RISK MANAGEMENT

Submitted to the

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES

In partial fulfillment for the completion of the

PROJECT

BY

Kilari Venkata Sai Sanjana - 192011124 (CSE)

Anumalasetty Jahnavi-192110065(CSE)

Under the guidance of

Dr.K.Vijaya Bhaskar

Assistant Professor

INSTITUTE OF SCIENCE AND HUMANITIES

SAVEETHA SCHOOL OF ENGINEERING
CHENNAI – 602 105
TAMILNADU, INDIA

January 2021

BONAFIDE CERTIFICATE

This is to certify that the project report entitled **“Risk management”** submitted by “Kilari Venkata Sai Sanjana-192011124 (CSE),Anumalasetty Jahnavi-192110065(CSE), to Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, is a record of bonafide work carried out by him/her under my guidance. The project fulfills the requirements as per the regulations of this institution and in my appraisal meets the required standards for submission.

Dr. K.Vijaya Bhaskar

Supervisor,
Department of Programming
Saveetha School of Engineering
SIMATS, Chennai – 602 105

Internal examiner **External Examiner**

S.No	CONTENTS	Page No
1	Abstract	5
2	Introduction	6
3	Objectives	7
4	Literature Review	8-9
5	Suggestions	10
6	Data Analysis	11-13
7	Risk Management Process	14-16
8	Benefits and challenges	17-18
9	Conclusion	19
10	References	20

ACKNOWLEDGEMENT

I take immense pleasure in expressing my gratitude to our Honourable Chancellor **Dr. N. M. Veeraiyan** for being our constant source of inspiration.

I sincerely thank our Vice-Chancellor, **Prof. Dr. Rakesh Kumar Sharma** for providing the academic ambience to complete the project successfully.

With profound gratitude, respect and pride, I express my sincere thanks to our Director, **Mrs. Ramya Deepak**, whose enthusiasm and dynamism being the driving force behind all our accomplishments.

I take this opportunity to extend our heartiest thanks to our beloved Principal, **Dr.B. Ramesh** for providing us excellent facilities and unstinting support which were the sustaining factors in carrying out the work successfully.

It is a genuine pleasure to express my deep sense of thanks and gratitude to my mentor and my project guide **Dr. K. Vijaya Bhaskar**, Department of Science and Humanities. His timely advice, meticulous scrutiny and scientific approach have helped me to a very great extent to accomplish this task and also his dedication and keen interest had been solely and mainly responsible for completing my work.

Last, but not least, a very special thanks to my parents and friends for their moral support and care extended during the demanding times.

ABSTRACT

Risk management is a structured approach/methodology for managing uncertainty related to threats; a series of human activities including: Risk assessment, developing strategies to manage it and risk mitigation using resource empowerment/management. Strategies that can be taken include moving risk to other parties, avoiding risks, reducing the negative effects of risk, and accommodating some or all of the consequences of certain risks

The goal of implementing risk management is to reduce the different risks associated with the chosen field at a level acceptable to the community. This can be in the form of various types of threats caused by the environment, technology, people, organizations and politics. The implementation of risk management involves all means available to humans, in particular, to risk management entities as human, staff and organization.

Risk management is important in an organisation because without it, a firm cannot possibly define its objectives for the future. If a company defines objectives without taking the risks into consideration, chances are that they will lose direction once any of these risks hit home.

In recent years, many companies have added risk management departments to their team. The role of this team is to identify risks, come up with strategies to guard against these risks, to execute these strategies, and to motivate all members of the company to cooperate in these strategies. Larger organisations generally face more risks, so their risk management strategies also need to be more sophisticated. Also, the risk management team is responsible for assessing each risk and determining which of them are critical for the business. The critical risks are those that could have an adverse impact on the business; these should then be given importance and should be prioritized. The whole goal of risk management is to make sure that the company only takes the risks that will help it achieve its primary objectives while keeping all other risks under control.

INTRODUCTION

Risk is part of the work life of individuals and organizations. Various risks, such as the risk of fire, being hit by another vehicle on the road, the risk of being flooded in the rainy season and so on, can cause us to suffer losses if we do not anticipate these risks from the start.

Risks are associated with possible events or circumstances that can threaten the achievement of organizational goals and objectives. The activities of a business entity or company basically cannot be separated from risk management activities. Operations of a business entity or company usually deal with business risks and non-business risks. In general, risk can be interpreted as a situation faced by a person or company where there is a possibility that is harmful.

Risk management is an important process because it empowers a business with the necessary tools so that it can adequately identify and deal with potential risks. Once a risk has been identified, it is then easy to mitigate it. In addition, risk management provides a business with a basis upon which it can undertake sound decision-making.

There are five steps in a risk assessment.

1. Identify Risks – If you can think of it, you can prevent it.
2. Prioritize Risks
3. Analyze Risk Response Strategies
4. Plan Risk Response
5. Monitor and Control Risks

Risk assessment is a subjective exercise. The power of the risk assessment does not come from creating the “right” assessment or operating under the belief that all risks will be eliminated; The true value comes from gathering together those individuals involved with the program or activity, having group discussions about risk, and determining what can be done to address risks. Ultimately, it’s not about your municipality having “no risks,” it’s about managing the risks.

OBJECTIVES

The objective of risk management is to control risks. When the potential risks are identified, measured, and monitored, then the final objective is to find out ways to deal with or control those risks.

Identifies and Evaluates Risk. Risk management identifies and analysis various risk associated with business organizations:

- Reduce and Eliminate Harmful Threats
- Supports Efficient use of Resources
- Better Communication of Risk within Organisation
- Reassures Stakeholders

LITERATURE REVIEW

Shahroudi et al (2012)- journal of effective risk management

Shahroudi et al 2012 in support confirmed that reducing exposed risk increase quality of service as well as firms and financial performance, they added that risk management and financial performance has a positive relationship. they revealed that firms with a reputable risk reduction practice produce more revenue and their risk maturity got linked with better return on asset and positive response on risk management.

Pac 2015- journal of strategic management

The pac2015 is about the management that lack of risk reduction has been evidenced by the recurring of observations of every year. However it most done on empirical studies on effects on risk management on performances had been done mostly in developed countries and in insurance companies in Kenya. Now a days it is a imp research topic many in business and industrial areas,

Feririo 2020-Journal of modern transportation

Feririo 2020 is the risk management review on driverless cars, feririo 2020 is the risk mangement that provided on the driverless cars in 2020 that they are becoming important note readly in society .Driverless cars rely on sensors and a complex system in order to function. However, by the technology it overcome with the driverless feature.

La and choi 2012-Jouranl of methodology of supply chain

La and choi are the two persons on risk management that has a positive significant relationship with organisational performance, Wanjohi agreed that risk management has a significant and positive relationship between financial performance of an organization. However, they posted there will be weak responses for our management also. But however, it will if there are strong decision in our management no matter occur whether it is right or wrong.

Azeredo et al 2014-Journal of risk management

Azeredo et al (2014) is the journal that provides a process analysis in a structured way to build a consistent theoretical framework that is based on delimination of field of knowledge the selection of database keywords, time filters and criteria for inclusion and exclusion that are misaligned with regard to central theme of research of risk management.

SUGGESTIONS

1. Be clear about your remit

Any gaps in responsibilities across your business present an increased opportunity for risk. Make sure that everyone knows exactly what part of the business and what activities and tasks they are responsible for.

2. Identify risks early on

It's never too soon to start thinking about risk. The sooner you do this, the easier it will be to manage the risk. Think about risk management at the start of every project or task. What Early Warning Indicators (EWIs) can we track for different risks? Risk management should be embedded into all of your work processes and corporate culture.

3. Be positive

Not all risks are negatives, so don't only focus on the downsides. Risks can be positive too, presenting and enabling us to take advantage of a given event or situation.

4. Describe risk appropriately

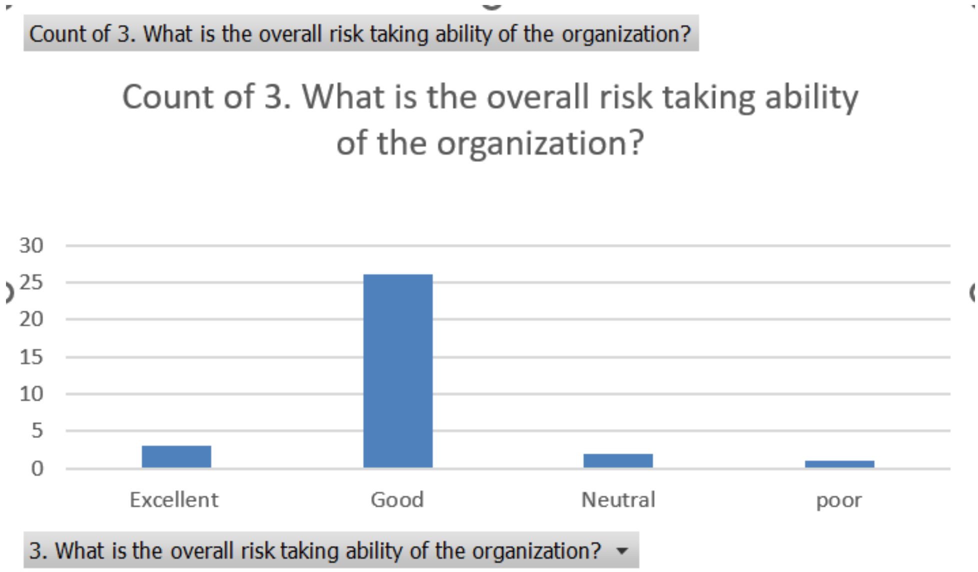
As part of the risk assessment process, it is good practice to create a risk 'string', distinguishing between cause and effect.

5. Estimate and priorities risk

Use a risk matrix to assess and priorities all known risks. You can calculate the severity of a risk by looking at both the probability (likelihood) and impact (severity).

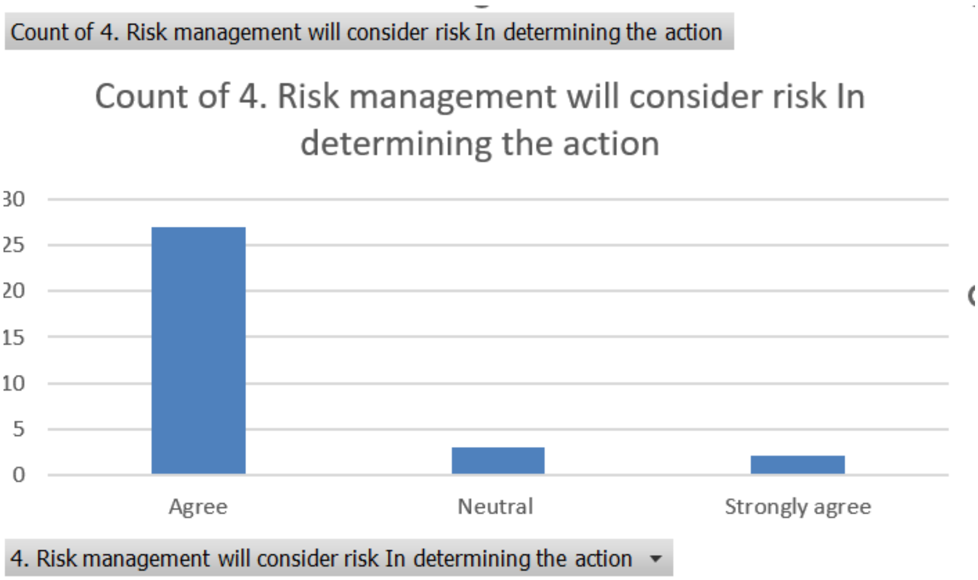
DATA ANALYSIS

➢ **Overall risk taking ability of the organistaion**



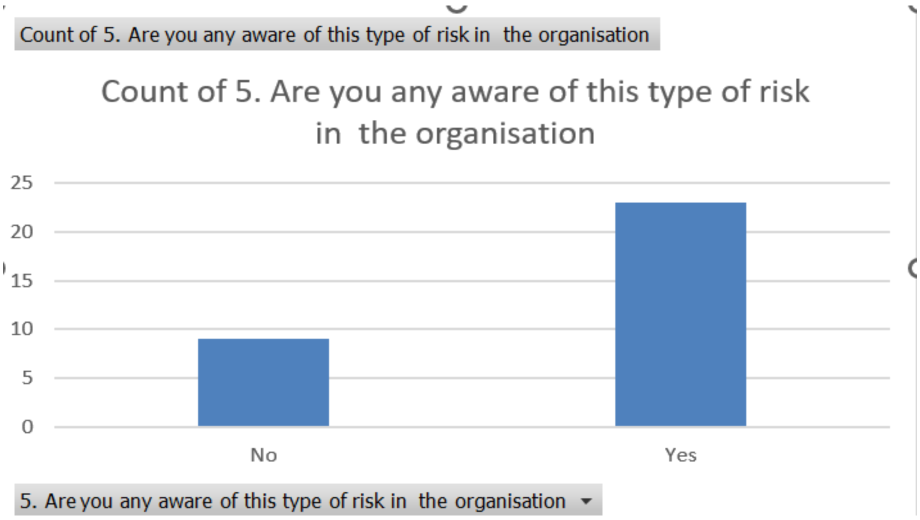
From this survey we can say that the overall risk taking ability of the organisation is good.

➢ **Risk management in determining the action**



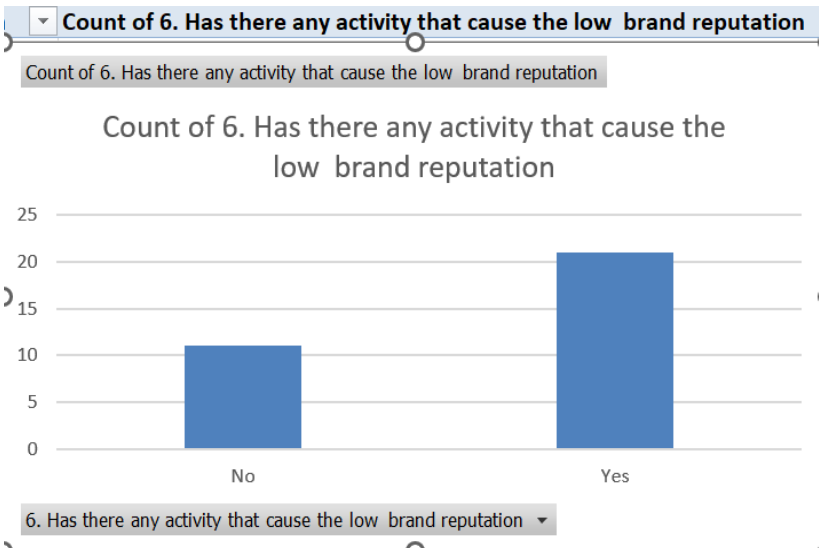
From this survey the overall risk management that will consider the risk determining the action is agreed by everyone.

- **Aware of any type of risks in the oragniation.**



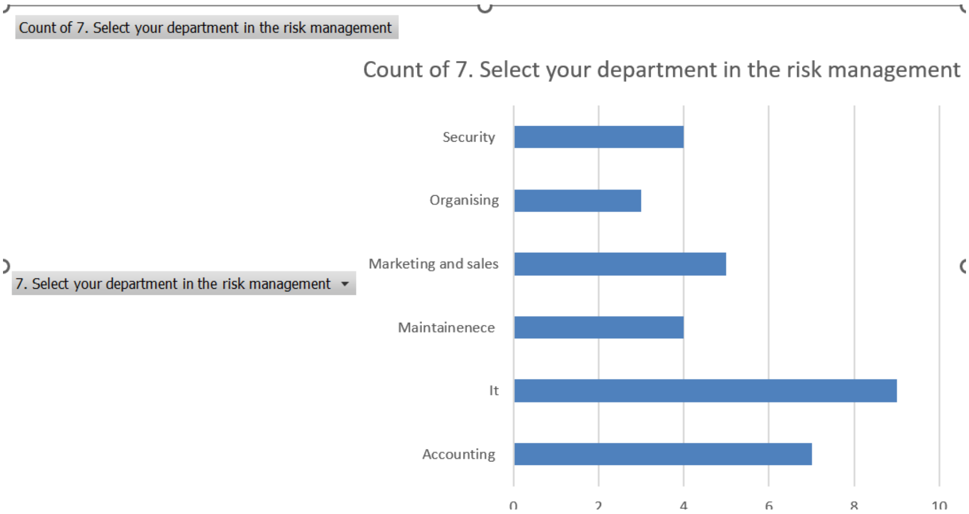
From this survey most of the people have agreed that they are aware of the any type of risk in the organization.

- **Brand reputation**



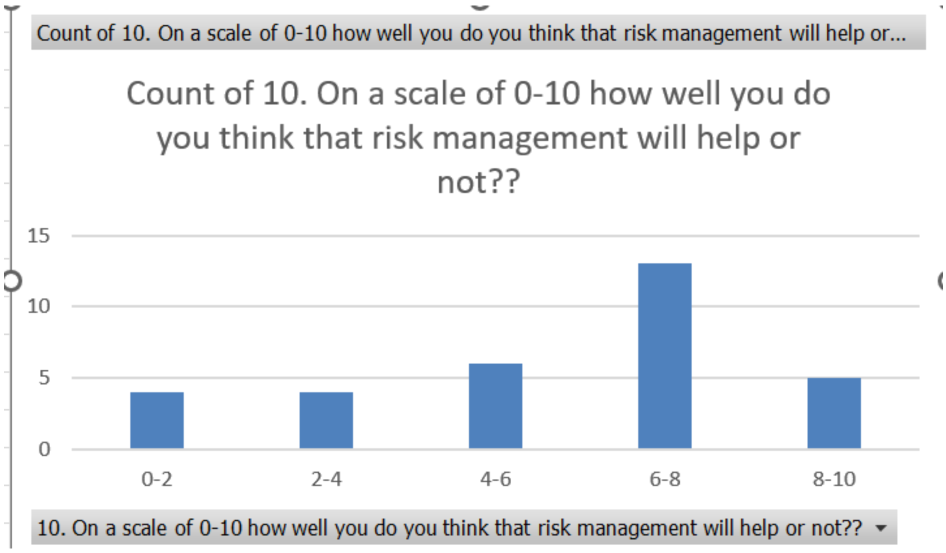
From this survey most of the people have agreed that there are activities that cause the low brand reputation in an organisation.

➢ Department in the risk management



From this survey we can say that least members belong to organising department and most of the people belong to IT department.

➢ Rating of risk management



From this survey most of the people giving an analysis on a scale of 6-8 mostly and most of the people think risk management will help in an organisation to suceed.

RISK MANAGEMENT PROCESS

The risk management discipline has published many bodies of knowledge that document what organizations must do to manage risk. One of the best-known sources is the ISO 31000 standard, *Risk Management -- Guidelines*, developed by the International Organization for Standardization, a standards body commonly known as ISO.

ISO's five-step risk management process comprises the following and can be used by any type of entity:

1. Identify the risks.
2. Analyze the likelihood and impact of each one.
3. Prioritize risks based on business objectives.
4. Treat (or respond to) the risk conditions.
5. Monitor results and adjust as necessary.

The steps are straightforward, but risk management committees should not underestimate the work required to complete the process. For starters, it requires a solid understanding of what makes the organization tick. The end goal is to develop the set of processes for identifying the risks the organization faces, the likelihood and impact of these various risks, how each relates to the maximum risk the organization is willing to accept, and what actions should be taken to preserve and enhance organizational value.

"To consider what could go wrong, one needs to begin with what must go right," said risk expert Greg Witte, a senior security engineer for Huntington Ingalls Industries and an architect of the National Institute of Standards and Technology (NIST) frameworks on cybersecurity, privacy and workforce risks, among others.

When identifying risks, it is important to understand that, by definition, something is only a risk if it has impact, Witte said. For example, the following four factors must be present for a negative risk scenario, according to guidance from the NIST Interagency Report (NISTIR 8286A) on identifying cybersecurity risk in ERM:

1. a valuable asset or resources that could be impacted;
2. a source of threatening action that would act against that asset;
3. a preexisting condition or vulnerability that enables that threat source to act; and
4. some harmful impact that occurs from the threat source exploiting that vulnerability.

In identifying risk scenarios that could impede or enhance an organization's objectives, many risk committees find it useful to take a top-down, bottom-up approach, Witte said. In the top-down exercise, leadership identifies the organization's mission-critical processes and works with internal and external stakeholders to determine the conditions that could impede them. The bottom-up perspective starts with the threat sources (earthquakes, economic downturns, cyber attacks, etc.) and considers their potential impact on critical assets.

Organizing risks by categories can also be helpful in getting a handle on risk. The guidance cited by Witte from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) uses the following four categories:

- strategic risk (e.g., reputation, customer relations, technical innovations);
- financial and reporting risk (e.g., market, tax, credit);
- compliance and governance risk (e.g., ethics, regulatory, international trade, privacy); and
- operational risk (e.g., IT security and privacy, supply chain, labor issues, natural disasters).

Another way for businesses to categorize risks, according to compliance expert Paul Kirvan, is to bucket them under the following four basic risk types for businesses: people risks, facility risks, process risks and technology risks.

The final task in the risk identification step is for organizations to record their findings in a risk register. It helps track the risks through the subsequent four steps of the risk management process.

BENEFITS AND CHALLENGES OF RISK MANAGEMENT

Effectively managing risks that could have a negative or positive impact on capital and earnings brings many benefits. It also presents challenges, even for companies with mature governance, risk and compliance strategies.

Benefits of risk management include the following:

- increased awareness of risk across the organization;
- more confidence in organizational objectives and goals because risk is factored into strategy;
- better and more efficient compliance with regulatory and internal compliance mandates because compliance is coordinated;
- improved operational efficiency through more consistent application of risk processes and control;
- improved workplace safety and security for employees and customers; and
- a competitive differentiator in the marketplace.

The following are some of the challenges risk management teams should expect to encounter:

- Expenditures go up initially, as risk management programs can require expensive software and services.
- The increased emphasis on governance also requires business units to invest time and money to comply.
- Reaching consensus on the severity of risk and how to treat it can be a difficult and contentious exercise and sometimes lead to risk analysis paralysis.

- Demonstrating the value of risk management to executives without being able to give them hard numbers is difficult.

RISK MANAGEMENT PRACTICES

A good starting point for any organization that aspires to follow risk management best practices is ISO 31000's 11 principles of risk management. According to ISO, a risk management program should meet the following objectives:

- create value for the organization;
- be an integral part of the overall organizational process;
- factor into the company's overall decision-making process;
- explicitly address any uncertainty;
- be systematic and structured;
- be based on the best available information;
- be tailored to the project;
- take into account human factors, including potential errors;
- be transparent and all-inclusive;
- be adaptable to change; and
- be continuously monitored and improved upon.

Another best practice for the modern enterprise risk management program is to "digitally reform," said security consultant Dave Shackleford. This entails using AI and other advanced technologies to automate inefficient and ineffective manual processes.

CONCLUSION

Our business ventures encounter many risks that can affect their survival and growth. As a result, it is important to understand the basic principles of risk management and how they can be used to help mitigate the effects of risks on business entities.

There are several areas where progress is required. Development in these areas would have a significant effect on risk management, by producing:

- A set of risk management tools and techniques which are fully integrated with project and business processes, with the existence of uncertainty being recognized and accepted at all levels (via integration of risk management).
- Improved analysis of the effects of risk on project and business performance, addressing its impact on issues wider than time and cost (via increased depth of analysis and breadth of application), and covering both threats and opportunities.
- Proper account being taken of human factors in the risk process, using assessment of risk attitudes to counter systematic bias and build risk-balanced teams (via behavioural aspects).

Attention to these areas will ensure that risk management continues to develop. Risk management must not remain static if it is to fulfil its potential as a significant contributor to project and business success, and if it is to take its place as an indispensable and effective management tool.

REFERENCES

1. Ali, Mashhud. 2006. Risk Management. Jakarta: PT Raja Grafindo Persada.
2. AS/NZS 4360:2004, Australian/New Zealand Standard Risk Management, Joint Technical Committee OB-007 Risk Management, 31 Agustus 2004.
3. Committee of Sponsoring Organization (COSO) of the Treadway Commission. What is COSO: Background and Events Leading to Internal Control-Integrated Framework. 1992.
4. Chapman, Christy. Bringing ERM into Focus. Internal Auditor, June 2003.
5. Darmawi, Herman. Risk Management. Bumi Aksara, 2005.
6. Djojosoedarso, Soeisno. Principles of risk and insurance management. 1999. Jakarta: Salemba Empat.
7. Iban, Sofyan. 2004. Risk Management. Jakarta: Graha Ilmu.
8. Kasidi. 2010. Risk Management. Jakarta: Ghalia Indonesia.
9. Mulyawar Setia, 2015, Risk Management, Bandung: CV of Faithful Library.
10. Simmons, Mark. COSO Based Auditing. The Internal Auditor, December 1997 The Institute of Internal Auditors. Internal Control
11. Simmons, Mark. COSO Based Auditing. The Internal Auditor, December 1997 The Institute of Internal Auditors. Internal Control.
12. Sumani. 2009, Risk Management, Mojokerto: Global People.
13. Vaughan, Emmet. Fundamental of Risk and Insurance. 2nd, John Willey, 1978.