Requirements Evaluation and Risk Analysis

[Electronic Tool Rental]

Task 1: Identifying and finding inconsistencies in vision document

- **1.1 Defect Table**
- **Time spent during inspection:** 6 hours

Defect #	Location	Defect Type	Classification	Description	Status	Date Corrected
1	Introduction	Minor	Poor Structuring	Introduction section is not properly broken up into subsections, such as objective, purpose, etc.		
2	Scope	Major	Inadequacy	The project's scope is unclear; is it dealing with all ages of clients or is there any restriction?		
3	Positioning - Problem Statement	Major	Omission	Only one component 'Need' is acknowledged, but 'Feature' is not stated.		
4	Positioning - Product Position Statement	Minor	Ambiguity	The ETR application does not specify whether it is a web-based app,		

				mobile app or both.		
5	Stakeholder Summary	Major	Omission	This section lacks important stakeholders (such as **Competitors**) who will influence the system's decisions		
6	Stakeholder Summary	Minor	Noise	Some stakeholders are not considered end users (such as **Tools/Equipment Insurance Company**) since they are not impacted or benefited by the ETR website.		
7	User Environment	Minor	Ambiguity	The term 'secure and stable internet' should be defined more specifically. For instance, to view the website, a minimum necessary speed is expected.		
8	Product Perspective	Minor	Opacity	This application should be scalable by design, but the document fails to explain how it will be achieved and provides an opaque idea of how it will be accomplished.		

9	Assumptions and Dependencies	Major	Noise	"In order to rent things from the website, users will have to provide their login credentials" - This statement was mislabeled as an assumption, which is erroneous because it is a need.		
10	Product Features	Major	Poor Structuring	Products are not bifurcated based on user satisfaction, most purchased things, discounted items, etc.		
11	Product Features	Minor	Inadequacy	'Alteration or recovery or forgot Password ' to regain access to the website is not clearly explained.		
12	Product Features	Major	Omission	The document does not specify any action to be taken if users do not come to the store to pick up the reserved tool during rental reservation period. In this case, the system must release the items		

				so that the other users can get them.		
13	Product Features	Major	Omission	The updating option of users' credit cards is not stated.		
14	Product Features	Major	Omission	It is not clarified how a refund is going to be received (whether it will be credited to a credit card or paid by cash)		
15	Other Product Requirements	Major	Overspecification	The database version has an impact on this application. If the database requires updating, the PHP version must be updated as well.		
16	Other Product Requirements	Major	Ambiguity	'Strong password' should be defined explicitly as different people will interpret it differently; whether it should contain alphanumeric, special symbols, upper case, lower case etc.		

1.2 Inconsistency Table

- **Time spent during inspection:** 6 hours

#	Location	Inconsistency Type	Classification	Description	Status	Date Corrected
1	User Summery	Designation	Weak	Admins authenticate using the system by entering their username and password from the website in order to access the dashboard.		
2	User Summary	Designation	Weak	Branch employees/ customers log in to the system using their login information to access the dashboard.		
3	Stakeholder Descriptions	Structure	Weak	Online rental orders and electronic tools on the website can be added, modified, or deleted by		

				branch employees		
4	Stakeholder Summary	Structure	Weak	Store branches are being added, modified, and deleted by system administrator		
5	User Summery	Structure	Weak	Adding, modifying, and deleting branch employees is done by the system administrator		
6	Product Features	Structure	Weak	Reservation/renting for any tool cannot be possible without users' registration.		
7	Assumptions and Dependencies	Structure	Weak	ETR website cannot be accessed without internet		
8	User Environment	Structure	Weak	ETR website cannot be accessed without laptop/desktop/mobile		
9	Product Features -	Structure	Weak	The system must confirm		

	Client Registration			that the customers are at least 18 years old when registering for the first time by entering a date of birth or submitting supporting documentation		
10	Product Features - Customer Dashboard	Structure	Weak	The user can enter into their account and add, change, or even delete a prior uploaded identity document.		

1.3 Other Comments:

- No glossary is available to help explain terms.

Task2: Documenting conflicts

- **2.1 Interaction matrix**

S1: Admins authenticate using the system by entering their username and password from the website in order to access the dashboard.

S2: Branch employees/ customers log in to the system using their login information to access the dashboard.

S3: Online rental orders and electronic tools on the website can be added, modified, or deleted by branch employees

S4: Store branches are being added, modified, and deleted by system administrator

S5: Adding, modifying, and deleting branch employees is done by the system administrator

S6: Reservation/renting for any tool cannot be possible without users' registration.

S7: ETR website cannot be accessed without internet

S8: Customers require access to a laptop/desktop/mobile to rent/reserve tools from the website.

S9: The system must confirm that the customers are at least 18 years old when registering for the first time by entering a date of birth or submitting supporting documentation.

S10: The user can enter into their account and add, change, or even delete a prior uploaded identity document.

Statements	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**	**S10**	**Total**
S1	0	1000	0	0	0	0	0	0	0	0	1000
S2	1000	0	0	0	0	0	0	0	0	0	1000
S3	0	0	0	0	1	0	0	0	0	0	1
S4	0	0	0	0	1000	0	0	0	0	0	1000
S5	0	0	1	1000	0	0	0	0	0	0	1001
S6	0	0	0	0	0	0	0	1	0	0	1
S7	0	0	0	0	0	0	0	1000	0	0	1000
S8	0	0	0	0	0	1	1000	0	0	0	1001
S9	0	0	0	0	0	0	0	0	0	1	1
S10	0	0	0	0	0	0	0	0	1	0	1
Total	1000	1000	1	1000	1001	1	1000	1001	1	1	**6006**

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

= 6.006

Conflicts = 0.006

Non-conflicting overlaps = 6

So, here in interaction matrix, there are 6 **Conflicting statements** in total.

Task 3: Conflict resolution

- **3.1. Conflict between S3 and S5:**

Avoid Boundary Condition:

The purpose of this method is to ensure that the boundary condition for a conflict can never become true

The boundary condition for strong conflict was seen to be ‘Admin can delete branch employees" and "Branch employee can add/modify/delete rental orders and tools on the website’. So it may happen that at the same time, admin deletes the employee, and at that very moment the same employee tries to alter the orders/tools on the system, which can result in conflicts. So, avoiding this boundary condition might be achieved by introducing a new requirement that an admin cannot delete an employee if they are logged and providing employees the ETR employee login portal to login first in order to handle any sort of activities on the system to minimize this friction.

- **Specialize conflict source or target:**

This method will identify the source objects involved in the conflicting statements S3 and S5 and specialize them so the conflicts will disappear.

This conflict between S3 and S6 can be resolved by explicitly clarifying the statement 3 that only **current valid** employees are capable of handling the rental orders placed by customers and thereby directing them login so the system can check whether they are currently employed or not to do any task related to the website.

3.2. Conflict between S6 and S8:

- **Specialize conflict source or target:**

This method will identify the source objects involved in the conflicting statements S6 and S8 and specialize them so the conflicts will disappear.

To expressly state that users must have access to a laptop, desktop, or mobile device as well as their login credentials in order to rent and reserve tools on the ETR website, thus resolving the issue between S6 and S8.

- **Weaken conflicting Statements:**

This method aims to make one or more of the conflicting statements less restrictive so as to resolve the conflict.

This conflict can be weakened by providing a direct access link to ETR's customer login portal in order to eliminate this friction.

3.3. Conflict between S9 and S10:

- **Restore conflicting statements:**

Statements (S9) and (S10) can be retained by requiring the user to show a hard copy of ID proof at the checkout of the branch store despite uploading one to their account.

- **Weaken conflicting Statements:**

This method will resolve the conflict by making one or more of the conflicting statements less restrictive.

The requirement of uploading identification when registering for the first time in statement (S9) can be optional, and an employee at the branch can verify an individual's identity with statement (S10).

Task 4: Conflict evaluation

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

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

1. **Evaluation for S3 and S5:**

		Options Scores	
Evaluation Criteria NFR	**Significance Weighting**	**Option1: Direct to Employee Login Portal link**	**Option2: Specify the statement clearly**
Fast response	0.3	0.9	0.7
Reliable response	0.6	0.8	0.8
Minimal inconvenience	0.1	0.8	0.7
Total	1.0	0.83	0.76

The option1 “**Direct to Employee Login Portal Link**” seems to be a better option according to the above estimates.

2. **Evaluation for S6 and S8:**

		Options Scores	
Evaluation Criteria NFR	**Significance Weighting**	**Option1: Access through laptop/desktop/mobile along with User registration**	**Option2: Access through customer login portal**
Fast response	0.3	0.9	0.8
Reliable response	0.6	0.7	0.8

Minimal inconvenience	0.1	0.7	0.7
Total	1.0	0.76	0.79

The option 2 “**Access through customer login portal**” seems to be a better option according to the above estimates.

3. Evaluation for S9 and S10:

		Options Scores	
Evaluation Criteria NFR	**Significance Weighting**	**Option1: The user can upload documents for the age verification**	**Option2: An employee at the branch can verify the ID of the users**
Fast response	0.3	0.5	0.7
Reliable response	0.6	0.6	0.8
Minimal inconvenience	0.1	0.5	0.7
Total	1.0	0.56	0.76

The option2 “**An employee at the branch can verify the ID of the users**” seems to be a better option according to the above estimates.

Task 5: Risk management

Risk Identification

Component Inspection:

i) Security Risk: There are currently no encryption techniques used by ETR to protect data. Hence, the chances of a data breach or hack are extremely high.

ii) Communication Loss/ Network Connectivity: Unnatural circumstances can result in data loss or downtime anytime.

iii) Performance Risk: There is a possibility that the server will throw errors such as downtime, which can take longer than 100ms for a page to load when numerous users are attempting to access the same content. In rare instances, the view function takes a longer time than expected to retrieve data.

iv) Database Server Failure Risk: There is a risk that the database component may crash and the replica for the database will not be available, which will render the entire system unavailable.

Risk Checklist:

Risk Checklists are the ones which can be built from risk categories that negatively impact the requirements of the system. Checklists include various elicitation criteria that depend on non- functional requirements of the system such as Cost, Deadline, Confidentiality, Useability etc.

i) **Confidentiality(Security Risk):** Hackers, cyberterrorists, and others have the ability to steal an authenticated user's ID, password, and other vital and sensitive information. Additionally, hackers prevent authorized users from accessing the system by conducting a DOS (Distributed Denial of Service) attack on it.

ii) **Cost(Performance Risk):** Making the system platform independent may increase the overall development cost.

iii) **Time(Performance Risk):** In order to make the system platform independent, the deadline for completing the project on time can also increase.

iv) **Useability:** With so many functionalities in the system, the user might find it difficult to operate without getting overwhelmed.

Risk Tree:

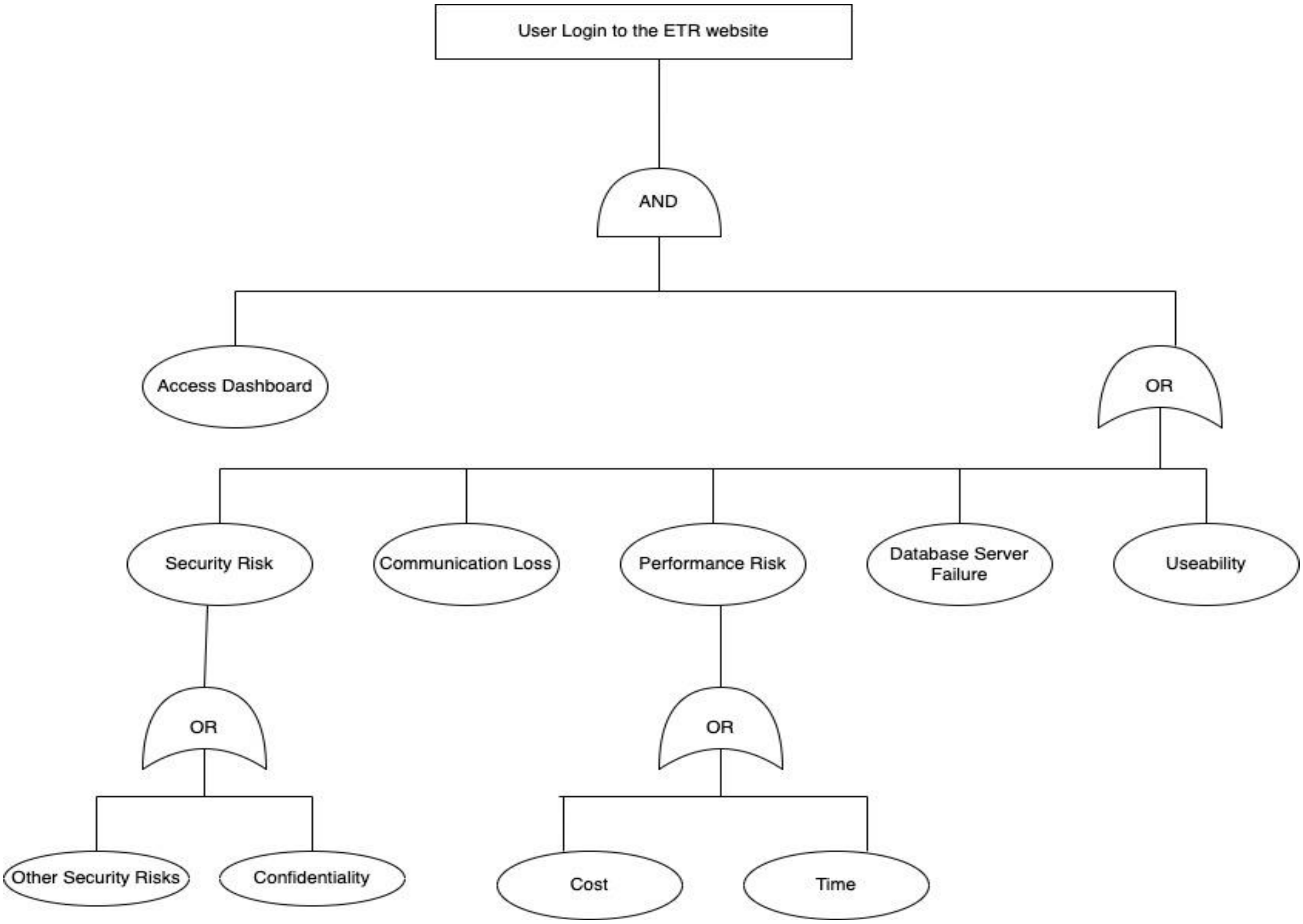

Figure 1: Risk Tree

- **Other Security Risks –** Integrity issues, Availability

Quantitative Assessment of Risk Identified:

Risk	**Rationale**	**Likelihood**	**Severity (1-10)**	**Risk Exposure (Likelihood* Severity)**
Security Risk /	There are very high chances of data breaches and	40%	8	3.2

Confidentiality	hacking if not using any encryption techniques (LIKELY)			
Communication Loss/ Network Connectivity	A high probability exists of unexpected events resulting in data loss or downtime at any time.(LIKELY)	35%	4	1.4
Performance Risk / Cost / Time	This can lead to numerous errors from the server. It can also take longer than expected for the view function to retrieve data in some cases.(POSSIBLE)	30%	6	1.8
Database Server Failure Risk	There is a risk that the database component may crash while under heavy load.(LIKELY)	35%	7	1.4
Useability	There is a probability that the user might find it difficult to operate the system because of the presence of so	15%	3	0.45

	many features in the system(POSSIBLE)			

Risk Control:

We will be using Risk Reduction Leverage (RRL) to calculate the better countermeasure for a particular risk.

$$Risk\ reduction\ leverage\ (RRL) = \frac{RE_{before} - RE_{after}}{Cost\ of\ risk\ reduction}$$

$$RE = risk\ probability\ x\ amount\ at\ stake$$

1. **Security Risk / Confidentiality:**

Estimated Cost = $80,000

Probability of this Risk = 0.40

Risk Exposure = impact x Risk Probability

= $80,000 x 0.04

= $32,000

Risk Exposure before = $32,000

Alternative Option 1: By Reduce Consequence likelihood tactic, this risk can be countered by introducing new requirement as, any information, particularly private information, stored into database must be stored in encrypted form.

Estimated Cost = $80,000

Probability of this Risk = 0.30

Risk Exposure = impact x Risk Probability

= $80,000 x 0.30

= $24,000

Risk Reduce Leverage (RRL1):

Cost of Risk Reduction = $9000
Risk Reduce Leverage (RRL1) = (RE before – RE after)/Cost of Risk Reduction

= (32,000 – 24,000)/9000

= 0.89

Alternative Option 2: By using the Reduce Risk Likelihood strategy, this risk can be mitigated by introducing new requirements, such as the need for the server to be digitally secure, which can be achieved by purchasing a firewall, securing the system code, implementing Secure Sockets Layer (SSL), limiting uploads, and employing passwords.

Estimated Cost = $80,000

Probability of this Risk = 0.20

Risk Exposure = impact x Risk Probability

= $80,000 x 0.20

= $16,000

Risk Reduce Leverage (RRL2):

Cost of Risk Reduction = $12,000
Risk Reduce Leverage (RRL2) = (RE before – RE after)/Cost of Risk Reduction

= (32,000-16,000)/12,000

= 1.33

Here, while comparing RRL of both the alternatives, option 2 looks more promising because the RRL value of option 2 (RRL2) is greater than 1.

2. **Communication Loss/ Network Connectivity:**

Estimated Cost = $40,000

Probability of this Risk = 0.35

Risk Exposure = impact x Risk Probability

= $40,000 x 0.35

= $14,000

Risk Exposure before = $14,000

Alternative Option 1: Using the Reduce Consequence Likelihood strategy, this risk can be reduced by introducing new requirements such as a good internet connection and the use of the best Internet Service Providers for the users.

Estimated Cost = $40,000

Probability of this Risk = 0.25

Risk Exposure = impact x Risk Probability

= $40,000 x 0.25

= $10,000

Risk Reduce Leverage (RRL1):

Cost of Risk Reduction = $2,500
Risk Reduce Leverage (RRL1) = (RE before – RE after)/Cost of Risk Reduction

= (14,000 – 10,000)/2,500

= 1.60

Alternative Option 2: This risk can be countered using the Reduce Risk Likelihood tactic by introducing new requirements, such as requiring users to use laptops or smart phones with battery backup, so they can remain connected even in case of power failure.

Estimated Cost = $40,000

Probability of this Risk = 0.30

Risk Exposure = impact x Risk Probability

= $40,000 x 0.30

= $12,000

Risk Reduce Leverage (RRL2):

Cost of Risk Reduction = $2,400
Risk Reduce Leverage (RRL2) = (RE before – RE after)/Cost of Risk Reduction

= (14,000-12,000)/1000

= 0.83

Here, while comparing RRL of both the alternatives, option 1 looks more promising because the RRL value of option 1 (RRL1) is greater than 1.

3. Performance Risk / Cost and Time:

Estimated Cost = $60,000

Probability of this Risk = 0.30

Risk Exposure = impact x Risk Probability

= $60,000 x 0.30

= $18,000

Risk Exposure before = $18,000

Alternative Option 1: Using the Reduce Risk likelihood tactic, this risk can be countered by introducing new requirements that should be introduced as, initially, the system should be designed for only one platform, and then when it performs well or is needed, it can be made platform independent.

Estimated Cost = $60,000

Probability of this Risk = 0.25

Risk Exposure = impact x Risk Probability

= $60,000 x 0.25

= $15,000

Risk Reduce Leverage (RRL1):

Cost of Risk Reduction = $3,200
Risk Reduce Leverage (RRL1) = (RE before – RE after)/Cost of Risk Reduction

= (18,000 – 15,000)/2,100

= 0.94

Alternative Option 2: A new requirement can be introduced as part of the Avoid Risk tactic to counter this risk. The new requirement is that the system should be developed by experienced developers who are proficient in several programming languages and able to work quickly.

Estimated Cost = $60,000

Probability of this Risk = 0.20

Risk Exposure = impact x Risk Probability

= $60,000 x 0.20

= $12,000

Risk Reduce Leverage (RRL2):

Cost of Risk Reduction = $3,500
Risk Reduce Leverage (RRL2) = (RE before – RE after)/Cost of Risk Reduction

= (18,000-12,000)/3,500

= 1.71

Here, while comparing RRL of both the alternatives, option 2 looks more promising because the RRL value of option 2 (RRL2) is greater than 1.

4. Database Server Failure Risk:

Estimated Cost = $70,000

Probability of this Risk = 0.35

Risk Exposure = impact x Risk Probability

= $70,000 x 0.35

= $24,500

Risk Exposure before = $24,500

Alternative Option 1: The Reduce Risk Likelihood tactic counters this risk by introducing new requirements, such as, ensuring the server is capable of handling a greater volume of traffic at a single time and scheduling regular backups of all data to be done on multiple servers.

Estimated Cost = $70,000

Probability of this Risk = 0.25

Risk Exposure = impact x Risk Probability

= $45,000 x 0.25

= $17,500

Risk Reduce Leverage (RRL1):

Cost of Risk Reduction = $7,500
Risk Reduce Leverage (RRL1) = (RE before – RE after)/Cost of Risk Reduction

= (24,500 – 17,500)/7,500

= 0.93

Alternative Option 2: The Risk Consequence Likelihood tactic can be applied to counteract this risk by introducing new solutions, such as offsite backups, cloud storage, and site duplication to prevent permanent loss of data and operational capabilities.

Estimated Cost = $70,000

Probability of this Risk = 0.20

Risk Exposure = impact x Risk Probability

= $70,000 x 0.20

= $14,000

Risk Reduce Leverage (RRL2):

Cost of Risk Reduction = $6000
Risk Reduce Leverage (RRL2) = (RE before – RE after)/Cost of Risk Reduction

= (24,500 -14,000)/6,000

= 1.75

Here, while comparing RRL of both the alternatives, option 2 looks more promising because the RRL value of option 2 (RRL2) is greater than 1.

5. Useability:

Estimated Cost = $30,000

Probability of this Risk = 0.15

Risk Exposure = impact x Risk Probability

= $30,000 x 0.15

= $4,500

Risk Exposure before = $4,500

Alternative Option 1: This risk can be minimized by introducing new requirements, such as a good and simple user interface that is intuitive and easy to use for everyone.

Estimated Cost = $30,000

Probability of this Risk = 0.10

Risk Exposure = impact x Risk Probability

= $30,000 x 0.10

= $3,000

Risk Reduce Leverage (RRL1):

Cost of Risk Reduction = $2,500
Risk Reduce Leverage (RRL1) = (RE before – RE after)/Cost of Risk Reduction

= (4,500 – 3,000)/2,500

= 0.60

Alternative Option 2: The Avoid Risk tactic can mitigate this risk by introducing a new requirement: System should contain a "How-to-use" pdf and a video explaining how to utilize various features of the system.

Estimated Cost = $30,000

Probability of this Risk = 0.07

Risk Exposure = impact x Risk Probability

= $30,000 x 0.07

= $2,100

Risk Reduce Leverage (RRL2):

Cost of Risk Reduction = $2,000
Risk Reduce Leverage (RRL2) = (RE before – RE after)/Cost of Risk Reduction

= (4,500 –2,100)/600

= 1.20

Here, while comparing RRL of both the alternatives, option 2 looks more promising because the RRL value of option 2 (RRL2) is greater than 1.

Task 0 - Logging

Tasks	**Section**	**Time Spent(Hours)**
Task 1	Identifying and finding inconsistencies in vision document	6
Task 2	Documenting conflicts	4
Task 3	Conflict resolution	3
Task 4	Conflict evaluation	4
Task 5	Risk management	4
Total: 21 hours		

Reference:

[1] Professor notes and slides

[2] Sample projects shared by professor