OnSite Risk Analysis Report

Executive Summary

The risk analysis report aims to assess the potential risks associated with the OnSite(https://www.onsite.run/#/databaseIntroduction) software project. By identifying and analyzing risks, this report provides insights to mitigate and manage them effectively, ensuring successful project completion.

Introduction

"Public Natural Driving Intelligent Vehicle Simulation Test Environment (OnSite)" serves as a public platform for evaluating the perception, decision-making, planning, and control modules of highly automated driving vehicles. This environment is based on the developing team's previous accumulation of road collection scenarios, test optimization algorithms, simulation tools, etc.

Risk Identification & Risk Assessment

No.	Quality Risk	Tech. Risk	Bus. Risk	Risk Pri. #	Extent of Testing	Tracing
1	Functionality					
1.01	Browsers unable to access the Web (at all).	5	1	5	Extensive	2.1
1.02	Browsers unable to register an account, while they input the correct personal details.	5	2	10	Broad	2.1.1.a
1.03	Browsers are unable to log in, while they input the correct ID and password.	5	2	10	Broad	2.1.1.b

1.04	Users logout fails.	5	4	20	Oppotunity	2.1.1.b
1.05	Fake or Fraudulent Registrations are not handled properly.	3	2	6	Broad	2.1.1.a
1.06	Inadequate validation of user input during the registration process.	5	2	10	Broad	2.1.1.a
1.07	Unable to be browsed in different OS, such as Windows, Android and IOS, as well as different browsers.	2	3	6	Broad	2.1
1.08	Inability of the software or infrastructure to handle increased workloads or user demands, leading to performance degradation or system failure under heavy usage.	3	2	6	Broad	2.1
1.09	Inaccurate or outdated information: There is a risk that the questions displayed may contain incorrect or outdated information, leading to confusion for users.	5	4	20	Oppotunity	2.1.3.a
1.10	Unreliable or biased answers: Users providing answers may provide unreliable or biased information, potentially misleading other users.	5	4	20	Oppotunity	2.1.3.d
1.11	Inaccurate or outdated information: There is a risk that the displayed background and functionality information may be inaccurate or outdated, leading to confusion for users.	5	2	10	Broad	2.1.4.a
1.12	Incomplete or unclear information: There is a risk of providing incomplete or unclear information about the testing techniques, which can hinder users' understanding.	5	3	15	Cursory	2.1.4.b
1.13	Outdated or unsupported tools: If the displayed testing tools are outdated or no longer supported, it can lead to confusion and wasted effort for users.	5	1	5	Extensive	2.1.4.c

1.14	Inconsistent or missing information: There is a risk of inconsistent or missing information for different scenarios, leading to confusion or incomplete understanding.	5	2	10	Broad	2.1.4.d
1.15	Incorrect or outdated competition information: There is a risk of displaying incorrect or outdated competition details, which can cause confusion and miscommunication among participants.	5	1	5	Extensive	2.1.4.e
1.16	Ambiguous or unclear rules: If the competition rules are not clearly defined or are open to interpretation, it can lead to disputes or unfairness.	5	2	10	Broad	2.1.4.d
2	Security					
2.01	Security Breaches: Unauthorized access or data breaches	2	1	2	Extensive	2.1.1.b
2.02	Weak Authentication: If the identity authentication mechanism is weak or poorly implemented, it may allow unauthorized individuals to gain access to user accounts.	3	1	3	Extensive	2.1.1.b
2.03	Insecure Storage: Storing personal information in an insecure manner can make it vulnerable to unauthorized access.	2	1	2	Extensive	2.1.1.c
2.04	Inadequate Access Controls: If the module lacks proper access controls, it may allow unauthorized users to view, modify, or delete personal information.	3	3	9	Broad	2.1.1.d
2.05	Brute-Force Attacks: Without proper measures to prevent brute-force attacks, malicious actors can attempt to guess or crack user passwords.	5	1	5	Extensive	2.1.1.b
2.06	Unauthorized Access to Scenario Document: If proper access controls	5	1	5	Extensive	2.1.2.a

	are not implemented, there is a risk of unauthorized individuals gaining access to the scenario document.					
2.07	Malicious or Malware-Infected Datasets: There is a risk of users uploading malicious or malware-infected datasets, which could compromise the security and integrity of the testing data management system.	4	1	4	Extensive	2.1.2.b
2.08	Unauthorized Access to Uploaded Datasets	4	1	4	Extensive	2.1.2.a
2.09	Data Integrity and Quality: When users are allowed to upload their own datasets, there is a risk of poor data quality, inconsistent formats, or incorrect data that could affect the overall testing process.	5	2	10	Broad	2.1.2.a
2.10	Resource Exhaustion: If there are no limitations or restrictions on dataset size or storage, users might upload large datasets that can consume excessive system resources	1	3	3	Extensive	2.1.2.a
2.11	Privacy and security concerns: If the questions include personal or sensitive information, there is a risk of exposing user data to unauthorized individuals.	5	2	10	Broad	2.1.3.a
2.12	Malicious code or scripts: Attackers may attempt to exploit vulnerabilities in the question posting functionality to inject malicious code or scripts.	5	2	10	Broad	2.1.3.b
3	Maintainability					
3.01	Difficulties in integrating various software components, modules, or third-party systems, resulting in interoperability issues or system instability.	2	2	4	Extensive	2.1

3.02	Lack of documentation.	4	2	8	Broad	2.1
3.03	Inconsistent coding standards and practices.	3	3	9	Broad	2.1
3.04	Inadequate error handling and logging	3	2	6	Broad	2.1
4	Usability					
4.01	Not meeting performance requirements, such as **slow response times**, high resource utilization, or scalability limitations.	4	5	20	Oppotunity	2.1
4.02	Spam or inappropriate content: Users may post spam or inappropriate content, which can negatively impact the user experience.	5	5	25	Report Bugs	2.1.3.b
4.03	Slow response time: If there is a large number of answers or inefficient retrieval mechanisms, the response time for browsing answers may be slow.	5	4	20	Oppotunity	2.1.3.c
4.04	Lack of moderation: Without proper moderation, there is a risk of inappropriate or offensive answers being posted.	5	5	25	Report Bugs	2.1.3.d
4.05	Poor user interface or user experience: If the information is not presented in a clear and intuitive manner, it can negatively impact user satisfaction.	5	4	20	Oppotunity	2.1.4
4.06	Difficulty in comprehending advanced concepts: If the techniques discussed are highly technical or complex, it may be challenging for users with limited knowledge to grasp them.	5	4	20	Oppotunity	2.1.4
4.07	Insufficient or unclear tutorials: If the tutorials lack necessary details or are not presented in a user-friendly manner, users may struggle to understand and utilize the testing tools effectively.	5	4	20	Oppotunity	2.1.4.c

4.08	Difficulty in interpreting the information: If the displayed information is not presented in a clear and concise manner, users may have difficulty interpreting and using it appropriately.	5	5	25	Report Bugs	2.1.4
5	Legal and Compliance					
5.01	The team does not have the right to run an official forum (copyright is not availiable).	5	1	5	Extensive	2.1
5.02	Legal and Compliance | Intellectual property infringement: Risk of violating copyright or intellectual property rights of third-party content or competition questions.	5	1	5	Extensive	2.1
5.03	Non-compliance with competition laws: Risk of non-compliance with competition laws, such as unfair competition practices or anti-trust regulations.	5	2	10	Broad	2.1

Conclusion

In conclusion, the risk analysis for the OnSite Website has identified several potential risks across different categories. These risks encompass security, maintainability, usability, and legal and compliance aspects. It is crucial for the website's developers and administrators to take proactive measures to mitigate these risks and ensure a secure, reliable, user-friendly, and compliant platform.