Risk Management

For

HealthTrack Fitness App

Submitted by

Team 1

IS663 - Professor Vassilka Kirova
NJIT
Longchao Da, Winona Patrick, Rohan Chopra, Khushali Sheth, Rutva Gandhi, Hao Mei, Vinoothna Chowdary Yarlagadda

Version: 2
Date Submitted: 3/22/2023

Introduction:

Risk management is the process of identifying, assessing, and controlling potential risks to minimize their negative impact on an organization's operations and objectives. It is an important aspect of project management, business continuity, and enterprise risk management. The main goal of risk management is to identify and mitigate potential risks before they become major issues.

Typical risk management activities include:

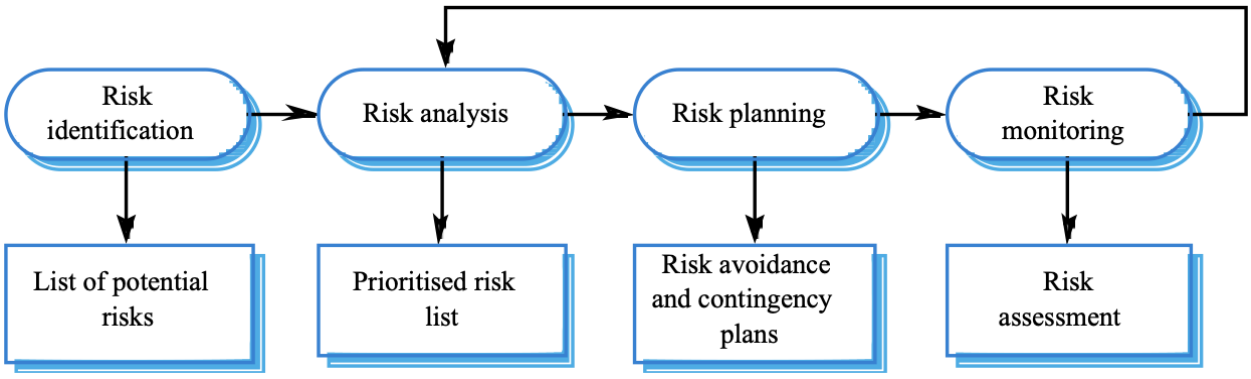
- Risk Identification: This is the process of identifying potential risks that could affect the project or business. This involves brainstorming, reviewing historical data, and involving stakeholders to identify potential risks.

- Risk Analysis: This process involves assessing the identified risks in terms of their likelihood of occurrence and potential impact on the project or business. This helps prioritize risks for mitigation and response planning.

- Risk Assessment: This process involves evaluating the identified risks against predetermined risk management criteria to determine the level of risk, and whether the risk is acceptable or not.

- Risk Mitigation: This involves developing strategies and plans to reduce the likelihood or impact of identified risks. Strategies may include developing contingency plans, implementing risk control measures, or transferring the risk to a third party.

- Risk Monitoring: This involves regularly monitoring the identified risks and their associated mitigation plans to determine their effectiveness and make necessary adjustments. This helps ensure that risk management strategies remain relevant and effective throughout the project or business lifecycle.



Two possible risks for our app HealthTrack, along with their probability, possible impact, and corresponding mitigation plans:

1. **Technical Risk:**
   The mobile application could experience technical issues, such as crashes, slow loading times, or malfunctions. This could impact the user experience and lead to negative reviews, decreased usage, and loss of customers.

   - **Probability:** Medium to high, as technical issues are common in mobile applications and can arise due to various factors such as bugs, compatibility issues, and hardware limitations.

   - **Possible Impact:** High, as technical issues can harm the reputation of the application, decrease user engagement, and lead to lost revenue.

   - **Mitigation Plan:** To mitigate this risk, the development team can conduct rigorous testing and quality assurance checks to identify and fix any technical issues before releasing the application. They can also implement monitoring and analytics tools to track the application's performance and quickly address any issues that arise.

2. **Privacy and Security Risk:**
   The mobile application could experience privacy or security breaches, such as unauthorized access to user data or a data breach. This could lead to loss of customer trust, negative publicity, legal consequences, and loss of revenue.

   - **Probability:** Medium to high, as mobile applications can be vulnerable to hacking, phishing, or other forms of cyber attacks. Additionally, privacy regulations such as GDPR and CCPA require organizations to protect user data, and failure to do so can result in hefty fines.

   - **Possible Impact:** High, as privacy and security breaches can harm the reputation of the application, lead to customer churn, and result in legal consequences and financial losses.

   - **Mitigation Plan:** To mitigate this risk, the development team can implement strong security measures, such as encryption, two-factor authentication, and regular security audits. They can also establish clear privacy policies and obtain user consent for data collection and usage. Additionally, they can prepare incident response plans to quickly address any privacy or security breaches that occur.

By maintaining a **risk register**, the organization can keep track of the identified risks, their likelihood and impact, and the corresponding mitigation plans. The risk register should be reviewed and updated regularly to ensure that the mitigation plans remain relevant and effective.