Concordia University

Engineering and Computer Science

SOEN 6481 Systems Requirements Specification

Delivery #2

Requirements Analysis and Risk Evaluation

Submitted To: **Prof. Dr. Rodrigo Morales**

Requirements Analysis and Risk Evaluation

Task 0 - Logging

S.No .	Task	Time Spent (Hours)
0	Task 0 - Logging	5 mins
1	Task 1 – Identifying and finding inconsistencies in the vision document	3
2	Task 2 – Documenting conflicts	2
3	Task 3 – Conflict resolution	1
4	Task 4 – Conflict evaluation	2
5	Task 5 – Risk management	4

Task 1 – Identifying and finding inconsistencies in the vision document

Defect #	Location	Defect type	Classification	Description	Status	Date Corrected
1	3.1. Stakeholder Summary	Omission	Major	Missing key Stakeholders to illustrate the requirements. No information regarding Competitors who are one of the primary stake holders		
2	3.2. User Summary	Omission	Major	Consumers age requirement is nowhere mentioned in the vision document.		
3	3.3. User Environment	Inadequacy	Minor	Not sufficiently describing the future enhancements of the product.		
4	3.4. Key Stakeholder or User Needs	Omission	Major	Tool reservation constraints were not explained in the User needs section.		
5	3.4. Key Stakeholder or User Needs	Omission	Major	Information regarding rental period is not mentioned as a part of user needs.		

6	4.1. Product Perspective	Inadequacy	Minor	Architecture Diagram can be more detailed. Only Abstract information are given. System's stack is not explained in the architecture diagram Only System's data flow is covered.		
7	4.2. Assumptions and Dependencies	Ambiguity	Major	Exceptional cases like rental tool lost, rental tool damage policies are not emphasized in the Assumptions and Dependencies section.		
8	5. Product Features	Inadequacy	Major	Products primary features like password recovery, Web Push Notification and Live chat were not included as a part of product features		
9	6. Other Product Requirements	Contradiction	Minor	Market is flooded with lot of browsers, there is no information about the best supported browsers to access the application.		

Task 1.1 - Inconsistencies Inspection Form

S.no	Location	Inconsistency type	Classification	Description	Status	Date corrected
1	***3.4. Key Stakeholder or User Needs*** S1 : Customers must be at least 18 years old. S2 : Customers must have a government-issued photo ID that is valid at the time of rental.	Designation	Weak	Customers who are 18 years old, might not have a valid government ID, as they would have just turned out 18, they might have applied for a government ID, there should be an option to accept college ID to verify the age.		
2	***3.2. User Summary*** S3 : Store branches are being added, modified, and deleted by system administrator. S4 : Customers can request a reservation for as early as the next day	Structure	Strong	Customers might rent tools or reserve tools in advance, but due to organization policies if Administrator tries to delete a branch, System shouldn’t permit the administrator to do		

	and up to 30 days in advance.			so as they were some existing rental reservations existing in advance for the respective store/Location.		
3	***3.4. Key Stakeholder or User Needs*** S5 : The branch employees are responsible for adding/removing tools for rental in their respective locations. S6 : The branch employees are also responsible to hand out the tools to the customers in store, and to receive them.	Designation	Major	Once the customer returns the equipment, the branch manager should place the tools in the store and failing to update in the system will never update the availability of tools and there will be an inconsistency between the tools available in the store and the available rental tools in the ETR system.		

Task 2 – Documenting Conflicts

A standard documentation technique consists of building an interaction matrix (Kotonya & Sommerville, 1997).

Statements	S1	S2	S3	S4	S5	S6	S7	S8	Total
S1	0	1	0	0	0	0	0	0	1
S2	1	0	0	1000	0	0	1000	0	2001
S3	0	0	0	1	0	0	0	0	1
S4	0	1000	1	0	0	0	1000	0	2001
S5	0	0	0	0	0	1	0	0	1
S6	0	0	0	0	1	0	0	0	1
S7	0	1000	0	1000	0	0	0	0	2000
S8	0	0	0	0	0	0	0	0	0
Total	1	2001	1	2001	1	1	2000	0	**6006**

Total number of non-conflicting overlaps and conflicts : 6006 / 1000 = 6.006

Conflicts = 0.006

So, according to interaction matrix,

Total number of conflicting statements = 6

Total number of overlapping statements = 6

Task 3 – Conflict Resolution

3.1. Conflict between S1 and S2 :

Operator Applied: Specializing Conflict source or target

This conflict can be resolved by specializing the conflict source or target by enabling the auto verification of the customers age by integrating the system with Federal system, whereas the customer can enter their last 4 digits of SIN id and the system can identify the customer's age by request authorization approved from the Government.

Operator Applied: Weaking Conflicting Statements

The conflicting statements can be weakened by, accepting any non-governmental ID's too which has the date of birth details in it.

3.2. Conflict between S3 and S4 :

Operator Applied: Avoid Boundary Condition

The specific boundary condition for this conflict is Admin's privilege to delete a branch and User's privilege to rent or return the tools, these two statements are contradicting and puts the system in a deadlock situation if the admins deletes a store which has some reservations and ongoing rental records, it will end up in data loss and financial loss, this can be eradicated by introducing a new requirement that, Admin will never be allowed to delete a store, until the store has no reservation or rental records.

Operator Applied: Restore Conflicting Statements

The statements S3 and S4 can be retained by, having a law imposed by board of directors of ETR organization, to not to delete a store until the organization decides to close the business in a particular location due to some non-functional and business-oriented issues.

3.3. Conflict between S5 and S6 :

Operator Applied: Avoid Boundary Condition

If the branch employee doesn't update the system after receiving the equipment from the rental customer the boundary condition would occur where the customer won't have the details of the updated inventory in the system, this can be avoided by having an automated system to perform an inventory count in the respective store before closing the business for the day and updating them in the system.

Operator Applied: Weaking Conflicting Statements

The Statement S6 can be made weaken by having a dedicated branch employee team who can focus only on receiving the tools and updating them in the system, this way the inventory details will be consistent with the available inventory.

Task 4 – Conflict Evaluation

Using Weighted matrices for evaluating alternative options for the above documented conflicts.

$$totalScore(opt) = \sum(Scores(opt, crit) \times Weight(crit))\ crit$$

4.1. Evaluation for S1 and S2 :

Option 1: Integrating ETR with government system to obtain User's age.

Option 2: Accepting Non-governmental Id's which has age details.

Evaluation Criteria	*Significance Weighting*	*Option 1*	*Option 2*
Time efficient	0.4	0.3	0.9
Minimal Inconvenience	0.2	0.4	0.7
Reliable Response	0.4	0.4	0.8
Total	1.0	0.36	0.82

From the above computation, **Option 2** can be used to resolve the conflict.

4.2. Evaluation for S3 and S4 :

Option 1: A new requirement that, Admin will never be allowed to delete a store, until the store has no reservation or rental records.

Option 2: A law imposed by board of directors of ETR organization, to not to delete a store.

Evaluation Criteria	*Significance Weighting*	*Option 1*	*Option 2*
Time efficient	0.3	0.2	0.8
Accessing the System	0.2	0.8	0.3
Reliable Response	0.5	0.9	0.2
Total	0.1	0.67	0.4

From the above computation, **Option 1** can be used in place of S4 to resolve the conflict.

4.3. Evaluation for S5 and S6 :

Option 1: An automated system to perform an inventory count.

Option 2: A dedicated branch employee team who can focus only on receiving the tools and updating them in the system.

Evaluation Criteria	*Significance Weighting*	*Option 1*	*Option 2*
Interactive	0.4	0.7	0.7
Quality	0.2	0.6	0.8
Time efficient	0.4	0.6	0.9
Total	1.0	0.66	0.77

From the above computation, **Option 2** can be used in place of S6 to resolve the conflict.

Task 5 – Risk management

A risk is an uncertain factor whose occurrence may result in a loss of satisfaction of a corresponding objective. It has a likelihood of occurrence and one or several undesirable consequences associated with it. Each consequence has a severity in terms of degree of loss of satisfaction of the corresponding objective Risks can be identified by several methods like risk checklists, risk trees and component inspection. And the identified risks are below as follows:

a) By component Inspection

1. Server/Database failure

2. Communication Network component failure

3. Hardware and Software component failure

a) By Risk Checklists: Considering the Non-Functional Requirements

4. Data Breach / Data leakage (Safety and Security)

5. Accidentally downloading malware (Installation)

6. Project not delivered at scheduled time (Time)

7. Developing the wrong software functions (User Interaction)

8. Lack of Budget (Cost)

a) Risk Tree

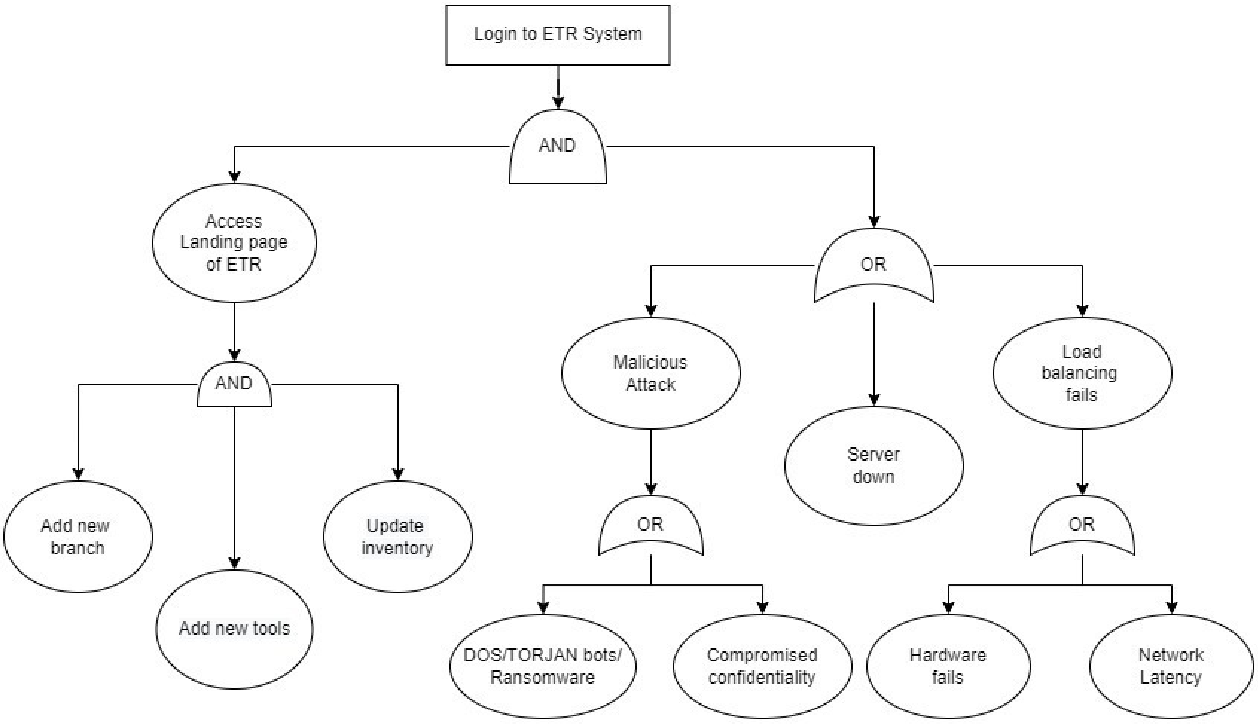

Figure 1: The risk tree shows the major point of failure where the stakeholders are unable to access the system

b) Risk Assessment: QUANTITATIVE

Risk Number	Likelihood	Probability	Impact (Thousands in Capital)	Exposure (Probability X Impact)
1	High	0.5	0.5	0.025
2	High	0.06	0.2	0.012
3	Moderate	0.01	0.3	0.003
4	Low	0.01	0.2	0.002
5	Low	0.01	0.2	0.002
6	Moderate	0.05	0.5	0.025
7	Moderate	0.05	0.5	0..025
8	High	0.04	0.8	0.032

b) Risk Assessment: QUANTITATIVE

1. Server Failure

Consequences	Likely	Possible	Unlikely
Error 404: This website is not available	Moderate	Severe – Scale 7	Moderate
Data loss	High	Severe – Scale 8	Low

2. Communication Network Failure

Consequences	Likely	Possible	Unlikely
users unable to login	Moderate	Severe – Scale 7	Moderate
Slow response	High	Severe – Scale 8	Low

3. Hardware and Software component failure

Consequences	Likely	Possible	Unlikely
Location of Store, GPS locating Functionality is misbehaving	Moderate	Severe – Scale 5	Moderate

4. Data breach or Data Leakage

Consequences	Likely	Possible	Unlikely
Hackers misusing the system’s data (user details compromise)	Low	Severe – Scale 9	High

5. Accidentally downloading malware

Consequences	Likely	Possible	Unlikely
Data corruption	Low	Severe – Scale 8	High

6. Project Not Delivered at scheduled time

Consequences	Likely	Possible	Unlikely
Losing Market value	Moderate	Severe – Scale 9	Moderate

7. Developing the wrong software functions

Consequences	Likely	Possible	Unlikely
User dissatisfaction	Low	Severe – Scale 5	High

8. Lack of Budget

Consequences	Likely	Possible	Unlikely
Incomplete Product	Low	Severe – Scale 9	High

c) Risk Control

1.
Option 1 – Frequent Backup
Option 2 – Replication of server for Server failure:
Both methods will help in preventing loss and corruption of data when risk happens.
.

Risk Reduction Leverage (RRL): Consider a server which maintains a repository of data. The probability of losing the data is 15%. The cost of losing the data is measured in terms of the cost of its reproduction and re-entry into the database which is estimated at $30,000. To reduce the risk of losing the data, there are two options. The first option is estimated to reduce the risk to 10%. It is estimated to cost to $2000. The second option is estimated to reduce the risk to 5%. It is estimated to cost $2500.

So here, we need to calculate the RRL for both options and choose the option that has value above 1.

Risk Reduction Leverage = (Risk Exposure Before) – (Risk Exposure After) / Cost of Risk Reduction
Risk Exposure Before = 30000 X 15 / 100 = 4500

Option 1 – Risk Exposure After = 30000 X 10 / 100 = 3000
Option 2 – Risk Exposure After = 30000 X 5 / 100 = 1500

RRL Option 1 = 4500 – 3000 / 2000 = 0.75
RRL Option 2 = 4500 – 1500 / 2500 = 1.2 **So, option 2 is better.**

2.
Option 1 – Fiber Optic Cable
Option 2 – Wireless Optical Networks for Communication Network failure:
Both methods will help in preventing loss and corruption of data when risk happens.

Risk Reduction Leverage (RRL): Consider a network company providing network services. The probability of losing the connection is 15%. The cost of losing the network is measured in terms of the cost of its coverage and re-establishment into the database which is estimated at $30,000. To reduce the risk of losing the data, there are two options. The first option is estimated to reduce the risk to 5%. It is estimated to cost to $2500. The second option is estimated to reduce the risk to 10%. It is estimated to cost $2000.

So here, we need to calculate the RRL for both options and choose the option that has value above 1.

Risk Reduction Leverage = (Risk Exposure Before) – (Risk Exposure After) / Cost of Risk Reduction

Risk Exposure Before = 30000 X 15 / 100 = 4500 Option 1 – Risk Exposure After = 30000 X 5 / 100 = 1500
Option 2 –Risk Exposure After = 30000 X 10 / 100 = 3000

RRL Option 1 = 4500 – 1500 / 2500 = 1.2
RRL Option 2 = 4500 – 3000 / 2000 = 0.75 **So, option 1 is better.**

3. *Reduce Risk Likelihood for Hardware and Software Component failure:* The risk can be prevented by replacing the GPS device or restoring the compass positioning of the system.

4. *Reduce Risk Likelihood for Data breach/ Data Leakage:* By opting methods like securing database, encryption, authentication, authorization we can create and maintain a safe web portal.

5. *Avoid the Risk for accidentally downloading malware:* This can be obtained by having an anti-virus installed in the system, avoiding advertisements, avoiding e-mail attachments.

6. *Mock-ups and Prototypes for Project Not delivered at scheduled time and for Developing the wrong software functions:* To avoid both risks we can practice the mentioned elicitation technique as it will be highly helpful to analyse and act accordingly. Scheduling a delivery and achieving it will give confidence to the team and if no will give them an idea on where to work, where they are lacking. Similarly, having evolutionary prototypes will help in achieving the features and can work on iterations to complete the product.

7. *Mitigate risk for Lack of Budget:* This risk can be handled by adding a separate team for handling the financial flow ensuring the team doesn’t run out of money.