# 6.9 Risk Management Plan

## 6.9.1 Introduction

The E-Cliniq system aims to provide an Electronic Health Record and Appointment system for the Asia Pacific College’s Clinic.

The development team's duties and responsibilities, the risk assessments plan, and an overview of the risk management process are all included in the risk management plan. The plan will also describe the risk monitoring and management procedures and risk response tactics. The plan's effectiveness will be judged by how quickly threats are identified and dealt with.

The following are information that are considered when developing a Risk Management Plan for the project, E-Cliniq:

* **Identifying Risk:** The E-Cliniq system development, implementation, and operation project group ought to be aware of any potential dangers. Risks may appear from several unusual places, including technical problems, legal requirements, cybersecurity, and human factors. Risks should be identified and then evaluated for both chance of occurrence and potential effects on the project.
* **Risk Monitoring:** Risk management is an ongoing activity that needs regular observation and evaluation. To guarantee that risk management procedures are still effective, risks are updated, and new risks are discovered, the project team should establish a frequent review process. All stakeholders should be informed of any changes during the review process, which should be open and transparent.
* **Contingency Plans:** The project team needs to create backup plans for major risks that could have a significant impact on the project's success. Plans for alternatives ought to specify the actions needed to lessen the risk's effects and keep the project moving forward. As the project develops and new risks are discovered, these strategies should be periodically reviewed and modified.
* **Risk Mitigation Tactics:** The project team should create a plan for minimizing or avoiding the risks after having identified and assessed the risks. Prioritizing mitigation tactics should be done in accordance with how well they reduce risk and how easily they can be implemented in terms of both time and money. Contingency planning, redundancy, risk transfer through insurance, and the creation of fallback processes strategies.

The E-Cliniq system development team will ensure that the project is executed effectively, satisfying all objectives while avoiding potential risks by taking these extra considerations into account in a risk management plan.

## 6.9.2 Top Three Risks

1. The E-Cliniq system would not synchronize the information of the patients being recorded if the internet connection is disrupted and/or lost during the process.
2. The information cannot be transferred/exchanged safely if the internet connection is lost and if there was a problem/issue that unexpectedly occurs with the router that connects the devices together.
3. The data in the E-Cliniq system can be vulnerable with risks when it comes to new employees being hired since the core data, which is the patient’s recorded data, can be interacted by the employees.

## 6.9.3 Risk Management Approach

The steps below are to help in being able to manage risks in the E-Cliniq system:

* **Risk Identification and Assessment:** The risks will be listed in a risk register together with details about their likelihood of happening, potential effects, and description. The identified risks will be assessed in terms of their likelihood of occurring and their effect on the project. The project team will rank each risk according to severity using the risk matrix. Risks with an elevated level of severity will be prioritized for either mitigation or contingency planning.
* **Risk Monitoring:** Risks will be continuously monitored during the project. To ensure that risks are being effectively managed, the project team will frequently review the risk register. As further threats are found and added to the risk register throughout the project, the risk assessment process will be repeated.
* **Risk Mitigation:** Plans for risk mitigation will be developed for risks having a high effect and likelihood of occurrence. The risk-mitigation strategies will be included in the mitigation plans. The project team will also decide on fallback plans for risks that cannot be minimized.
* **Risk Communication:** Risk communication is the process of alerting relevant parties—including the project sponsor, the project team, and other stakeholders—about risks and related management strategies. If any risks are identified, assessed, and dealt with, the project team will keep all stakeholders informed and maintain regular communication.

## 6.9.4 Risk Identification

During risk assessment meetings, the development team and relevant stakeholders were asked to identify and evaluate risks to the project's success. The dangers that were found were listed in a risk registry.

The risks discovered during the risk assessment meeting were documented in a manner consistent with the Agile risk management plan. To guarantee that new risks are found, and old risks are efficiently managed, the risk register is updated on a regular basis. The development team will keep an eye on and manage risks all the way through the project. The following are the project's potential risks for the E-Cliniq system:

* **Human Error:** Errors made by relevant stakeholders, having the potential of having an influence on the system.
* **Security Vulnerabilities:** The initiative runs the risk of being exposed to security lapses or data loss, both of which might have dire repercussions.
* **Unforeseen Circumstances:** There is a chance that unanticipated events (such as connection loss) could have an unexpected effect on the system.

## 6.9.5 Risk Qualification and Prioritization

The development team will regularly review and update the risk record to make sure that risks are prioritized appropriately. The risks mentioned in the risk records were classified and evaluated using a probability-impact matrix. Risks that would have a significant effect on the project and a high possibility of occurring were given top consideration. Determining the probability and impact of each risk after analyzing potential risks related to the E-Cliniq system. Following is an overview of the likelihood of risks and their effects on the project:

* Extreme: Risks that could seriously harm the system and have an extremely high possibility of happening.
* High: Risks that could have a significant impact on the system and have a high chance of happening. The development team must immediately address these risks and create mitigation plans for them.
* Medium: Risks that have an average chance of happening and a fair impact on the system. To prepare for these risks, mitigation plans should be created, and these risks should be continuously monitored.
* Low: Risks that have a small impact on the system and a low likelihood of occurring. Periodically monitoring these risks will allow for the development of mitigation plans in case that they occur.
* Negligible: Risks that have little chance of happening and negligible effect on the project. These dangers can be disregarded.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RISK ASSESSMENT MATRIX | | | | | |
| PROBABILITY  IMPACT | RARE  (1) | UNLIKELY  (2) | POSSIBLE  (3) | LIKELY  (4) | ALMOST  CERTAIN (5) |
| INSIGNIFICANT  (1) | N | N | N | N | L |
| MINOR  (2) | N | N | L | L | M |
| SIGNIFICANT  (3) | N | L | L | M | H |
| DISASTROUS  (4) | N | L | M | H | E |
| CATASTROPHIC  (5) | L | M | H | E | E |

**Technical Risks:**

• High probability and high impact.

• Lack of technical expertise to develop the system.

• Failure of the new system to integrate with the current systems.

**Resource Risks:**

• Medium probability and medium impact.

• Inadequate resources for the project.

• Security Risks.

• Medium probability and medium impact.

• Unauthorized access to the system.

The development team will first concentrate on creating mitigation methods for the extreme and high priority hazards in accordance with prioritizing. The medium and low priority hazards will be regularly monitored, and if necessary, mitigation methods will be developed. The exceptionally low probability of occurrence and the exceedingly small impact on the project mean that the minimal priority risks will be disregarded.

## 6.9.6 Risk Monitoring

The E-Cliniq Risk Management Plan offers a framework for actively tracking risks throughout the project. To do this, it is crucial to closely document the process, including defining the circumstances that might set off risks, and to regularly monitor risks during the system lifecycle.

The high-scoring risks will be incorporated into the project schedule, and the risk manager will be given responsibility for their monitoring. This will make it easier for the project manager to decide when hazards need to be closely monitored and when the risk manager should provide project team meetings with updates. The risk manager will oversee monitoring the risk trigger circumstances. The project manager will also make sure that the project team is informed of the risks that have been identified and their potential effects on the project. Any new risks or modifications to existing risks should be reported to the risk management by the project team so that they can be evaluated and given the appropriate level of priority.

The agile risk management methodology, which emphasizes flexibility and constant improvement, will be used by the development team. To guarantee that the system’s goals and quality standards are met, the effectiveness of the risk management plan will be periodically evaluated and changed, as necessary.

## 6.9.7 Risk Mitigation and Avoidance

The project team will develop the risk management plan based on the value that each risk is given. The first stage in risk mitigation and avoidance is to identify and prioritize the potential risks. Strategies to prepare for likely delays could include preparing backup plans, allocating more resources, or changing project deadlines. The project team should determine which risks have the highest likelihood and potential impact and then establish plans to reduce or eliminate those risks. The project manager has the following main factors and choices to think about:

* **Resource Allocation:** The project manager must make sure the team has the necessary resources, including competence, abilities, and expertise, as well as access to tools and equipment, for the system to be effective and efficient. The project manager oversees the system, making sure that the team has access to these resources to complete the system on schedule and within the allocated budget.
* **Risk Assessment:** To effectively estimate and manage potential hazards, the development team should do a detailed analysis of them. Early in the project, the risk assessment should be finished, and the project manager should move quickly to identify and reduce any potential risks.
* **Contingency Planning:** The project team must develop backup plans for emergencies to be ready for potential dangers. The project manager is responsible for supervising the creation, validation, and testing of these strategies for each potential risk.
* **Agile Approach:** Risk management can be done in a flexible and quick manner by using the Agile methodology. The team's use of the Agile methodology, which permits continual risk management and the capacity for change, must be ensured by the project manager.
* **Communication:** The project manager must encourage open and transparent communication between the development team, and relevant stakeholders to reduce risks and avoid misunderstandings.

## 6.9.8 Risk Register

Each risk, its likelihood, potential repercussions, and any mitigation steps will be fully explained in the risk register, which will be maintained throughout the project. The risk register will be reviewed and updated frequently to make sure it accurately reflects the state of the project at the present time. The risk registry, which will be stored in a central location, which will be accessible to all relevant stakeholders.

This risk management strategy is often in line with the Agile methodology and places an emphasis on early and frequent risk discovery, collaborative risk management, and continuing risk monitoring. By foreseeing and resolving potential risks, the E-Cliniq system development team can decrease the effects and increase the likelihood that the project will succeed. The risk register will be based on the following standards:

* Risk ID - Each risk will receive a special identification number.
* Risk Description - The risk event will be clearly and concisely described.
* Risk Category - Risks will be categorized as technical, organizational, or legal.
* Risk Owner - Will oversee keeping an eye on and managing every risk.
* Probability - On a scale of 1 to 5, with one denoting the lowest chance and five denoting the highest, the likelihood of a risk occurring is evaluated.
* Impact - On a scale of 1 to 5, where 1 represents the least significant impact and five represents the most significant impact, the risk's potential impact on the project is evaluated.
* Risk Score - To calculating the overall risk score, the likelihood and impact scores are compounded.
* Mitigation Strategy - explains the precise steps must be done to reduce the risk.
* Status - The current state of the risk, including whether it is open, ongoing, or closed, is also recorded.
* Target Resolution Date - predicted day that the risk will be resolved.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| RISK ID | RISK RANK | RISK | DESCRIPTION | CATEGORY | DESTINATION/  OWNER | PROBABILITY | IMPACT | STATUS |
| RISK001 | 1 | Technical  Risk | The system may not work well with current hardware and software systems, which could lead to errors and delays in the system. | Technology | Project  Lead | High | High | In Progress |
| RISK002 | 2 | Resource  Risk | There is a chance that there will not be enough resources available to finish the project on schedule, which will cause delays and cost overruns. | Organizational | Project Manager | Medium | Medium | In Progress |
| RISK003 | 3 | Security  Risk | Data breaches and cyberattacks pose a threat that could compromise sensitive data. | Technical | System Developer | Medium | Medium | In Progress |
| RISK004 | 4 | Technical Risk | The users may not be able to understand how to use the system initially. | Technical | User | Medium | Medium | In Progress |