Analysis Risk Technology information Use ISO 31000 on Application GRAB

Jumani [1], Sherly Silviani [2], Joy Nashar Utamaja, S.Kom.,M.M.S.I [3]

[1]Student, Information System, JL.AW.Syahranie No.4 RT 32, Batu Ampar, Kec.North Balikpapan, Balikpapan City, East Kalimantan.

[2]STMIK Borneo International, JL.AW.Syahranie No.4 RT 32, Batu Ampar, Kec.North Balikpapan, Balikpapan City, East Kalimantan.

[3]Lecturer,STMIK Borneo International, JL.AW.Syahranie No.4 RT 32, Batu Ampar, Kec.North Balikpapan, Balikpapan City, East Kalimantan.

Corresponding Author: Jumani.18@stmik-borneo.ac.id

Abstract: - The Grab application is an application that really helps humans in daily life, with the increasingly sophisticated information technology, applications have been created that greatly help human activities in everyday life. But we also need to pay attention to the quality of services provided from this Grab Application and also a risk analysis is needed to maintain the Quality of Service on this Grab Application and prevent possible risks that will occur in the future. Risk analysis using ISO 31000 in the Grab application is expected to prevent and minimize possible risks that will occur in the Grab application.

Key Words: — ***Grab, Risk Analysis, Risk Treatment, ISO 31000.***

I. INTRODUCTION

Human needs vary according to their nature, which is always increasing, while the ability to achieve something they need is limited. The increasing needs of life, causing people to look for ways to meet their needs in a more practical way. Seeing the situation in this modern era, people have used technology wherever they are. Technology has become common in people's lives, thus requiring service companies to innovate to create businesses that follow and take advantage of technological advances in order to compete in the business world. Technology is developing rapidly and increasingly sophisticated, providing great benefits to convenience in various aspects of people's lives. People's lives are made easier; the influence of the internet is clearly visible in people's lives, giving rise to the idea of one service company how to link communication media with online transportation services, which at the same time can open job vacancies for the community. One company that is now famous for the services provided is Grab[1]. Grab is one of the businesses online transportation that earns income by utilizing technology through online-based service offering applications.

Manuscript revised September 07, 2021; accepted September 08, 2021. Date of publication September 10, 2021.
This paper available online at www.ijprse.com
ISSN (Online): 2582-7898; SJIF: 5.494

The services provided by Grab for customers are food delivery, couriers, credit purchases, bill payments, and services booking transportation delivery to destination locations that can be selected according to customer needs such as GrabBike (motorcycle), GrabTaxi (taxi), and GrabCar (car). However, becoming a Grab driver is not easy, but you must first meet several requirements in accordance with the standards set by the Grab Company, considering that humans (HR) as drivers play a big role in the quality of a company's services.[2]. Grab services are not far from quality problems services, students as Grab customers certainly have different perceptions about it, some are positive and some are negative. According to (Philip Kotler, 2009:179) perception is the process by which we select, organize, and translate information input to create a picture of the world. In viewing services on the application Grab powered by technology With sophisticated information, the Grab application is of course a necessity for humans because it makes our needs easier. However, if the Grab application is attacked in the form of threats and risks and is not handled immediately, it will hamper the application process and automatically the Grab application process will not run optimally or even stop. Risk management can anticipate losses and implement procedures [3]. Therefore, considering the importance of risk management based on several problems, it is necessary to create and implement a security risk management system in the Grab application by conducting a risk assessment to follow up based

on the risks that have been given in order to minimize the risks that may occur in the Grab application [4].

To find out the risk value in the existing Grab Information Technology application, ISO 31000:2018 is used in the risk management system in the Grab application. ISO 31000 : 2018 is the latest version of the risk management standard modified by ISO (International Organization for Standardization) which was officially released on February 14, 2018 which replaces the previous management standard, namely ISO 31000:2009 Risk Management – Principles and Guideline [5][6].

II. RESEARCH METHOD

Research conducted on the Grab application was carried out by means of observation and interviews with Grab drivers and customers. Observations and interviews were conducted to obtain problem data and conduct an audit assessment on the Grab application. After getting the results of the audit, then you can assess the risks obtained from the ISO 31000:2018 Stages. The method that I will use in this research is the case study research method. This method focuses on one case and samples used individually or in groups. So with this method the author can collect more data on the object and will be investigated to answer the existing problems. The data in this study are primary data, where the data sources are collected in the form of documents that have been validated and verified by the informants. Sources of data from.

III. RESULT AND DISCUSSION

3.1 Risk Assessment

Stage of risk assessment or risk assessment is the first stage carried out in accordance with ISO risk management analysis guidelines 31000. At this stage there will be 3 processes, namely risk identification, risk analysis, and risk evaluation. These three processes must be passed to the next stage.

3.2 Risk Identification

The first process in the risk assessment stage is the risk identification process or asset identification in the Grab application, which is carried out through an interview process with the Grab Driver. At this stage, identification of assets from data, software to hardware related to the Grab application is carried out.

System Components Information	Grab Assets
Data	User Client Data, Data Information Grab
Software	Grab
Hardware	Mobile, Database Server, System Application

After identifying assets from data, software to hardware related to the Grab application. Next is to identify possible risks associated with Grab application assets that can arise from various factors such as nature/environment, people, systems and Infrastructure.

Factor	Possible Risk
Natural	Flood
	Earthquake
	Fire
	Lightning
Man	Device/data theft
	Human error
	Information accessed by parties who
	Data and information do not match
	Human-made damage (cybercrime and vandalism)
system and Infrastructure	Server Down
	Corrupt data
	Backup failure
	Hacking against the network
	Memory full
	Network connection lost
	Overheat
	Overload
	Poor network quality
	Power outage

3.3 Risk Analysis

After the possible risks and impacts have been identified, the next step that will be processed is risk analysis. In this process there is a table of likelihood criteria and a table of impact criteria that are used as a reference for the risk analysis process. That table of the likelihood criteria or the probability value that has been determined. In the likelihood

assessment, it is divided into 5 criteria and classified by how much the risk can occur in a certain period of time.

Score	Criteria	Information	Frequency Incident
1	Rare	Risk Almost Never Happen	> 2 years
2	Unlikely	Rare Risk Happen	12 years old
3	possible	Risk sometimes Happen	7 – 12 months
4	Likely	Frequent Risk Happen	4 – 6 months
5	Certain	Risk Will Happen	13 months

The Next table is a table of impact values if the risk is likely to occur in the company. In the assessment, there are 5 criteria for possible impacts. These criteria are distinguished from the impact that has no effect to the impact that most affects the Grab Application.

Score	Criteria	Informati on
1	Insignificant	Does not interfere with performance
2	Minor	App performance a bit hampered but the company's core
3	Moderate	Causing disturbance to process so that the application performance is slightly
4	Major	Slows down almost all application activity and performance.
5	Catastropic	App activity stopped because the application process is experiencing a total

After the probability and impact values have been determined, the next step is to conduct a one-by-one assessment of the possible risks.

Of the 19 possible risks, the likelihood and impact values are determined one by one based on the table reference made previously.

Table.1. Assessment of possible risks with likelihood and impact

No	Possible Risk	Likelihoo	Impact
1	Flood	1	2
2	Earthquake	1	2
3	Fire	1	3
4	Lightning	2	2
5	Device/data theft	2	2
6	Human error	3	2
7	Information accessed by Unauthorized party	2	2
8	Data and information are not according to facts	2	2
9	Man-made damage man	3	2
10	Server Down	1	1
11	Corrupt data	1	1
12	Backup failure	2	2
13	Hacking against the	1	2
14	Memory full	4	3
15	Network connection lost	3	3
16	Overheat	2	2
17	Overload	2	2
18	Not good quality network	3	2
19	Power outage	2	2

3.4 Risk Evaluation

The last process to complete the risk assessment stage is the risk evaluation process. This process uses a reference in the form of a risk evaluation matrix. Where in the matrix is divided into 3 risk levels, namely low, medium and high. Then the likelihood of the risk that has been determined by the likelihood value and the impact value in the previous process will be distinguished again according to the existing matrix.

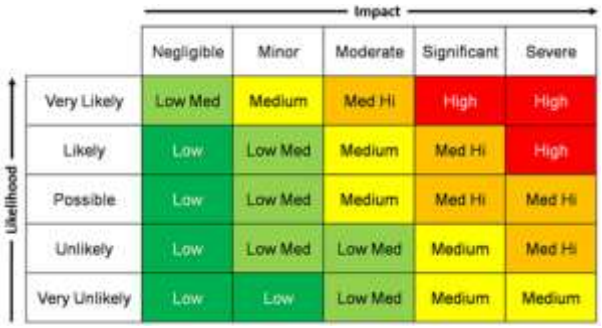

Fig.1. Risk Matrix

Possible risks based on likelihood and impact will be included in the risk evaluation matrix by looking at the mapping in the previous evaluation Risk matrix image. In the Risk Matrix image, evaluate the identity of each possible risks listed in table 5 are included into the column that matches the criteria likelihood and impacts made previously.

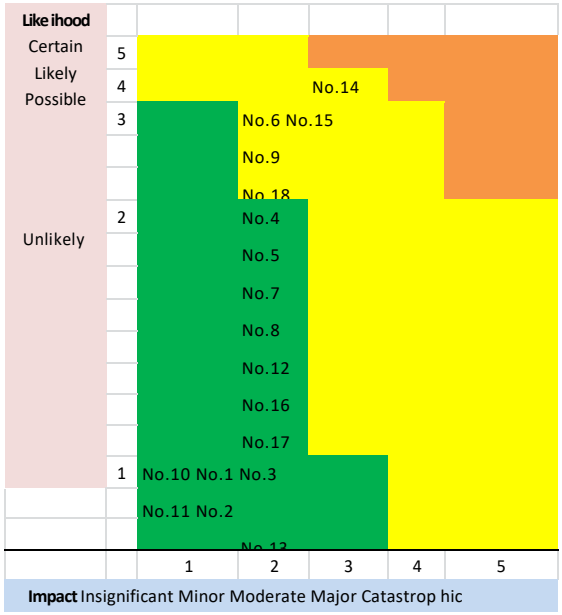

Fig.2. Risk Evaluation Matrix Based on Likelihood and Impact

Then after all possible risks have been entered into the risk evaluation matrix column in Figure 2, it will spelled out from 19 possible risks that are included in the level of risk with high, medium or low levels based on likelihood and impact criteria.

No	Possible Risk	Likeliho	Imp	Risk
1	Flood	1	2	Low
2	Earthquake	1	2	Low
3	Fire	1	3	Low
4	Lightning	2	2	Low
5	Device/data theft	2	2	
6	Human error	3	2	Medium
7	Information accessed by parties the one who is not authorized	2	2	Low
8	Data and information do not	2	2	Low
9	Human-made damage	3	2	Medium
10	Server Down	1	1	Low
11	Data corrupt t	1	1	Low
12	Backup failure	2	2	Low
13	Hacking the network	1	2	Low
14	Memory is full	4	3	Medium
15	The network connection is	3	3	Medium
16	Overheat	2	2	Low
17	Overload	2	2	Low
18	Not good quality as network	3	2	Medium
19	Power outage	2	2	Low

Fig.3. Risk Level from Possible Risks

The results of the risk evaluation process can be seen in Figure 3 of 19 there may be 5 that are included in the level of risk medium level. As well as 14 which are included in level of risk low level.

3.5 Risk Treatment

The stages after risk identification are risk treatment stage. At this stage, the author will provide suggestions regarding the treatment that must be carried out for all possible risks that exist in the Grab application. or minimize the possible risks that exist shown in Figure 3. It is also used by the company to prevent the possibility of existing risk.

No	risk Level	Risk Action
1	Low	Installing a backup server in a different location. Perform database mirroring. Provide a high place to store company assets.
2	Low	Installing a backup server in a different location. Mirroring the database.
3	Low	Installing a backup server in a suitable location different. Perform database mirroring. Installing fire hydrants inside company buildings to prevent this from happening
4	Low	Installing lightning rods in company buildings
5	Low	Carry out password maintenance periodically. Installing CCTV in company buildings.
6	Medium	Doing previous training against New Users. Create a knowledge management system as knowledge documentation for new users so they don't make the same mistakes.
7	Low	Carry out password maintenance periodically. Installing CCTV in company buildings.
8	Low	Carry out password maintenance periodically.
9	Medium	Changing server passwords periodically. Installing CCTV in company buildings

10	Low	Carry out checks periodically within 1 day against the database of the Grab application and the company's main database. Refresh the usage log, temp, and RAM of the Grab application and main database to prevent server down.
11	Low	Perform data backups periodically.
12	Low	Pay attention to memory usage storage that is used regularly. Backup data contained in the Grab application and main database on a regular basis
13	Low	Changing server passwords periodically. Don't give information to suspicious people and don't reply Unclear e-mail address
14	Medium	Check memory usafe periodically increase memory capacity before full.
15	Medium	When the network connection is lost immediately report to the network section,and perform network maintenance at the company on a regular basis
16	Low	Make sure the air conditioner is able to keep the hardware cool.
17	Low	Conduct periodic checks to the database of the Grab application and the company's main database. Refresh the log, temp, and RAM usage of main application and database before
18	Medium	When the network connection is blocking the company immediately reports to the network. Changing the ISP (Internet Service Provider) if the network used interferes with the company's activities.
19	Low	Using a power source that different.

V. CONCLUSION

From the results of the risk analysis, it can be seen that there are 19 possible risks that have the potential to disrupt the performance of the Grab application and its company. And there are also 5 possible risks that are included in the medium level of risk, namely human error, damage caused by humans, full memory, disconnected network connection and poor network quality. And there are 14 possible risks that are included in the low level of risk, namely device/data theft, data corruption, backup failure, overload, information accessed by unauthorized parties, overheating, flooding, lightning, network hacking, earthquakes, fires. , data and information do not match the facts, Server Down, and power outages. Actually, the process of overcoming the risks carried out by the Grab company has been carried out, because the Company and the Grab application are companies that focus on Culinary, Transport using Information Technology. However, there is a possibility that the Company does not carry out Risk Treatment on a regular basis, which could affect the Processes and Activities of the company and the Grab Application. so it is hoped that the results of this research can be used by the company to be able to manage and minimize the possible risks that may occur to the company in the future.

REFERENCES

[1]. D. W. Iswari and E. K. Omar, “Design Management Risk Technology Information on Key Support Process APO02, APO06 and APO08 in Service Communication And informatics (DISCOMINFO) Government City Bandung Use Framework COBIT 5,” vol. 3, no. 2, pp. 3476–3482, 2016.

[2]. T. aven, “Risk assessment and risk management: Review of recent advances on their foundations," vol. 0, pp. 1–13, 2016.

[3]. A. novia, R.Yanuar, F.A.W.St.,D. Bi, and J.St., "Analysis Risk Technology Information Based on risk Management Use ISO 31000 (Case Study : i-Gracias Telkom universities)"

[4]. A.standard,“for US/NZS ISO 31000:2009 risk management - Principles and guidelines," 2018.

[5]. K.um, “ISO 31000:2009; ISO/IEC 31010 & ISO Guide 73:2009 International Standards for the Management of risk," 2009.

[6]. V.Sousa, N. M. De Almeida, and L. A. Dias, “Risk Management Framework for the Construction Industry According to the ISO 31000: 2009 Standards," vol. 2, no. 4, pp.261–274, 2012.

[7]. P.Zainal A. Hasibuan, "Methodology Study on Field Knowledge Computer and Technology Information," pp. 1-194, 2007.