Risk Management Plan Initial Draft: Risk Assessment Plan And Risk Mitigation Plan

Introduction

Risk is a situation where there is a chance of a positive or negative impact, which can affect the outcome of a project. During the procedure of a project, the risk factor is called Risk Management. The purpose of Risk Management is to reduce the output of events that affects the project. The processes related to Risk Management include Risk Management planning, analysis, control and identification. The risks of the project must be recognized before the project is started. As the project proceeds, risks also increase. When risk is recognized, it should be properly analyzed in regards to the impact, cost, probability, probability of occurrence, and then it must be set accordingly. All risks recognized must be written down in a Risk Register which is known as a Risk Statement.

However, in documenting a risk, there are two more significant factors which must be mentioned. They are; Mitigation steps and Contingency plan. Mitigation steps have a significant loss. Occasionally, the loss of mitigating risk can go beyond the loss in assuming and experiencing the risks. Before implementing the contingency plan, it is necessary to assess the probability and result of each risk against the mitigation cost strategy. Contingency plan that are applied before the occurrence of risk, are prepared actions projected to eliminate the impact of risk. If contingency plan occurs after the occurrence of the risk, it can only reduce the impact of risk. Therefore, identification and documentation actions that lead to the risk outcome in regards to the project are just the initial and first step. Timely monitoring of all risks, by a Risk Management team must be carried out equally, and it must be further mentioned in the Project status Report.

Purpose: This plan gathers all the records related to procedures and tools that will further be used to direct and manage those actions that can have a negative result on the HNetExchange, HNetPay, and HNetConnect products. It consists of a document, which is used in controlling and managing all the risks related to the project. This plan includes Risk Management Planning, Risk Assessment and Risk Mitigation plans.

Importance

Risk is such a dangerous event that it can stop the progress of the project as planned. The project might be left as incomplete due to the risk factor. Risks can be recognized from many different number of sources. Some risks are well-known and can be recognized even before the start of the project. Other risks can be recognized when the project is being carried out, and it can also be recognized by anyone who is related to this project. Some risks are built into the project while the other risks are affected due to external power that is outside the source and control of the project team

Outline of Plan

The Risk management plan demonstrates the strategies with which Risk management is done. There are multiple activities under a risk management plan. All potential risks and stakeholders are identified in this plan. Afterwards, a Risk assessment is performed on a Risk Assessment worksheet and then a Risk mitigation plan is devised.

Scope

The scope of this Risk assessment plan is confined to products of Health Network, Inc. that are: HNetExchange, HNetPay, and HNetConnect.

Compliance Laws and Regulations

Compliance risk is known as integrity risk. Organizations like Health Networks, Inc. must make sure that it is GDPR Compliant. If not so, GDPR can cost many organizations millions of dollars. In addition to that, the company should follow the data breach rules of the state. The rules state that companies can't enforce data to be stored of individuals, especially patients, for reasons not known to the individual. Personal data includes: Names, Photos, Social Security numbers, Banking information, Email addresses, Social media posts, Medical information, IP addresses and Addresses. Laws pertaining in EU and US data breach laws must also be followed for customers using the services from those geographic areas.

Key Roles and Responsibilities

The entire responsibility of the project risk management rests with the Project Manager. The entire tasks specific to project risks are distributed among team members, to eradicate the risk of the project. When a project is being carried out, in all the stages of a project, Risk identification is a topic that will always be discussed. The objective of this discussion is to train the project team on risk awareness, identification, communication and documentation, and how to react in all related conditions.

Schedule for risk management planning process

Activity Timeline Comments

Identify risks of HNetConnect 1 week N/A

Assess risk of HNetConnect 1 week N/A

Identify risks of HNetPay 1 week Due to the criticality of this module, it needs proper time for financial modules to be assessed and risks to be identified.

Assess Risks of HNetPay 2 weeks N/A

Identify risk of HNetExchange 1 week N/A

Assess Risks of HNetExchange 2 week N/A

Collective Risk Assessment Report 2 weeks A report containing risk assessment of all three modules must be devised at the end of each assessment.

Risk Assessment Plan

Introduction

In risk awareness, every team member must be knowledgeable to the degree of risk within the project. They must also know the factors that could strongly affect the risk in either a positive or a negative way. In Risk Identification, team members must be able to analyze the risk that can have a strong impact on the project. Plus, the documentation of each characteristic of risk must be done. Risk communication involves acknowledging the risk factors to the project managers and team. It is always the responsibility of HNetExchange, HNetPay, and HNetConnect project managers to support the whole project team and the other stakeholders with identification of risk and record the known risks in the Risk Register. After the change in the factors of risk, the Risk Register must be updated and restructured accordingly.

The Risk management team will talk about the new and latest risk factors that will be analyzed by the HNetExchange, HNetPay, and HNetConnect Project Managers. The Project Manager will further sort out to eliminate the identified risks, and will perform risk quantification and risk response development. When the risk is addressed to the HNetExchange, HNetPay, and HNetConnect Project Manager via email or communication, it is necessary for the Project Manager to record this in the Risk Register. When a new risk is reported, there are some items that must be included in the Risk Register.

- Quality Impact- A risk can cost the project in lessening the quality of function or the outcome. This can damage the whole project and the hard work dedicated to the project can go in vain.
- Scope Impact- This contains the impact, the risk will have on the predicted objective of the project.
- Scheduled Impact- The risk factor can affect the number of hours, days, and months etc. that are allocated for the completion of project. Due to risk, the project may not be completed on time and can be delayed.
- Probability that the event will occur- The risk factor is always associated with the probability of its outcome. Usually there is always 50% chance of the occurrence of risk factor.
- Cost Impact- Risk factor of a project can affect the cost of the budget. The planned budget of the project can be increased which can lead to loss.
- Description of the risk factor- The risk factor must be completely and clearly defined, to analyze the factor.

Outline

In this plan, we mention the Probability of Occurrence matrix with standard values. We also mention the Risk Assessment Plan by stating Risk factors, there impact and their Priority.

Scope

The scope of this Risk assessment plan is confined to products of Health Network, Inc. that are:

HNetExchange, HNetPay, and HNetConnect.

Summarize RA approaches

There are various Risk Assessment approaches for risk management. Some of them are:

1. what-if analysis: in this method, what-if questions are asked to know what can potentially go wrong
2. Checklist: in this method, the known threats and hazards are listed down that are mentioned in assignment description.
3. hazard and operability study (HAZOP): In this approach, a detailed analysis is performed with an interdisciplinary team to make sure the in-depth knowledge of operations and threats along with their causes
4. Failure mode and effect analysis (FMEA): in this approach, potential failures are identified and it is found out that which failures would have what effects. Each element within a system is analyzed for potential failure points.
5. Fault tree analysis (FTA): In this approach, all those things are identified that could potentially cause a catastrophic event. One by one, an event is taken and possible causes towards that event are figured out.

For the Risk Assessment of Health Networks Inc., the following Probability matrix is used:

The key roles and responsibilities of individuals

- Risk Identification: All project stakeholders, beta customers, Testing Team
- Risk Registry: Project Manager
- Risk Assessment: All project stakeholders, IT Team, Testing Team
- Risk Contingency Planning; Project Manager(s), Testing Team
- Risk Response Management; Project Managers, ITS Team
- Risk Reporting; Project Manager

Proposed schedule

Activity Timeline Comments

Identify risks of HNetConnect 1 week N/A

Assess risk of HNetConnect 1 week N/A

Identify risks of HNetPay 1 week Due to the criticality of this module, it needs proper time for financial modules to be assessed and risks to be identified.

Assess Risks of HNetPay 2 weeks N/A

Identify risk of HNetExchange 1 week N/A

Assess Risks of HNetExchange 2 week N/A

Collective Risk Assessment Report 2 weeks A report containing risk assessment of all three modules must be devised at the end of each assessment.

Risk Mitigation Plan

Introduction

In this document, the Risks identified in the previous two phases are now analyzed for steps on how to remove them from the system. In an ideal case, good mitigation strategy is to adopt a Cloud computing solution for all these three products of the company and adhere to their rules and regulations. The cloud providers have decent backup solutions and data centers to make sure data is never lost. In addition to this, cloud providers have infrastructure backup as their Disaster recovery solutions which make the company safe and the services are always up and running. In this document, we mention the threats that are existing and newly identified and offer the cloud related mitigation solution to that threat.

Identified threats described in the scenario

The existing threats include:

1. Loss of company data due to hardware being removed from production systems
2. Loss of company information on lost or stolen company-owned assets, such as mobile devices and laptops
3. Loss of customers due to production outages caused by various events, such as natural disasters, change management, unstable software, and so on
4. Internet threats due to company products being accessible on the Internet
5. Insider threats
6. Changes in regulatory landscape that may impact operations

New threats

As a part of this assignment, the following text highlights the new threats that can be

HNetExchange

Identified Threat Probability Qualification Mitigation technique

Are the rules GDPR Compliant? H Make company GDPR compliant

Contract breach risks with customers H Specify contracts with details

Abuse of Exchange services M Keep data in cloud

Spreading false messages with MiM attacks H Keep connections secured via VPN

Natural disasters H Deploy disaster recovery solutions

Hardware failure due to a storm. H Deploy disaster recovery solutions

HNetPay

Threat Probability Qualification Mitigation technique

A user leaves behind a Trail after a financial transaction. This leads to hackers finding him through his trail and getting money from account H Never leave trails

Shear phishing and modern smart phishing attack to steal Payment information. H Cybersecurity systems adoption

Bad encryption at back-end M Enable latest Encryption techniques

Attacks due to IoT systems and devices M Adopt Cybersecurity cloud techniques

A compromised system or financial transaction module H Deploy Cybersecurity solutions

OR

Adopt cloud computing financial transaction handling

Stolen data and Identity threats H Implement multi-factor authentication

HNetConnect.

Identified Threat Probability Qualification Mitigation technique

The tracking of location based on a GPS device that users own H Turn off GPS most of the time while being on network.

Stolen ID and user account details. H Use multi-factor authentication

Status updates based on location L Avoid tagging of location in status

Enabling stalking from profile. L Keep privacy settings under cheek.

Conclusion

Health Networks Inc. has three products for which a detailed Risk management, Risk Assessment and a Risk mitigation plan is needed. In this report, we have outlined basic factors on which risks are defined, identified, assessed and hence mitigated. Many mitigation techniques are mentioned in the report. The best, however is to adopt a Cloud computing solution and implement all three products over the cloud based on a cloud provider's' infrastructure for best services to customers with good security.