Disasters	1	Rare	1	Affected	Ignored	Ignored	Catas-tropic	5	5	1	5	Supplementary Issue	
3	Trans-mission Backbone Operation	1	Fiber Optic cable broken due to excavation	3	Unlikely	2	Affected	Ignored	Ignored	Major	4	4	2	8	Supplementary Issue	(8 + 8 + 8 + 5 + 6) : 5 = 35: 5 = 7
		2	Disconnected cable under the sea	3	Unlikely	2	Affected	Ignored	Ignored	Major	4	4	2	8	Supplementary Issue	
		3	Coaxial cable broken due to the flood	3	Unlikely	2	Affected	Ignored	Ignored	Major	4	4	2	8	Supplementary Issue	
		4	Lost of Satelite from its Orbit	1	Rare	1	Affected	Ignored	Ignored	Catas-tropic	5	5	1	5	Supplementary Issue	
		5	Lightning strikes VSAT link causing slow access to ATM Bank	3	Unlikely	2	Affected	Ignored	Ignored	Moderate	3	3	2	6	Supplementary Issue	

cont. Table 4

No	Depart-ment		Description of Risk	Likelihood			Impact					Score Risk			Risk Criteria	Average Risk Score
				Occur in Year	Occurance	Score	Financial	Work Safety	Image	Impact Size	Score	Impact Score	Likelihood Score	Risk Score		
4	IP/MPLS Operation	1	Error of IP destination by the vendor resulting problem in data access	3	Unlikely	2	Affected	Ignored	Ignored	Major	4	4	2	8	Supplementary Issue	(8 + 8 + 8 + 4 + 5) : 5 = 33 : 5 = 6,6
		2	Error in routing and layer setting by employee caused problem in data network	3	Unlikely	2	Affected	Ignored	Ignored	Major	4	4	2	8	Supplementary Issue	
		3	Error in changing the network layer that affects the MPLS network and result in disruption of internet, video streaming and sosial media access	3	Unlikely	2	Affected	Ignored	Ignored	Major	4	4	2	8	Supplementary Issue	
		4	The decline in the quality of the international Backbone Network	1	Rare	1	Affected	Ignored	Ignored	Major	4	4	1	4	Acceptable	
		5	The Network broke up due to carelessness of employee	1	Rare	1	Affected	Ignored	Ignored	Catas-tropic	5	5	1	5	Supplementary Issue	
5	Access Operation	1	Lack of human capital while tools and technology are increasing	7	Likely	4	Affected	Ignored	Ignored	Moderate	3	3	4	12	Issue	(12 + 8 + 8 + 6 + 8) : 5 = 42: 5 = 8,4
		2	Work environment security against theft (laptop, hp, etc)	7	Likely	4	Ignored	Affected	Ignored	Minor	2	2	4	8	Supplementary Issue	
		3	Human Errors and Work Accident	7	Likely	4	Affected	Ignored	Ignored	Minor	2	2	4	8	Supplementary Issue	
		4	Lack of Operational vehicles	6	Possible	3	Affected	Ignored	Ignored	Minor	2	2	3	6	Supplementary Issue	
		5	Computer/laptop facilities for outsourced employees are minimal make their performances are low	8	Likely	4	Affected	Ignored	Ignored	Minor	2	2	4	8	Supplementary Issue	
6	CME Operation	1	Frequent power outages at the site so that BTS and BSC devices are disrupted	7	Likely	4	Affected	Ignored	Ignored	Moderate	3	3	4	12	Issue	(12 + 6 + 6 + 6 + 9 + 9) : 6 = 48: 6 = 8
		2	Frequent delay of generator check	6	Possible	3	Affected	Ignored	Ignored	Minor	2	2	3	6	Supplementary Issue	
		3	Generator set (Genset) does not work automatically	3	Unlikely	2	Affected	Ignored	Ignored	Moderate	3	3	2	6	Supplementary Issue	
		4	AC for inner (MSC, BSC dan BTS) is damaged and takes a long time to have the new ones	3	Unlikely	2	Affected	Ignored	Ignored	Moderate	3	3	2	6	Supplementary Issue	
		5	The ability of employees regarding air conditioners, batteries and generators are low	3	Unlikely	3	Affected	Ignored	Ignored	Moderate	3	3	3	9	Issue	
		6	Land leased for tower placement is not renewed by the owner	3	Unlikely	3	Affected	Ignored	Ignored	Moderate	3	3	3	9	Issue	

cont. Table 4

No	Department		Description of Risk	Likelihood			Impact					Score Risk			Risk Criteria	Average Risk Score
				Occur in Year	Occurance	Score	Financial	Work Safety	Image	Impact Size	Score	Impact Score	Likelihood Score	Risk Score		
7	Core Operation	1	Configuration errors on PS, CS and IN-VAS core systems by new vendors or company employees	6	Possible	3	Affected	Ignored	Ignored	Minor	2	2	3	6	Supplementary Issue	(6 + 6 + 6 + 4 + 8) : 5 = 30 : 6 = 6
		2	"Action hardware" error while working on MSC location	4	Unlikely	2	Affected	Ignored	Ignored	Moderate	3	3	2	6	Supplementary Issue	
		3	Lack of supervision on vendors	6	Possible	3	Affected	Ignored	Ignored	Minor	2	2	3	6	Supplementary Issue	
		4	Employees provide sms and voice of subscribers without the permission of the company and the police	1	Rare	1	Ignored	Ignored	Affected	Major	4	4	1	4	Acceptable	
		5	Outsourching employees get 'user' that not match their level	3	Unlikely	2	Ignored	Ignored	Affected	Major	4	4	2	8	Supplementary Issue	
8	Configuration Management	1	The server device collapse	6	Possible	3	Affected	Ignored	Ignored	Minor	2	2	3	6	Supplementary Issue	(6 + 4 + 6 + 3 + 8) : 5 = 27 : 5 = 5,4
		2	Server is dmaaged	4	Possible	2	Affected	Ignored	Ignored	Moderate	2	2	2	4	Acceptable	
		3	The Server is exposed to virus	6	Possible	3	Affected	Ignored	Ignored	Minor	2	2	3	6	Supplementary Issue	
		4	Password of the server is given to person who is not available	1	Rare	1	Ignored	Ignored	Affected	Major	3	3	1	3	Acceptable	
		5	The company uses imported server modules and materials, so it takes time for ordering and dan installation	3	Unlikely	2	Affected	Ignored	Ignored	Major	4	4	2	8	Supplementary Issue	
9	Partner Management	1	Vendor (supplier) approach employees through rewards to facilitate maintenance contract cooperation	1	Rare	1	Ignored	Ignored	Affected	Major	4	4	1	4	Acceptable	(4 + 6 + 4 + 4 + 4) : 5 = 22 : 5 = 4,5
		2	Collaboration between employee and vendors in creating maintenance reports	3	Unlikely	2	Ignored	Ignored	Affected	Moderate	3	3	2	6	Supplementary Issue	
		3	Employees get rewards from vendors (supplier) in order to win contract tenders	1	Rare	1	Ignored	Ignored	Affected	Major	4	4	1	4	Acceptable	
		4	Employees reduce penalties to vendors	1	Rare	1	Ignored	Ignored	Affected	Major	4	4	1	4	Acceptable	
		5	Employees are not objective in determining the winning vendor	1	Rare	1	Ignored	Ignored	Affected	Major	4	4	1	4	Acceptable	

Source: the author's own work, based on Table 1., 2., and 3

RISK EVALUATION

The evaluation steps ensure that not all risks identified require risk control plan. From the risk list in all departments in the Network Operation Center division as many as 49 risks, there are 9 risks with Issue criteria, 30 risks with Supplementary Issue criteria, and 10 risks with acceptable criteria. The operational risk can be classified as: risks caused by human error – 12 risks; customer Satisfaction Risk – 2 risks; partnering risk – 6 risks; fraud risk – 3 risks; procurement risk – 3 risks; human resources risk – 3 risks; business interruption risk – 4 risks; capital availability risk – 3 risks; disaster risk – 3 risks; procedure risk – 4 risks; environment risk – 2 risks; and equipment risk – 4 risks.

The results of the risk analysis are submitted to the highest responsible manager of risk in the work unit for validation. Further validation results are used to establish risk control system plan to reduce the likelihood and the impact of risk occurrences in each department. Evaluation conducted on each department in the Network Operation Center PT. IO is described in Table 5.

TABLE 5. Risk Evaluation

Department	Risk Evaluation
a. Front Office Department	1. Travel risk for employees on night shift. This problem is solved by giving instructions to employees on shift-2 (14:00–22:00), who cannot possibly return home due to rainy days or other reasons, to continue work until shift-3 (22:00–06:00) replacing co-workers who were supposed to work on shift-3. The next day the replaced partner will work with two shifts, namely shift-2 and shift-3. 2. Technician fell asleep so shift alarm become late. This risk is dealt with by making work instruction (IK), that sleeping during working hours will be sanctioned. Each shift leader should pay attention to his team's work every 10 to 15 minutes. Thus, the risk of late alarm can be avoided. 3. Employees provide their usernames and passwords to unauthorized employees. This risk is overcome by creating a written rule of Standard Operating Procedures (SOPs), that employees are prohibited from giving their username and password to other employees. If the action resulted in a loss to the company, then the employee will get sanction in the form of dismissal. Prevention efforts are also done in cooperation with Security Management i.e.: a) employees are only given access to the information and network systems they need. b) implementing methods of identifying and authenticating data owned by security management and disabling passwords when not used for a certain period of time. 4. Error in describing technical root cause by Customer Contact Services (CCS). This risk is mitigated by facilitating two weekly meetings with Customer Contact Services (CCS) to resolve issues surrounding customer complaints on the network and root cause information in simple ways.
b. Regional Operation Departmen	1. Customer complaints against bad signal. Some ways to deal with this are as follows: a) if it occurs in urban areas, then Repeater or signal booster will be added. b) if it happens inside the building, then Repeater or BTS Indoor specifically for building, hotel and mall will be added. c) when it occurs in small urban areas or rural areas, then the addition of BTS will be added by first reviewing the business side in coordination with the sales and marketing team. 2. Hoodlum, the person who impersonates as youth organization request security money. Some ways to deal with this are as follows: a) cooperation with the police. b) personal Approach, i.e. approach to youth groups or influential people in the area. c) assign local thugs or youth in the area as security guards or site security officers.

cont. Table 5

cont. b. Regional Operation Departmen	3. Complaint handling is slow. To solve this problem the department assigns a rapid reaction team from technical team. 4. Lack of Technicians: To solve this problem is by training and practice sharing knowledge to existing teams in order to master and handle the technical problems of various things as well as efforts to add new employees through outsourcing. 5. Lack of operational vehicles. To solve this problem is by optimizing available operational car, by bringing the team simultaneously to a distant area. As for the surrounding area is by empowering the employee's motor and give rewards that can be claimed to the department. 6. Limited Stock of modules/devices, affect BTS and MSC that need to be repaired. This issue will be resolved by informing to the division and to the partner management department to immediately order the module to the designated vendor. 7. Natural disasters. This problem is resolved by providing spare part stock at headquarters.
c. Transmission Backbone Operation Department	1. Fiber Optic cable broken due to excavation. This problem is solved by cooperating with Ministry of Public Works&Housing (PU) and Regional Water Company (PDAM), so that PT. IO can monitor whether work was done that passed its cable. 2. Disconnected cable under the sea. This problem is solved by cooperating with TNI AL and POLAIR to monitor and check the cable channel under the sea. 3. Coaxial cable broken due to the flood. This problem is solved by cooperating with Search And Rescue (SAR) team. 4. Lost of satellite from its orbit. This problem is solved by risk transfer method – transfer the potential loss to the insurance company. 5. Lightning strikes VSAT link causing slow access to ATM Bank. This problem is dealt with by adding anti-lightning devices in every building containing VSAT.
d. IP/MPLS Operation Department	1. Error of IP-destination by the vendor resulting problem in data access. This problem is addressed by requiring SOPs and explanatory impacts from vendor as well as being supervised by field supervisor. In addition, vendor is allowed to leave the site after 30 minutes of work completed to ensure no impact on the data or network. 2. Error in routing and layer setting by employee caused problem in data network. This problem is solved by making SOPs of routing and layer settings. 3. Error in changing the network layer that affects the MPLS network and result in disruption of internet, video streaming and social media access. This problem is solved by creating SOPs of network layer. 4. The Network broke down due to carelessness of the employee . This problem is solved by creating SOPs for network layer.
e. Access Operation Department	1. Lack of human capital while tools and technology are increasing. This problem is solved by training and sharing knowledge with existing teams in order to master and deal with technical problems on access issues (BTS, BSC and PDH) and working with regional access teams to address access issues at level-2 that are not too difficult. Besides, efforts are done to add new employees through outsourcing. 2. Work environment security against theft (laptop, mobile phone, etc.). This problem is addressed in several ways i.e. install CCTVs and make cooperation with the CME team to create an access reader machine at the entrance of the workspace. 3. Human Errors and Work Accidents. The problem of human error is solved by providing training and outing division activities as well as family gathering to provide refreshment for employees. Work accidents are handled by the Department of Health and Work Safety. 4. Lack of operational vehicle. This problem is solved by optimizing operational vehicles. For non-urgent work that can be done through remote from the office or from home, will be decided without visiting the location. 5. Computer/laptop facilities for outsourced employees are minimal which causes slow performance. The manager strives for all outsourced employees to have adequate access to computer.

cont. Table 5

f. CME Operation Department	1. Frequent power outages at the site so that BTS and BSC devices are disrupted. This problem is solved in cooperation with the State Electricity Company (PLN), by making an agreement that every time there will be a power outage, PLN will notify PT. IO so that it can immediately replace it with a generator or battery as an alternative backup. 2. Frequent delay of generator check. This problem is solved by generating SOPs of generator check and every technician on duty should fill out he checklist generator check. 3. Generator does not work automatically. This problem is solved by generating SOPs of generator inspection. Every technician in charge should fill out the generator and battery checklist. 4. The ability of employees regarding air conditioners, batteries and generators are low. This problem is solved by providing training and sharing knowledge. 5. Land leased for tower placement is not renewed by the owner. This problem is forwarded to the division to be followed up by team planning and partner management. 6. AC for inner (MSC, BSC and BTS) is damaged and takes a long time to replace with the new ones. This issue is resolved by informing the division and the partner management department
g. Core Operation Department	1. Configuration errors on PS, CS and IN-VAS core systems by new vendors or company employees. This problem is solved by making SOPs that vendors and employees must comply with as well as training and sharing knowledge for employees. 2. "Action hardware" error while working on MSC location. This problem is solved by making SOPs for technical personnel assigned to the MSC site, as well as training and knowledge sharing for employees. 3. Lack of supervision on vendors. This problem is resolved by reinforcing the SOPs as well as the obligation for supervisors to accompany vendors up to 30 minutes after vendor work is completed to ensure that there is no impact on the system or network. 4. Outsourching employees get 'user' that not match their level. This problem is solved by monitoring and sanctions for employees who violate SOPs, unless approved by the manager. The Department also works with a team of Security Management to take precautions.
h. Configuration Management Department	1. The server device collapse. The manager reminds the employees to always work based on SOPs and do check on the server two times a day, that is when it starts to work and after finish the work so that server conditions can be detected earlier. 2. The server is exposed to virus. This problem is solved in cooperation with the IT division to always upgrade the latest anti-virus on all server devices and employees are required to do the scan before using the server. 3. The company uses imported server modules and materials, so it takes time for ordering and installation. This problem is solved in collaboration with Partner Management Departments and Project Division team to make an order at least 6 months before it is used.
i. Partner Management Department	1. Collaboration between employee and vendors in creating maintenance reports. This problem is solved by strengthening existing SOPs and also applying sanctions to employees who collaborate with vendors.

RISK MITIGATION

Determination of risk response or risk mitigation is carried out against the risks that have been filtered out in the evaluation step, to further control plan. Risk treatment and risk mitigation options generally include:

1. Avoidance of risk, means not carrying out or continuing activities that may cause risk.
2. Risk reduction, risk treatment to reduce the likelihood of occurring or reduce exposure to its impact, or both.

3. Risk sharing, an action to reduce the possibility of risks through insurance, outsourcing, subcontracting, acts of protection, transactions of foreign currency values, etc.
4. Risk Acceptance, not doing anything against the risk.

In the Network Operation Center division there exist 35 documents that covers all the risks that have been evaluated, as a way to risk mitigation as described in Table 6.

MANAGERIAL IMPLICATIONS

The managerial implications of operational risk mitigation at PT. IO can be done by using Planning, Organizing, Actuating, and Controlling (POAC) approach, namely:

1. Planning

PT. IO can plan a more comprehensive operational risk mitigation strategy through discussions conducted by Risk Managing Division. This plan is undertaken by evaluating all identified risks in the company and together with all departments formulate mitigation actions to be taken to address those risks. Separate risk management in each department will result in different ways of handling the same type of risk. So risk management becomes inefficient.

2. Organizing

Organizing can be done by placing the right person in the risk management process. The risk assessment process should be performed by the department head. Delegate tasks to the incompetent staff may affect the validity of the data.

3. Actuating

PT. IO needs to play an active role in raising participation and awareness of employee regarding the risks and their effort to mitigate the risks.

4. Controlling

Supervision on corporate risk mitigation implementation can be done by improving the supervision function of Risk Management Division.

TABLE 6. Risk Mitigation Documents in Network Operation Center Division PT.IO

No	Name of Documents	Responsible Unit
1	Cooperative Contract between PT.IO, PU and PDAM	Transmission Backbone Operation
2	Cooperative Contract between PT.IO and TNI	Transmission Backbone Operation
3	Cooperative Contract between PT.IO and POLAIR	Transmission Backbone Operation
4	Working Instruction (IK) – Working shift	Consumer Front Office
5	IK – Night Working Shift	Consumer Front Office
6	SOPs Security User	Consumer Front Office
7	Form Customer Complaint	Consumer Front Office
8	SOPs Field Inspection	Regional Operation
9	IK – Field Inspection	Regional Operation
10	IK – Work safety	Regional Operation
11	Cooperative Contract between PT.IO and POLRES	Regional Operation
12	Establish rapid reaction team	Regional Operation
13	IK – Professionalism: Outsourcing	Regional Operation

cont. Table 6

14	Cooperative Contract between PT.IO and ASTRA Rent Car	Regional Operation
15	IK – Work Standard Module	Regional Operation
16	SOPs Countermeasures earthquake	Regional Operation
17	SOPs Fire Prevention and Countermeasures	Regional Operation
18	SOPs IP/MPLS System	IP/MPLS Operation
19	SOPs Configuration Routing	IP/MPLS Operation
20	SOPs Monitoring Traffic	IP/MPLS Operation
21	IK – Professionalism: Outsourcing	Access Operation
22	SOPs Environmental Safeness	Access Operation
23	SOPs Device Inspection	Access Operation
24	Division System Budgeting	Access Operation
25	SOPs Genset Preparation	CME Operation
26	IK – Genset Checklist	CME Operation
27	IK – Professionalism: Outsourcing	CME Operation
28	Long term contract with Landowner	CME Operation
29	SOPs Configuration System	Core Operation
30	SOPs Hardware and Software Protection	Core Operation
31	SOPs Vendor Monitoring	Core Operation
32	SOPs User Security	Core Operation
33	SOPs Server Control	Configuration Management
34	SOPs Procurement	Configuration Management
35	SOPs code of ethics with vendors	Partner Management

Source: Network Operation Center, PT.IO, Jakarta.

CONCLUSIONS

The results showed that the company have to focus on 9 risks with Issue criteria, which require immediate action to manage risk or reduce risk. Most of the operational risks in Network Operation Network Division of PT. IO, i.e. 40 out of 49 identified risks have been handled properly, indicated by low levels of risk with acceptable and supplementary issue criteria, and it has 35 documents as a way of mitigation. Nonetheless, efforts are still needed to improve and update mitigation strategies because of the possibility of new risks and increased risk levels.

This study demonstrated the importance of identifying, measuring risk, and evaluate the risks for the company. Thus, it can be seen how far the company has prepared mitigation against identified risks, and the need to improve mitigation strategy.

This study has not fully explained the overall impact, such as financial losses of any identified risks. In addition, the evaluation and mitigation of impacts undertaken were still at the senior managers and engineers level. Therefore, it became a proposal for further research.

REFERENCES

AS/NZ, 2009. Australian Standards/New Zealand Standards. Risk Management-Principles and Guidelines, retrived from https://policy.deakin.edu.au/download.php?id=214&version=3&associated [accessed:].

DARMAWAN A., 2011. Perancangan Pengukuran Risiko Operasional Pada Perusahaan Pembiayaan Dengan Metode Risk Breakdown Structure (RBS) dan Analytic Network Process (ANP) (Design of Operational Risk Measurement at Financing Company With Risk Breakdown Structure »RBS« and Analytic Network Process »ANP«) [in Indonesian]. Thesis. Magister Manajemen Teknologi Industri, FTI UI, Jakarta.

DEWI D., 2012. Penerapan Sistem Manajemen Risiko pada Industri Nasionals ebagai masukan untuk Program PLTN (Implementation of Risk Management System in national industry as input for PLTN Program) [in Indonesian], Prosiding Seminar Nasional Pengembangan Energi Nuklir V, 7 Maret.

DEWI H., 2010. Pengelolaan Risiko Usaha (Business risk management) [in Indonesian], Penerbit Fakultas Ekonomi UI, Jakarta.

DJOHANPUTRO B., 2004. Manajemen Risiko Korporat Terintegrasi (Integrated Corporate Risk Management) [in Indonesian], Penerbit PPM, Jakarta.

GUNAWAN F.A., WALUYO M., 2015. Risk Based Behavioral Safety, Penerbit PT, Gramedia Pustaka Utama, Jakarta.

HANAFI M.M., 2006. Manajemen risiko (Risk management) [in Indonesian], Jakarta, Penerbit UPP Sekolah Tinggi Ilmu Manajemen YKPN.

LAM J., 2007. Enterprise Risk Management, Alih Bahasa Tim BSMR, Penerbit PT, Ray, Jakarta.

MUSLICH M., 2007. Manajemen Risiko Operasional (Operational Risk Management) [in Indonesian], Penerbit PT, Bumi Aksara, Jakarta.

RISTIC D., 2013. A Tool for Risk Assessment. Safety Engineering 3(3), 121–127.

ROSIH A.R., CHOIRI M., YUNIARTI R., 2015. Analisis Risiko Operasional Pada Departemen Logistik Dengan Menggunakan Metode FMEA (Operational Risk Analysis in Logistics Department using FMEA method) [in Indonesian], Universitas Brawijaya, Malang.

SUNARYO T., 2007. Manajemen Risiko Finansial (Financial risk management) [in Indonesian], Penerbit Salemba Empat, Jakarta.

TISYANA R., 2011. Mitigasi Risiko para pihak dalam pemberian kredit ke perusahaan menara Telekomunikasi (Analisis perjanjian Kredit) (Risk mitigation of the parties in the provision of credit to the telecommunication company (Credit agreement analysis)) [in Indonesian], FH UI, Jakarta.

WIRYONO K.S., SUHARTO., 2008. Analisis Risiko Operasional di PT. TELKOM dengan pendekatan metode ERM (Operational risk analysis at PT. TELKOM with ERM method approach) [in Indonesian], Jurnal manajemen Teknologi, 7, SMB ITB, Bandung.

Summary: This research is try to identify the operational risks in Network Operation Center division of PT. IO; measure and evaluate the risks, as well as make control and response measures to operational risks. The research method was a survey and Focus Group Discussion, by using a questionnaire as a research tool. The sample selection is done by Quota sampling and Convenience sampling methods to the employees in Division Network Operating Center PT.IO, which has had experience of at least 5 years. The results showed that as many as 40 out of 49 identified risks have been handled properly. Against these risks,

the company have 35 standard operating procedure documents (SOPs) as a mitigation of those risks. Nonetheless, efforts are needed to improve and update mitigation strategies because of the possibility of new risks and increased risk levels. It becomes a suggestion for further research as well as suggestion to undertake further research on mitigation at the division and director level.

Key words: risk, likelihood, impact, risk criteria, risk mitigation

JEL: M10, L21

Corresponding author: Ktut Silvanita Mangani, Universitas Kristen Indonesia – UKI, Graduate Program, Master of Management Study Program, Jakarta, Indonesia, e-mail: ktut.silvanita@uki.ac.id

Received: 27.07.2017
Accepted: 15.04.2018