UNIVERSITY PARTNER

UNIVERSITY OF WOLVERHAMPTON

HERALD COLLEGE KATHMANDU

Academic Skills And Team-based Learning(4CIO18)

Report Writing

<Individual Task>

Student ID :np03cs4a220510

Student Name : Janak Gharti

Group : <L4CG17>

Lecturer : Mr.Manish Deuja

Word count. : 1867

Submitted on : <10-12-2022>

Abstract

Risk management is a way of dealing with hazards and potential threats to an organization. There are various ways of controlling a risk in an organization such as mitigation, transference, avoidance and acceptation of threats. Each of this strategy is deployed according to threat and is selected via various tools such as base lining, cost benefit analysis, benchmarking and so on. This report deals with use of these tools and strategies for identifying and controlling threats. This report also deals with OCTAVE method which is a practice in order to make plan for identifying and creating plans for risk management.

Table of Contents

Table Of Figure

1. Introduction

1.1 Definition

Risk management can be defined as a way of dealing with hazards. It is the logical process of identifying risks and deciding if those risks need to be prevent or leave them uncontrolled. (Federal Aviation Administration, 2009) Risk management consists of various activities such as recognition of risk, risk assessment, developing or coming up with strategies to maintain it and so on. It is not a new concept or a tool so a lot of standardization has been done. ACT 2004, FAA 2007, HB 2004 are couple of document that are available regarding this topic. It is a very important part of decision making in an organization. (Berg, 2010) According to guide book on risk management issued by The State of Queensland "risk management is the process of identifying, assessing and responding to risks, and communicating the outcomes of these processes to the appropriate parties in a timely manner." (Queensland Treasury, 2011)

1.2 Aims and objective

The main aim of this report is to study about various risk management and control strategies such risk avoidance, transference, mitigation and avoidance. This report also deals with Cost Benefit Analysis (CBA) and OCTAVE method.The objective of this report is to understand various risk control strategies and learning which one to select or use in various situations.

2. Background

2.1 History

The study of risk management is said to started after the World War II during late 1950s and early 1960s. There was no document available regarding risk management at that time and universities also did not offer any courses related to risk management. The first book regarding this field of study was published in 1963 by Hedges and the second book was published a year later by authors William and Hems. (Dionne, 2013)

2.2 Control Strategies

Risk control strategies can be can be divided into four basic types which are avoidance, transference, mitigation and acceptance. Each of these strategies are explained below.

2.2.1 Avoidance

Avoidance is considered to be one of the best risk control strategy. It is done by avoiding the activity containing the risk altogether. (Anon., 2016) This strategy is mostly used is mostly used when the activity is very dangerous and contains very high chances of loss or serious injury, it is also used when risk is beyond organizations or individuals control and does not necessarily fulfill any goals. (OSBIE, 2016) This strategy is often used when risk of the activity to be conducted exceeds the risk appetite of the organization.

2.2.2 Transference

Transference is the strategy where any unwanted risk or uncertain risk of an organization is transferred to another person or organization. Risk transference is done via various means and the most popular ones are contracting and insurance. Contract can be defined as a written or oral agreement that prevents involved parties from doing something, in this case activities containing risk. Insurance is other hand is the means of protecting against unexpected loss. Insurance can be purchased from insurance company. (Crane, et al., 2013) Risk may be completely transferred or even partially transferred.

2.2.3 Mitigation

Risk mitigation deals with creating plans and developing option in attempt to reduce the damaged caused by the exploitation on vulnerabilities. (islingtoncollege, 2012) (The MITRE Corporation, 2013) This strategy includes three types of plans which are explained below;

I dent response plan

Incident response plan or IRP is a well organized approach to addressing a security breach or attacks. It is a set of written instructions which minimizes the damage and reduces recovery time and cost. (Rouse, 2016)

Disaster recovery plan

Any events that disrupts the flow of work in an organization is called disaster. (IBM, 2007) It can be fire, earthquake, hurricanes etc. Disaster recovery plan or DRP is a short term recovery plan. When a disaster occurs in an organization this plan ensures the continuity of the work flow in an organization. (Rouse, 2016) Some time the scale of disaster is too big to be managed by DRP in which case Business continuity plan (BPC) is deployed. (islingtoncollege, 2012)

Business continuity plan

When DRP fails to recover an organization after a disaster Business continuity plan is deployed. It is a long term recovery plan which ensures the survival of an organization. It is procedures for activation back plans such as back up servers, data center etc. in case of major disasters such as terrorist attacks, fire breakout etc. (islingtoncollege, 2012) (CPNI, N.d)

2.2.4 Acceptance

Acceptance is a risk control strategy that depends on how much an organization risk appetite is. If the activities have far more benefits than it has drawbacks, then this strategy is deployed. (Cowan Insurance Group, 2013)Using this strategy also depends on various factors such as reputation, mission, future benefits etc. (Metheny, 2013)

2.3 Risk Appetite

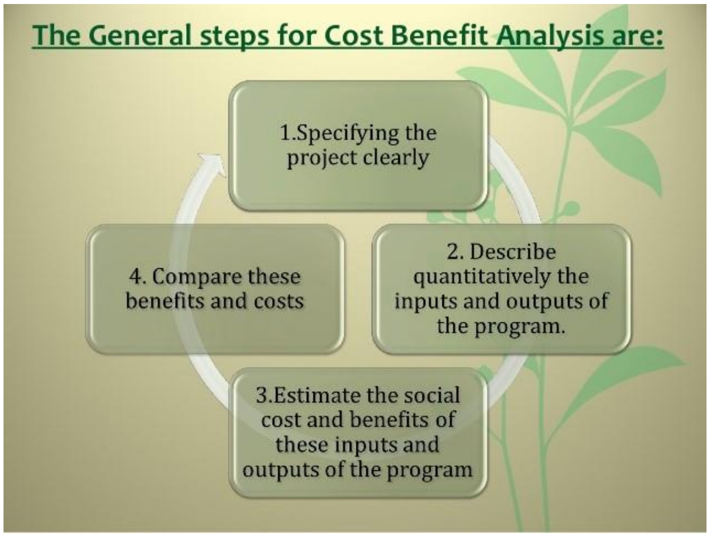
Risk appetite can be defined as the amount of risk an organization is willing to take in order to fulfill their end goals. Knowing an organization risk appetite is extremely important for selecting a risk control strategy. (Institute of Risk Management, 2016) Risk appetite of an organization can be figured out via various methods such as benchmarking, CBA, gold standards and so on. (islingtoncollege, 2012)

2.4 Selecting risk control strategy

2.4.1 Cost benefit analysis

Cost benefit analysis(CBA) is an analytical tool that determines whether or not a control strategy is worth implementing. (Tech target, 2011) The cost of implementing risk control strategy for the activity is first taken and after that the cost is compared to the benefit from the implementation of the strategy. (Wethli, 2014) This is done via CBA formula

[CBA = ALE(prior) – ALE(post) – ACS]. In this formula ALE(prior) stands for Annualized loss expectancy before the strategy is implemented and ALE(post) is the ALE examined after the strategy for risk control is implemented whereas ACS stands for Annual cost of safeguard. (islingtoncollege, 2012)



The General steps for Cost Benefit Analysis are:

1.Specifying the project clearly

2. Describe quantitatively the inputs and outputs of the program.

3.Estimate the social cost and benefits of these inputs and outputs of the program

4. Compare these benefits and costs

Figure 1: The General steps for the Cost benifit Analysis

2.4.2 Alternative to Cost benefit analysis

CBA is not the only tool for selecting a risk control strategy. There are various other tools such as benchmarking, government recommendation, due care and due diligence and so on.Benchmarking is done by studying the practices of similar organization that achieve the desired goals or objectives whereas due care means the government enforced security measures in an organization and due diligence refers to whether an organization is implementing and maintaining the standards. These standards are known as due care standards. Another popular alternative for CBA is government regulation. It is very useful for organization and industries that are maintained by government agencies. It is also considered as source of information on what some organizations might be doing for controlling the risk. (islingtoncollege, 2012)

2.5 Risk control practices

There are various risk control practices such as Delphi technique, qualitative measures, OCTAVE method etc. This report focuses on OCTAVE method which is explained below.

2.5.1 The OCTAVE method

The term OCTAVE stands for The Operationally Critical Threat, Asset and Vulnerability Evaluation. It is a framework that allows organizations to analyze and understand their information security risks. It is not a product but rather a process to identify threats and address them. (Panda, 2009)

In order to identify and address the issues the OCTAVE method uses a three phase approach. (islingtoncollege, 2012) The phase 1 of this method is to Build asset-based threat profiles. It deals with identifying assets of an organization and what is being done to protect them, after that flaws or threats in those practices are identified regarding each asset and threat profile is created. Phase 2 is Identifying infrastructure vulnerabilities. It deals with identifying key components or critical assets and determine up to which extent they are exposed to threats. The final phase or phase 3 is to Develop security strategy and mitigation plans. In this phase the information that are gathered in phase 1 and phase 2 are thoroughly analyzed and then is used to develop plans to protect the assets and to mitigate the risks. (The CERT division, 2016) (Panda, 2009)

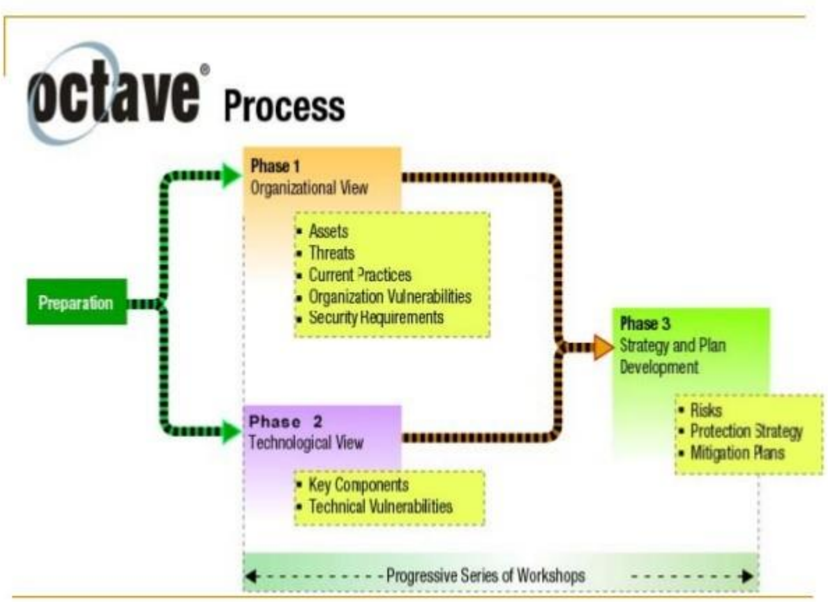


Figure 2: Octive Process

3.Analysis

There are various risk control strategies and each of them are useful according to place, condition or the type of risk. These strategies are selected via various methods and feasibility study. One of the most popular tool for selecting the risk control strategy is Cost benefit analysis but it is mostly useful when the risk is related to cost such as development cost of software and whether the benefits outweighs the cost or not. What this tool does not take into consideration are the factors such as organizations reputation and future prospects for current loss. There are various alternatives to CBA. Benchmarking and government recommendations use other organizations practices in order to create or select the risk control strategies. While some organization study other organizations there are some who study their own practices and improve upon then which is known as base lining. There are various risk control practices followed by organizations in order to identify and deal with risks.

4. Conclusion

Risk management and risk control is an integral part of any organizations policy. It is very necessary to identify the risks in an organization and come up with a plan for dealing with it. It is extremely important for an organizations growth and future. Without a risk control strategy, it is very difficult for an organization to grow or even exist in the long run. So, risk management and control plays a vital role in an organization progress and success.

5. Reference

5.1Appendix

5.1.1 Appendix A (abbreviations)

ACS	= Annual Cost of Safeguard
ALE	= Annualized Loss Expectancy
BCP	= Business Continuity Plan
CBA	= Cost Benefit Analysis
DRP	= Disaster Recovery Plan

IRP	= Incident Recovery Plan
OCTAVE	= Operational Critical Threats, Assets and Vulnerability Evaluation

5.1.2 Appendix B (presentation slide)