Automated Code Review System

(Risk Assessment and Mitigation)

SOEN 6841 – Software Project Management

By

Prof. Joumana Dargham

Submitted By – Group 18

NAME	STUDENT ID NUMBER
Dhruv Panchal	40226430
Udisha Kaura	40266183
Khushal Nirmal Jain	40233877
Aman Kumar	40278443

TABLE OF CONTENTS

Risk Assessment and Mitigation

Objective

The purpose of this document is to conduct a thorough risk assessment and mitigation study for **Automated Code Review System (ACRS)**, identifying potential challenges, risk assessment and uncertainties associated with the project and to develop a risk mitigation plan accordingly.

Risk Identification

This will, therefore, be critical in looking at all likely challenges and impediments that are likely to bear negatively on the Automated Code Review System project. This would, therefore, call for the project team to brainstorm and consult widely, exploring from where most of the possible project risks could be coming from. And these sources are then further broken down to technical, operational, and external issues, covering such problems as software bugs or integration issues, project delays, or regulation changes and competition on the market. This is then further expanded. This is in an attempt to cover all the project perspectives: development process, technology stack, user experience, and project management practices. Aiming to have a complete list of risks. This ensures that the team is well-prepared to address any issues that might arise during the project lifecycle.

Ten risks have been identified and their IDs are listed below.

- R1: Incomplete Requirements
- R2: Estimated cost is less than the actual cost of requirements.
- R3: Technology Integration Challenges
- R4: Compromised Security System
- R5: Unpredicted scalability issues
- R6: More resources are needed.
- R7: Delay in third-party component deliveries
- R8: User accepted challenges
- R9: Changes in government regulations
- R10: Business Partners Acceptance

Risk Identification Table

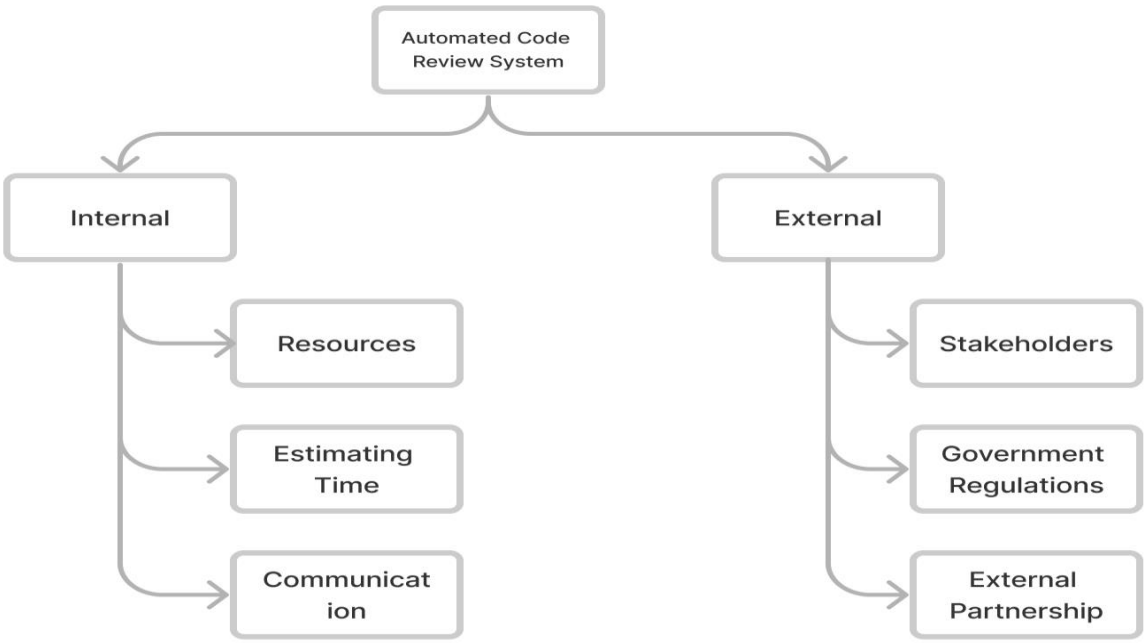
This is a valuable tool for tracking and managing risks within the life of a project, ensuring all the members of a team are appraised of challenges that may come up and take precautionary measures to tackle the same.

ID	Description	Category	Root Cause	Triggers	Mitigation Plan	Risk Owner	Impact	Probability
R1	**Missing requirements**	**Schedule delay**	**Stop the project**	**Early**	**Conduct thorough requirements analysis**	**Project Manager**	**HIGH**	**MEDIUM**
R2	Estimating wrong cost	**Cost Overrun**	**Stop the project**	**Mid**	**Re-estimate cost for the project**	**Installation team**	**HIGH**	**HIGH**
R3	Missing compatibility	**Schedule delay**	**Lack of compatibility between systems**	**Early**	**Find alternatives to the problem**	**Technical lead**	**HIGH**	**HIGH**
R4	**Errors in the implementation**	**Schedule delay**	**Have a response team**	**Continuous**	**Implement regular security assessments**	**Security Officer**	**HIGH**	**MEDIUM**
R5	**The product is not scalable**	**Quality**	**Have a scalable infrastructure**	**Early**	**Implement regular stress test to test the system**	**Infrastructure Lead**	**HIGH**	**HIGH**
R6	**If the project has new cost that will cause delays**	**Cost Overrun**	**Not having correct cost of subparts**	**Mid**	**Have experts review cost**	**Manager**	**LOW**	**MEDIUM**
R7	**Delays in components for the system**	**Schedule delay**	**Not estimating the right component delivery**	**Continuous**	**Have a contingency plan**	**Procurement manager**	**MEDIUM**	**MEDIUM**
R8	**User acceptance challenges**	**Quality**	**Not easy to use**	**Mid**	**Have a user feedback mechanism**	**User Experience Lead**	**HIGH**	**MEDIUM**

R9	**Change in regulation**	**Cost overruns**	**Government changes**	**Mid**	**Have teams on standby for changes**	**Compliance officer**	**LOW**	LOW
R10	**Stockholder satisfaction**	**Schedule delay**	**Level of acceptance**	**End**	**Implement changes**	**Sales and marketing director**	**MEDIUM**	**MEDIUM**

Risk Breakdown Structure

The Risk Breakdown Structure gives a picture of the identified risks in a hierarchal manner. The structure helps the project team classify every identified risk in a systematic manner, depending upon its nature and source of the risk. The most common are technical risks related to project technology and tools, organizational risks related to the management of the project and behavior of the team, operational risks related to the activities and procedures of the project, and external risks that involve the factors laying out of the control of the project team, like trends in the market or regulations.



Probability Impact Matrix

It is a prioritization of risks that are likely to happen with high probability and have potential magnitude to project. In this way, the team is able to focus its resources and efforts more efficiently on controlling those risks that can be most threatening to the success of the project. Risk Identification Table The risk identification table is an elaborative document that entails a list of all identified risks with detailed descriptions that include the source of the risk, the impact it might have on the project, and where in the project. This table is a central repository of risk information to give the project team a clear and accessible overview. Each entry on the risk table shows the likelihood of occurrence, impact level, and notes on associated mitigation strategies or contingency plans. The table is a live document and is usually updated at regular intervals whenever new risks are identified, or where there are changes in the existing risks.

Risk Response Planning

Risk Response Planning is inclusive of developing strategies that could apply in tackling the identified risks, hence ensuring preparedness by the project to deal with evolving issues. This is the stage at which an appropriate response is chosen for each risk, which may include avoidance, mitigation, transfer, or acceptance. Avoidance strategies aim at complete eradication of the risk, most times with changes in project plans or specifications. Mitigation means those actions which shall reduce the likelihood or consequence of risk. The transfer strategies shift the risk to another party: usually, this refers to outsourcing or insurance. Acceptance is a decision to continue with the project while knowing the risks, usually with plans to handle likely outcomes. The project team makes up a clear plan of answers, which can be presented as specific activities for each of the risks, responsible people, and timing of the required work. In a proactive manner, this assures that the team is well-preformed and most likely able to respond to the risks in a quick and effective way, with the result that the risks are minimized for the successful endif. By fully elaborating these elements within the risk management plan of the Automated Code Review System project, your efforts will significantly empower the project to face adversity and successfully deliver.

Risks	Response Strategies
R1, R2, R6	**Risk acceptance**
R8	**Risk avoidance**
R9	**Risk transference**
R3, R4, R5, R7, R10	**Risk mitigation**

Risk Mitigation Strategies

- Regular Backups and Version Control: We meticulously back up our work in multiple locations to safeguard against potential losses. If any code or data is lost, these backups serve as a recovery source. Additionally, we employ version control systems like Git to monitor changes, allowing us to revert to previous versions if new updates prove problematic.
- Training and Documentation: We offer comprehensive training and clear guidelines on the optimal use of the Automated Code Review System to prevent misuse-related errors. This approach also enables new team members to quickly become proficient.
- Testing Regularly: We frequently test the system for bugs or issues, including scrutinizing new features before their implementation and ensuring overall system compatibility. Early identification of problems facilitates timely fixes, averting more significant issues down the line.
- Keep Software Updated: Our commitment to using updated software versions guards against security risks and ensures system efficiency. Staying current also means benefiting from new features and improvements that enhance system performance.
- Risk Reviews: Bi-weekly meetings allow us to discuss new risks and evaluate the effectiveness of our current strategies, making adjustments as necessary. This practice keeps everyone informed about potential issues and our response strategies.
- Diversify Technologies: We avoid dependence on a single technology, software, or tool. This diversification strategy means that a fault in one technology won't halt our entire project, and employing various technologies often provides safer and more flexible problem-solving options.
- Communication Plan: We have established clear protocols for risk-related information sharing, ensuring that any observed issues are promptly reported to the appropriate parties. Effective communication is key to addressing problems before they escalate.

By adhering to these strategies, we strive to maintain the Automated Code Review System project's safety and reliability, preventing significant difficulties and preparing to efficiently resolve minor issues.