Sri Lanka Institute of Information Technology

Proactive Policy Development for Risk Management

IE3072 – Information Security & Policy Management

Group Assessment Report

Submitted by:

Student Registration Number	Student Name
IT19029146	Eranda H.P.D
IT19040936	S.M.Rathnayaka
IT19029214	J. C. Hapuarachchi
IT18220902	Mandhanayaka D. D

22/08/2021
Date of submission

Table of Contents

Abstract

As the 3rd year 2nd semester Cyber Security undergraduates at SLIIT, under the module **IE3072 – Information Security & Policy Management,** we were asked to create a report for any "organizational policy" related topic that were provided by the Lecturer-In-Charge. So, we were given the freedom to choose any topic as per our wish. After having several discussion rounds with my fellow team members, we have decided to choose the topic **"Proactive Policy Development for Risk Management"** for this assessment.

So, in the assessment, we are supposed to create a full report of 15-20 pages about the selected topic. After the report is completely done, we are supposed to create a 15-minute video summarizing the contents of the above report. The main learning outcome from this assessment is to gain the ability of critically evaluating the Information Security Policy and Management practices.

This report would not have been a success without the kind and consistent support from our lecturer in charge Ms. Chathurangika Kahandawaarachchi. So, first of all I would like to thank our lecturer, Ms. Chathurangika & other fellow instructors for providing their kind support and guidance throughout the assessment.

For the ease of understanding, we have divided our main topic into several sub sections. So, it would be much easier when allocating the marks as well.

1) Introduction to the Proactive Risk Management
2) Significance of Proactive Policy Development for Risk Management
3) Critical Evaluation of the Proactive Policy Development
4) Conclusion and Recommendations

Introduction

Today, we all are living in a modern technological era that quickly adapts according to new innovative ideas. When the organizations all around the globe are considered, most of them have already adapted for this new technological era. However, with the modern technological improvement, currently organizations are facing massive amounts of threats annually. Some of those catastrophic threats are capable of bringing a particular organization at their knees too. So that, the Risk Management has already become a vital necessity for each and every organization in the modern world. A particular organization's success completely depends on their implemented risk management framework. Having a proper risk management framework establishes a strong confidence within both the employees & stakeholders of the organization.

However, when it comes to the risk management, there are 2 different approaches of performing it [1].

1) Reactive Risk Management
2) Proactive Risk Management

The key differentiation factor among those 2 approaches is the **timeframe that the risks are handled**. So, the additional information on **Reactive Risk Management** & the shortcoming of that particular approach will clearly be explained later in this report. When it comes to the proactive risk management, it always tries to avoid or manage potential risks towards the organization. Basically, in the proactive risk management, the organization plans & prepares for the worst-case scenario that may occur in the future [1]. So, in order to achieve this ultimate goal, they implement various sorts of proactive risk management polices within their organization [7]. As the very 1st step, the risk management team of the organization performs a critical assessment to identify the potential risks towards the organization. Then they prioritize those risks according to the appropriate risk levels. After that they develop a comprehensive contingency plan to mitigate those risks much as possible. As the final stage, they implement necessary mitigation mechanisms in a timely manner. Furthermore, proactive policy development helps an organization to frequently keep up with new emerging security risks that occurs in the world. Additionally, due to the proactive risk management policies, organizations tend to make much accurate decisions as well.

Significance of the topic

Importance of Risk Management Policies

An organization can save money and ensure its future by developing a risk management plan and considering the many risks or events that may occur before they occur. This is because a strong risk management strategy aids a company in developing action plans to limit possible threats, reduce their impact, and deal effectively with the results. Companies can be more confident in their business decisions if they can recognize and control risk. Furthermore, solid corporate governance standards, with a particular emphasis on risk management, aid a company's achievement of its objectives [1].

Risk management has the following benefits [2]:

- Provides a safe and secure workplace for all employees and consumers.
- Increases business operations' stability and lowers legal liability.
- Reducing the events that bring negative impacts to the organization.
- Provides protection for both the corporation and the environment in the case of a disaster.
- All connected people and assets are protected from actual risks.
- Assists in confirming the company's insurance requirements to avoid paying needless premiums.

The steps that make up the overall risk management process are the same in all risk management plans:

- Establish context
- Risk identification
- Risk analysis,
- Risk assessment and evaluation,
- Risk mitigation,
- Risk monitoring,
- Communicate and consult.

Why proactive policy making is more suitable for risk management?

No matter either it is proactive policy or a reactive policy, all the policy making procedures are same. All policy makings happen according to the policy cycle. Policy cycle can be customized. It is not required for all the policy making processes to have all the 6 stages or can have even more than 6 stages. When compared with reactive policy making, proactive policy development is more suitable for risk management. As in proactive policy development will help in prevent the risk from happening. Reactive policy development is a reaction for a particular event. If an attack or any kind of event bring damage to an organization, then the management thinks of developing policies. This way is not recommended. There can be situation in which an event or an attack can bring a large impact to the organization that even there is a possibility that organizations can become bankrupt due to high damage. To prevent these sorts of things it is recommended to develop the required policies before a bad thing happens and to prevent the bad thing from happening or prevent the organization from getting impacted.

Proactive Policy Development vs Reactive Policy Development

Proactive Policy development	Reactive policy development
More prepared for upcoming events and unpredictable events.	Unprepared for upcoming events and unpredictable events.
Knowing exactly what to do (how to react) during an emergency.	Not sure what are the steps to be taken during an emergency.
Faster recovery.	Slower recovery.
Better customer satisfaction.	Lesser customer satisfaction.

Critical Evaluation of the topic

What is Risk?

Simply risk can be defined as the condition that will occur from a certain activity. It is situation in which a person/system/asset is exposed to any sort of danger. Risk is not a certain event. It is an uncertain event which will happen in future and will affect the objectives of any sort of organization. Risk can occur in any part of the organization. Risk can be classified into various types as [5].

***Business/Operational risk* -** These are the risks that an organization might face while doing the business daily activities and processes. Most of the time, Operational risk happens due to humans. Human factor give arise to business/operational risk. Humans' decisions sometimes lead to failures and humans make mistakes. These failures and mistakes are the key factors that give arise for business/operational risk [6].

***Environmental risk* -** Environment risk is the type of the risk that occur due to environmental changes. Environment risk has a global impact. Due to lack of required methodologies in waste management, waste transport and waste disposal, humans may be affected in the long run.

***Country risk* –** This is the risk which is associated with the decisions that affects the entire country. Most of the time political decisions give rise to country risk. Other than that, from overseas taxation, involvement of overseas parities can give rise to country risk [5].

***Financial risk* –** Financial risk is associated with credit operations and procedures in a certain organization. This type of risk can be classified as.

i. ***Credit risk*** → The losses that might occur if another company fails to work according to the contracts that are developed between organizations.
ii. ***Currency risk*** → The value of money can change and fluctuates with the fluctuation that happening currency levels (Foreign exchange rate).
iii. ***Interest rate risk*** → Fluctuation in interest rates might affect the organization.
iv. ***Liquidity risk*** → This is kind of a risk that an organization faces when realising a product for the market.

What is Risk management?

Risk management can be defined as process to understand about the risks that a particular organization have and then managing the identified risk in the most suitable way. To manage risks there are risk management plans. By implementing a risk management plan the organization can save their business from the possible risks, consequences and to protect the future, well-being of the company. Risk management provides various benefits for organizations. Risk management is important for any organization either it is small organization or a large organization [7]. Some benefits of risk management are.

- Providing an environment for the employees to do their activities in a secure and a safe manner.
- Increases business stability and decreases legal liability.
- Protects the company/organization from harmful events that effects the company, employees, and environment.

Mainly there are **5 steps** in risk management.

1. Risk Identification
2. Risk Analysing
3. Risk Evaluation
4. Risk response planning
5. Monitoring and reviewing risks

Risk Identification → Identifying every possible risk in the given scope in an organization. Need to consider about every possible risk such as environmental risk, financial risk, reputational risk etc.

Risk Analyzing → In this step the identified risks are analyzed. This step mainly focuses on giving a value for the risk. To calculate the value of the risk, the equation **Risk = Impact * Likelihood** is used.

Risk Evaluation → According to the values of the risks, risks are prioritized.

Risk response planning → In here the controls for the prioritized risk will be selected.

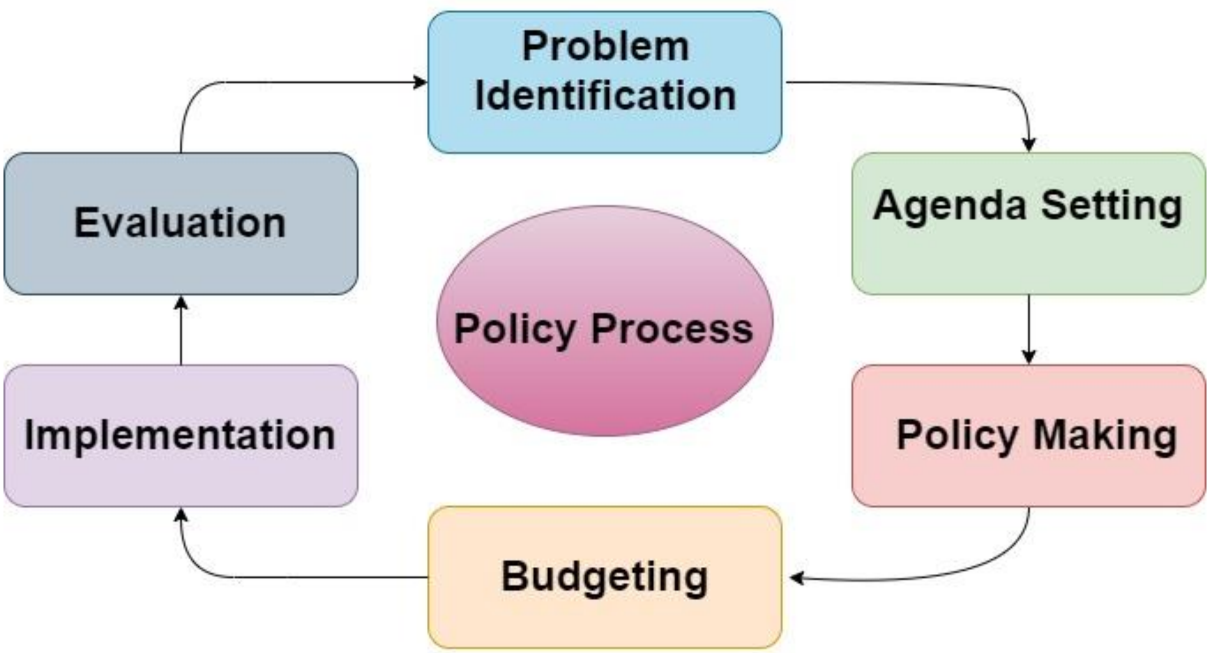
Monitoring and reviewing risks → After the controls are selected, the controls will be implemented. It is necessary to monitor and review the implemented controls continuously in order to make sure that implemented controls are effective and the organization do not uselessly waste money on controls, in which there is not any risk [8].

What are policies?

Policies are simply a set of rules or guidelines that can be used by an organization to follow in order achieve organization objectives. The purpose of policies is to explain the employees what the organization wants and how the organization want it to happen.

How to develop policies?

To develop policies there is a cycle that need to be followed. This is called as policy process.



Problem Identification → Determine the root cause of the problem and build up a problem statement. In this the organization should decide whether this problem need a policy or not. If the identified problem needs a policy, it is required to start the policy building journey.

Agenda setting → In this step it is required to focus every setting that is involved in the problem. Need to identify every possible harmful event that the problem will give rise to.

Policy making → After the problem are identified and according to the problems that are identified, policies must be created to address the identified problems. Then the created policy formulations must be authorized under an appointed panel.

Budgeting → The management should determine how much of budget will be allocated for each policy. Before budgeting for a particular policy, it is required to authorize and adopt a policy.

Implementation → There are agencies who are responsible to implement policies.

Evaluation → After implementing policies it is required to find out whether the implemented policy is effective. Need to continuously monitor whether implemented policies are solving the identified problems.

Shortcomings of reactive policy development for Risk Management

Risk management is an important part of any effective planning strategy and overall business strategy. Risk recognition and mitigation are beneficial to businesses in a variety of ways. Risk management programs have traditionally used a reactive approach to risk assessment. These risk management programs were designed to assess, report, and reduce risk with a focus on limiting the company's damage and minimizing impact [1].

Reactive risk management focuses primarily on events rather than causes and is based on responding to risks that have already affected the company. It has limited problem-solving capabilities because it lacks predictive analysis and innovative problem-solving capabilities.

The biggest issue with reactive risk management is Investigation and mitigation of future events takes place only after the company has been adversely affected. The affect varies. If a large part of the organization gets affected or if the organization gets affected financially in a large scale it will cause a problem.

Procurement management needs to be more forward-looking to maintain a competitive advantage, address security issues and safeguard current and future profitability. Proactive risk management enables businesses to identify and minimize (or eliminate) potential risks before they affect the business [1].

Proactive Policy Development for Risk Management

Risk management allows a company to predict, minimize, or manage current and potential threats. Organizations that practice proactive risk management are quick to adapt and respond to bad events or crises. Simply put, proactive risk management helps a company plan for tomorrow's worst situation [1].

Proactive risk management integrates and replaces reactive risk management. Because reactive risk management solutions are used to develop preventative actions against known issues but do nothing to protect against future risks.

The way risks are analyzed, disclosed, and mitigated distinguishes a proactive risk management approach from a reactive approach. These include carefully studying a situation or evaluating processes to identify potential risks, identifying risk drivers to understand the underlying cause, assessing the probability and impact of prioritizing risks, and developing an emergency plan accordingly. Risk managers need to learn to analyze the strengths of an organization's innovation component and use that information effectively against existing and new risks to achieve this. Also, focus on utilizing the skills of experienced risk managers to apply strategic risk management [3].

This proactive risk management includes solving new problems, making analytical predictions, and highlighting the root causes of risks, using a comprehensive analysis of historical, current, and future databases to identify risks.

This risk management method is linked to the human factor of creative thinking and human solution, using tools such as artificial intelligence (AI), process automation, and data analysis. In here various methods are designed and tested to identify the root causes of risks and to apply human intelligence as well as to reduce or adjust the risk of bringing the company's risk to an acceptable level through machine learning [3].

By taking a proactive approach to providing a consistent, formal, and positive customer experience, organizations can limit the number of risks that can interfere with a positive customer experience. Minimizing, if not eliminating, such hazards protect the brand's reputation, profit, and regulatory compliance.

The main objectives of Proactive Risk Management [2]:

- Identify risky behaviors at early stages.

- Identify the root causes before an incident occurs.

- Understand the security inputs of the program - that is, the basic reasons for secure performance.

- Reduce the impact to the organization if any bad thing happens.

- Prevent problems, risks, or any sort of emergencies from happening.

- to provide a strategic approach and to implement policies that will bring a positive change for the organization.

- Knowing exactly what thing(steps) to do during an emergency.

- Recovering from disaster faster and easier.

- Becoming prepare or ready for any kind of unpredicted event.

There are several key elements that all proactive risk management models should share [3]**:**

- Risk assessment
- Timely reporting of potential risks
- Effective mitigation measures
- Managing emerging risk groups
- Prioritize risks
- Prepare a detailed emergency plan
- Review policies annually or after a significant change

Benefits of Proactive Policy Development

1) Gives control

Instead of waiting for a disaster or danger to come, organization can prepare. This method provides control and allows organization to choose what the consequences will be. Proactive management includes constant monitoring of systems, processes, cyber security, competition, market trends, weather etc. All risks must be regularly monitored as part of a proactive approach. It also includes frequent risk assessments to keep the organization up to date on current and emerging risks. This method ensures that management is continually informed about risk trends. While looking for strategies to reduce long-term risks, management may decide to prioritize short-term potential risks. The organization can monitor key risk indicators and update risk levels when risk levels rise or decline [4].

2) Helps limit exposure

Companies must incorporate proactive risk management into their risk culture as a continuous activity. The identification of risks can take days, weeks, or even months. Companies can, however, anticipate risks and devise strategies to avoid them after they have been discovered. The typical approach to any risk is always one of corrections, which aims to fix a problem after it has occurred. It is much easier to neutralize dangers and restrict exposure if you go from a reactive to a proactive approach [4].

3) Saves resources

Once a threat has occurred, managers are bound to spend more on cleaning than planned for it. By looking at risk in advance, organization can find ways to minimize risk and save business from big losses.

4) Continuous improvement

A proactive approach requires constant monitoring of risk and internal processes so that the company can continue to improve as it seeks to reduce risk. Also, learning more about the risks and ways to prevent them can improve decision making. Management will get more confidence from the partners as the organization is ready for anything [4].

Conclusion & Recommendations

Risk is an unguessable and unpredictable thing. Also, most importantly nobody can maintain a process without having any risk. When comes to the business point of view, nowadays most organizations are looking forward and identify what are the major risks that they need or have to face in the future.

Risk management plans are very important fact when considering the business continuity. A good risk management plan will help the organization to achieve their milestones in future. Basically no one can prevent the risks or avoid them permanently. The only thing we can do is establish a good risk management plan and work on that. We can define risk briefly in this manner: There are internal and external forces at work in organizations that make it difficult to predict whether or not they will accomplish or surpass their goals. Risk is the result of this uncertainty on the organization's goals. Furthermore, a good risk management plan can have some serious benefits to the organization. As an example, a good risk management plan will protect both the corporation and the environment in the case of a disaster and most importantly it will Increases business operations' stability and lowers legal liability.

When dig deep into this risk management plans, we can clearly see a common set of steps which make up the overall risk management process. Those are, establish context, Risk identification, Risk analysis, Risk assessment and evaluation, Risk mitigation, Risk monitoring, Communicate and consult. When preparing the risk management plan the organizations should be aware about what are the available risk types and how they categorized into different scenarios. Basically, there are 5 varies of risk such as business, operational, environmental, regional and financial. According to these classification organizations can identify and sort out their risks according to a damage level.

After developed a risk management plan organization's internal body needs to implement policies to provide guidance regarding the management of risk to support the achievement of corporate objectives, protect staff, and business assets and ensure financial sustainability. Furthermore, we can simply define policy as a set of rules or guidelines [9].

On the other hand, policy statement is like a tool for organizations to determine and respond to risks in a way that minimizes their impact. In order to implement a good policy statement companies must have to go through a process. Which is Problem Identification, Agenda setting, Policy making, Budgeting, Implementation and Evaluation After dig deep into risk management policies, we can find two major categories. Those are reactive policies and proactive policies.

When considering about the reactive policies, it can be defined as the policies which designed to remedy problems that already exist. These policies are useful only when the incident happened. The main disadvantage of reactive policies is these policies cannot prevent the upcoming risks. Due to that reason reactive policies don't do get much effective results when comparing with the proactive policy development.

In proactive policy development there are more effective results, because when developing the proactive policies organizations are considering their future. due to that reason, they can prepare for upcoming, unpredictable events. The most important thing is that many researchers prove that proactive policies are gaining a faster recovery after a disaster. In this report we identified some main benefits of proactive policy development. those are,

1) **Gives control to the organization and they can prepare for an unpredictable event with identified consequences.**
2) **neutralize dangers and restrict exposure.**
3) **organization can find ways to minimize risk and save business from big losses.**
4) **Organizations can continue to improve as it seeks to reduce risk and can improve decision making process.**

Finally, after studying this report, we can clearly identify proactive policy development has some greater benefits to the organizations. Also, this approach will drive companies to a sustain future profitability and growth using future predictions. Due to these facts, preparing to future incidents is always better than repairing the damage [10].

Recommendations

It is always good to have some risk prevention mechanisms with company's risk management plans in order to achieve higher growth and profitability. Most importantly, we can clearly see there are many disadvantages in the reactive approach. Due to that organizations can use proactive approaches to make organization's policy statements to fulfil their risk management plans. Most of the time organizations are only rely on reactive risk management policies. Because reactive policies are cheaper than proactive policies when implementing the policies inside the organization. Furthermore, in practically we can find only few applicable proactive policies. Hence, it's always good to do some research regarding practical approaches of the proactive policies for risk management.

References

[1] L. DelVecchio, "planergy.com," 25 08 2019. [Online]. Available: https://planergy.com/blog/proactive-risk-management-approach/

[2] T. Britton, "http://aviationsafetyblog.asms-pro.com," SMS, 18 04 2018. [Online]. Available: http://aviationsafetyblog.asms-pro.com/blog/aviation-sms-proactive-risk-management-4-activities

[3] "metricstream.com," [Online]. Available: https://www.metricstream.com/insights/proactive-risk-management-approach.htm.

[4] "moneyoutline.com," 2020. [Online]. Available: http://www.moneyoutline.com/risk-management-strategies-for-your-business-proactive-vs-reactive/

[5] Jasmin Harvey, "Introduction to managing risk," 05 04 2008 [Online]. Available: https://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_intro_to_managing_rist.apr07.pdf

[6] Bibliography [1]T. Segal, "Operational Risk," Investopedia, Sep. 13, 2020.

https://www.investopedia.com/terms/o/operational_risk.asp.

[7] B. Cole, "What Is Risk management?," SearchCompliance, 2019.

https://searchcompliance.techtarget.com/definition/risk-management

[8] C. Reddy, "Advantage and Disadvantage of Risk Management - WiseStep," WiseStep, Oct. 12, 2018. https://content.wisestep.com/advantage-disadvantage-risk-management/

[9] D. Sarokin, "What Is a Risk Management Policy Statement?," 01 September 2020. [Online]. Available: https://smallbusiness.chron.com/risk-management-policy-statement-68528.html. [Accessed 17 August 2021].

[10] Metricstream , "Proactive Risk Management - The Key to Business Excellence," Metricstream , 10 January 2020. [Online]. Available: https://www.metricstream.com/insights/proactive-risk-management-approach.htm. [Accessed 17 August 2021].