Ryerson University

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

Course Title:	Software REQs Analysis SPEC
Course Number:	COE691
Semester/Year (e.g.F2016)	W2024

Instructor:	Rasha Kashef

Assignment/Lab Number:	5
Assignment/Lab Title:	Requirement and Risk Management

Submission Date:	2024/04/08
Due Date:	2024/04/08

Student LAST Name	Student FIRST Name	Student Number	Section	Signature*
Sarim	Shahwar	501109286	02	SS

*By signing above you attest that you have contributed to this written lab report and confirm that all work you have contributed to this lab report 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/senate/current/pol60.

Sarim Shahwar

Project Document

Risk Register

IT in Business
(E-commerce)
2024/04/03

Executive Summary:

The current IT project is focused on boosting E-commerce operations and offers various chances to improve consumer, supplier, and employee relations via a new system that incorporates both functional and non-functional requirements. While the project is ambitious, with goals of streamlining processes, improving data quality, and providing a more intuitive user experience, it confronts a number of technological, financial, and legal challenges.

Most Serious Risks Identified

Through a rigorous risk management and analysis process, including Monte Carlo simulations, the following risks have been identified as the most crucial to the project's success.

1. Regulatory Compliance: The danger of failing to follow existing or developing rules governing online transactions and data security, with a danger Factor (RF) of 1.36. Noncompliance could end up in legal costs, financial losses, and reputational harm.

2. Data Security Breach: The risk of illegal access to critical customer and supplier data, with an RF of 1.34. Breaches could destroy confidence in the platform, resulting in consumer loss and legal consequences.

3. User Adoption: The danger that the new system's user interface may not match consumer expectations, resulting in poor adoption rates, with an RF of 1.34. Poor user adoption might have a severe influence on the project's ROI and long-term sustainability.

4. Change Management Issues: The issue of managing organizational changes connected with the new system's implementation, with an RF of 1.31. Resistance to change could jeopardize the integration of systems and operational efficiency.

Areas of Most Concern

The main areas of concern include maintaining regulatory compliance, guaranteeing solid data security, encouraging high user adoption through intuitive design, and efficiently managing change within the firm. Failing to handle these risks may result in financial losses, lower market competitiveness, and a ruined brand name.

1. **Probable Events and Risk Audit Regulatory Compliance**: Risks include penalties and regulatory action, as well as redesigning system components to satisfy compliance standards.
2. **Data security breaches**: Data security breaches result in a loss of consumer confidence, financial obligations, and probable downtime to rectify security weaknesses.

3. **User Adoption**: Platform utilization is lower than projected, forcing further marketing, training, and system change.
4. **Change management issues**: Change management issues include operational interruptions, postponed project timeframes, and increased expenses as a result of internal opposing views.

Current State vs. Ideal State:
Although the project is new and has the potential to improve E-commerce operations, it currently faces risks that might undermine its success. The ideal situation would be one in which these risks are adequately managed, resulting in regulatory compliance, data security, high user adoption, and simple change management procedures.

Risk Number:	**1**	**Risk Rating:**	**High**	**Risk Owner:**	**Compliance Officer**
Description:	**Risk of non-compliance with data protection and online transaction regulations which could result in legal sanctions, fines, and reputational damage.**				
Project Objective(s) Impacted:	**Cost, Time, Scope, Quality**				
Risk Probability:	0.53	Risk Impact:	**2.57 (Critical)**		
Potential Triggers or Precursors:	• **New regulatory requirements, failure in regular compliance review.**				
Potential Mitigation	• **Regular legal updates, compliance checks integrated into the CI/CD pipeline.**				
Potential Responses:	• **Consult legal experts, update the system to comply, communicate changes to stakeholders.**				
Root Causes (if identified):	• **Lack of compliance expertise, inadequate risk assessment, insufficient regulatory tracking.**				

Risk Number:	**2**	**Risk Rating:**	**High**	**Risk Owner:**	**Chief Security Officer**
Description:	**Unauthorized access to sensitive customer and supplier data leading to breaches.**				
Project Objective(s) Impacted:	**Cost, Time, Scope, Quality**				
Risk Probability:	0.51	Risk Impact:	**2.61 (Critical)**		
Potential Triggers or Precursors:	• **Phishing attacks, weak passwords, unpatched vulnerabilities.**				
Potential Mitigation	• **Strong encryption, regular security training, up-to-date security patches.**				
Potential Responses:	• **Activate incident response plan, notify affected parties, strengthen security measures.**				
Root Causes (if identified):	• **Lack of security protocols, outdated software, human error.**				

Risk Number:	**3**	**Risk Rating:**	**High**	**Risk Owner:**	**Head of User Experience**
Description:	**System not meeting user expectations, leading to lower adoption rates.**				
Project Objective(s) Impacted:	**Cost, Scope, Quality**				
Risk Probability:	0.53	Risk Impact:	**2.53 (Marginal to Critical)**		
Potential Triggers or Precursors:	• **Negative user feedback, high learning curve for new system.**				
Potential Mitigation	• **Iterative design with user testing, feedback loops, user training programs.**				
Potential Responses:	• **Redesign features based on feedback, targeted user support, marketing campaigns.**				
Root Causes (if identified):	• **Misalignment of product features with user needs, poor usability design**				

Risk Number:	**4**	**Risk Rating:**	**High**	**Risk Owner:**	**Change Management Lead**
Description:	**Resistance to new processes and systems among employees.**				
Project Objective(s) Impacted:	**Time, Scope, Quality**				
Risk Probability:	0.52	Risk Impact:	**2.52 (Marginal to Critical)**		
Potential Triggers or Precursors:	• **Lack of communication, sudden changes, inadequate training.**				
Potential Mitigation	• **In-depth change management plans, gradual implementation, transparency**				
Potential Responses:	• **Address employee concerns, enhance training, adjust pace of change.**				
Root Causes (if identified):	• **Cultural inertia, lack of engagement with stakeholders, lack of perceived benefits.**				

Cause-and-Effect Diagram

Sarim Shahwar
501109286

Risk Cause and Effect Diagram