Ryerson University

Department of Electrical, Computer, & Biomedical Engineering
Faculty of Engineering & Architectural Science

Course Number	COE691
Course Title	Software Requirements Analysis and SPEC
Semester/Year	Winter Semester 2024
Instructor	Dr. Rasha Kashef
TA Name	Aman Yadav

Lab/Tutorial Report No.	Lab 5

Report Title	Lab 5: Requirement and Risk Management

Section No.	06
Submission Date	Week of April 8, 2024
Due Date	April 12, 2024

Student Name	Student ID	Signature*
Hamza Malik	501112545	HM

**By signing above you attest that you have contributed to this submission and confirm that all work you have contributed to this submission is your own work. Any suspicion of copying or plagiarism in this work will result in an investigation of Academic Misconduct and may result in a "0" on the work, an "F" in the course, or possibly more severe penalties, as well as a Disciplinary Notice on your academic record under the Student Code of Academic Conduct, which can be found online at: http://www.ryerson.ca/content/dam/senate/policies/pol60.pdf*

Hamza Malik

Project Document

Risk Register

IT in transportation
Autonomous Emergency
Response System (AERS)
2024/04/05

Executive Summary:

The AERS project is a cutting-edge initiative aimed at enhancing emergency response capabilities through automation. Despite the promising benefits such as quicker response times, fewer human errors, and enhanced efficiency, the project faces a series of risks. These risks, if not managed appropriately, could severely impact the project's viability and effectiveness.

Most Serious Risks Identified:

A thorough risk management process, which included Monte Carlo simulations, has highlighted several critical risks to the project's success:

1. **Regulatory Compliance**: The risk of non-adherence to evolving aviation and ground regulations with a Risk Factor (RF) of 1.42. Non-compliance could lead to severe legal repercussions and erosion of stakeholder trust.

2. **Cybersecurity Threats**: The threat of cyber intrusions poses a risk with an RF of 1.40. A breach could critically undermine system integrity and public confidence.

3. **Sensor Malfunction**: The risk that sensor failures could compromise the system's operational integrity with an RF of 1.25. This could result in failure to respond to emergencies effectively.

4. **Change Management Issues**: Difficulty in managing change within the organization due to the adoption of the AERS, with an RF of 1.31. Resistance could significantly delay project milestones.

Areas of Most Concern:

The principal concerns revolve around ensuring regulatory compliance, robust cybersecurity measures, reliability of technical components, and smooth organizational change management. Addressing these risks is crucial to maintain financial integrity, market position, and reputation.

1. **Regulatory Compliance**: Risks include legal sanctions and the necessity to adapt system components to meet new standards.

2. **Cybersecurity Threats**: Involves potential system downtimes to address vulnerabilities and restore data integrity after breaches.

3. **Sensor Malfunction**: May necessitate additional investments in technology to enhance reliability and prevent malfunctions

4. **Change Management Issues**: Encompasses the risk of disrupting operational workflows and additional costs due to resistance from the workforce.

Current State vs. Ideal State:

Currently, the AERS project is in an embryonic phase, facing significant risks that could impede progress. The ideal state is one where the identified risks are mitigated to ensure seamless integration of the AERS into existing emergency response frameworks, with all stakeholders aligned and engaged.

Risk Number:	1	Risk Rating:	High	Risk Owner:	Compliance Officer
Description:	Regulatory Compliance: The risk of non-adherence to evolving aviation and ground regulations.				
Project Objective(s) Impacted:	Cost, Time, Scope, Quality				
Risk Probability:	56.9%	Risk Impact:	2.75 (Critical)		
Potential Triggers or Precursors:	• New aviation or ground regulations, gaps in regulatory updates.				
Potential Mitigation:	• Ongoing legal training, incorporation of regulatory updates into development cycles.				
Potential Responses:	• Engage with regulatory bodies, revise protocols, update compliance strategies.				
Root Causes (If Identified):	• Lack of up-to-date legal knowledge, inadequate change management in legal practices.				

Risk Number:	2	Risk Rating:	High	Risk Owner:	Chief Security Officer
Description:	Cybersecurity Threats: The threat of cyber intrusions that may critically undermine system integrity and public confidence.				
Project Objective(s) Impacted:	Cost, Time, Scope, Quality				
Risk Probability:	55.7%	Risk Impact:	2.70 (Critical)		
Potential Triggers or Precursors:	• Phishing attacks, unpatched system vulnerabilities.				
Potential Mitigation:	• Implementation of advanced cybersecurity measures, regular penetration testing.				
Potential Responses:	• Immediate incident response, public communication, and system fortification.				
Root Causes (If Identified):	• Insufficient cybersecurity measures, delayed response to threat intelligence.				

Risk Number:	3	Risk Rating:	High	Risk Owner:	Head of Technology
Description:	Sensor Malfunction: The risk that sensor failures could result in an ineffective emergency response.				
Project Objective(s) Impacted:	Time, Quality				
Risk Probability:	52.5%	Risk Impact:	2.55 (Marginal to Critical)		
Potential Triggers or Precursors:	• Hardware failures, software glitches in sensor operation.				
Potential Mitigation:	• Regular system diagnostics, redundancy in sensor arrays.				
Potential Responses:	• Swift replacement of faulty sensors, software updates, and hardware checks.				
Root Causes (If Identified):	• Inadequate sensor quality assurance, lack of robust hardware testing protocols.				

Risk Number:	**4**	**Risk Rating:**	**High**	**Risk Owner:**	**Change Management Lead**
Description:	**Change Management Issues: The difficulty of managing organizational change with the AERS adoption**				
Project Objective(s) Impacted:	**Time, Scope, Quality**				
Risk Probability:	**51.8%**		**Risk Impact:**	**2.52 (Marginal to Critical)**	
Potential Triggers or Precursors:	• **Organizational resistance, inadequate training programs.**				
Potential Mitigation:	• **Comprehensive change management strategies, gradual system roll-out.**				
Potential Responses:	• **Enhancing engagement initiatives, improving training materials.**				
Root Causes (If Identified):	• **Cultural resistance to change, poor communication of benefits and procedures..**				

Cause-and-Effect Diagram