Visualizing the Software Vulnerabilities based on different significant scopes

Authors: Puya, Henil, Kanika

Stakeholders: Illinois Tech

Nov. 24th

Version 1.1

**Risk Management Plan**

**1. Introduction**

This Risk Management Plan outlines the approach for identifying, analysing, and managing risks associated with the Software Vulnerability Data Analysis project. It provides a structured methodology to minimize the impact of potential risks on project objectives.

**1.1 Purpose**

The purpose of this Risk Management Plan is to:

* Identify potential risks that could affect the project
* Assess the likelihood and impact of these risks
* Develop strategies to mitigate or respond to risks
* Establish a framework for ongoing risk monitoring and control

**1.2 Scope**

This Risk Management Plan covers all aspects of the Software Vulnerability Data Analysis project, including:

* Data collection from NVD, CVE, and OSV sources
* Database design and implementation
* Data processing and analysis
* Dashboard creation and visualization
* Project timeline from November 11 to November 29, 2024

**1.3 Definitions, Acronyms, and Abbreviations**

| **Term** | **Definition** |
| --- | --- |
| Risk | An uncertain event or condition that, if it occurs, has a positive or negative effect on project objectives |
| Probability | The likelihood of a risk occurring |
| Impact | The potential effect of a risk on project objectives |
| Mitigation | Actions taken to reduce the probability or impact of a risk |
| Contingency | A plan of action to be taken if a risk occurs |
| NVD | National Vulnerability Database |
| CVE | Common Vulnerabilities and Exposures |
| OSV | Open Source Vulnerabilities |
| API | Application Programming Interface |

**2. Risk Management Process**

**2.1 Risk Identification**

Risks will be identified through:

* Team brainstorming sessions
* Review of similar projects
* Expert consultation
* Ongoing project monitoring

**2.2 Risk Analysis**

Risks will be analyzed based on:

* Probability (1-5 scale, where 1 is very low and 5 is very high)
* Impact (1-5 scale, where 1 is very low and 5 is very high)
* Risk Score = Probability \* Impact

**2.3 Risk Response Planning**

For each identified risk, one of the following strategies will be chosen:

* Avoid: Eliminate the threat by eliminating the cause
* Mitigate: Reduce the probability or impact of the risk
* Transfer: Shift the impact of the risk to a third party
* Accept: Acknowledge the risk but take no action unless it occurs

**2.4 Risk Monitoring and Control**

Risks will be monitored through:

* Weekly team meetings
* Project status reports
* Continuous risk log updates

| **Risk ID** | **Description** | **Probability (1-5)** | **Impact (1-5)** | **Risk Score** | **Response Strategy** | **Mitigation/Contingency Plan** | **Owner** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R1 | API changes in data sources | 3 | 4 | 12 | Mitigate | - Monitor source documentation - Design flexible data ingestion scripts - Maintain backup data sources | Puya |
| R2 | Data quality issues | 4 | 4 | 16 | Mitigate | - Implement robust data cleaning procedures - Perform regular data quality checks - Develop data reconciliation process | Puya |
| R3 | Scope creep | 3 | 3 | 9 | Avoid | - Clearly define project boundaries - Implement change control process - Regular scope review meetings | Kanika |
| R5 | Performance issues with large datasets | 3 | 3 | 9 | Mitigate | - Optimize database queries - Implement data partitioning - Consider cloud-based solutions for scalability | Puya |

**3. Risk Register**

**4. Risk Management Roles and Responsibilities**

| **Role** | **Responsibilities** |
| --- | --- |
| Kanika Capoor | - Overall responsibility for risk management - Facilitate risk identification and analysis - Ensure risk responses are implemented |
| Kanika Capoor | - Identify and manage technical risks - Implement risk mitigation strategies |
| Kanika Capoor | - Identify risks related to data quality and analysis - Develop contingency plans for analytical challenges |
| All Team Members | - Participate in risk identification - Report new risks as they arise - Implement assigned risk responses |