Sorting the risks on the basis of their risk exposure:

Risk ID	Risk Summary	Probability	Impact	Risk Exposure
1	Failure in Updating Information	80%	1	Rs. 72,000/month
2	Old data about train timings	70%	2	Rs. 56,000/month
3	Error in synchronization of admin and user module	60%	1	Rs. 48,000/month
4	Infiltration of Database	50%	2	Rs. 20,000/month
5	Violation of privacy	40%	3	Rs. 16,000/month

Impact:

1 – Catastrophic
2 – Critical
3 – Marginal
4 – Negligible

Risk Exposure:

Risk: Failure in Updating Information
The platform is meant to be used by daily commuters and tourists. Failure in updation of information can cause false timings and error in tracking. This can lead to chaos at stations and bus stops and create unnecessary congestion.

Risk Probability: 80%

Risk Impact:

The risk impact would be catastrophic as this would defeat the whole purpose of developing such an application.

The risk can be mitigated by regularly updating the app and staying in touch with the authorities for the latest information and schedule about the city transport. Hence, we create a team to stay in constant touch with the authorities and help us update our application.

This would consist of two members with charges of Rs. 45,000/month. For twomembers it would amount to Rs. 90,000/month.

Risk Exposure:

RE = 0.8 x Rs. 90,000 = Rs. 72,000/month.

Risk Information Sheet:

Risk ID: 1	**Date:** 25/03/2021	**Probability:** 80%	**Impact:** Catastrophic
Description: Failure in updation of information can cause false timings and error in tracking which can lead to chaos and congestion on the railway and bus stations.			
Refinement/Context: Sub condition 1: Change in timings of trains constantly could lead out of hand and then fail to update on the applications servers.			
Mitigation/Monitoring: 1. To regularly updating the app and staying in touch with the authorities for the latest information and schedule about the city transport.			
Management: RE computed to be Rs. 72,000 per month.			
Current Status: Mitigation steps to be initiated.			
Originator: Yash Dalwani		**Assigned:** Manav Gandhi	

Risk Exposure:

Risk: Old data about train timings.

Old redundant data can be harmful and decrease the accuracy in real time tracking of trains. This can create a confusion for the regular commuters and even more for tourists visiting the specific city.

Risk Probability: 70%

Risk Impact:

The risk impact would be catastrophic as this would lead to a lot of confusion among the commuters and create unnecessary chaos on the stations.

The risk can be mitigated by giving users to mark the train as no longer acccurate. A department consisting of two members would be set up to analyse this and remove them if not applicable from the platform.

The department would consist of two members with charges of Rs. 40,000/month. For two members it would amount to Rs. 80,000/month.

Risk Exposure:

RE = 0.7 x Rs. 80,000 = Rs. 56,000/month.

Risk Information Sheet:

Risk ID: 2	**Date:** 25/03/2021	**Probability:** 70%	**Impact:** Catastrophic
Description: Old redundant data can be harmful and decrease the accuracy in real time tracking of trains. This can create a confusion for the regular commuters and even more for tourists visiting the specific city.			
Refinement/Context: Sub condition 1: Authorities may update schedule oftenly.			
Mitigation/Monitoring: 1. Users will get an option to mark trains which are no longer accurate 2. Department will be set up to remove these trains from the application			
Management: RE computed to be Rs. 56,000 per month.			
Current Status: Mitigation steps to be initiated.			
Originator: Yash Dalwani		**Assigned:** Manav Gandhi	

Risk Exposure:

Risk: Error in synchronization of admin and user module.

The application has two modules which help in accurate updation of the schedule by both admin and the user. Error in synchorinisation of the same may lead to incorrect communication between the two modules.

Risk Probability: 70%

Risk Impact:

The risk impact would be critical as this would seriously affect the performance of the website. The increase in loading time of the website would lead to unsatisfied users. These users may switch to other websites. Therefore, there is a very big need to maintain the admin and user modules proactively.

The risk can be mitigated by making sure that the two modules are communicating with each other and testing them with various tests for eg stress, performance, etc. This will be done by the testing department. This will ensure that the modules run at optimal performance levels under any amount of workload.

The department would consist of two members with charges of Rs. 40,000/month. For two members it would amount to Rs. 80,000/month.

Risk Exposure:

RE = 0.6 x Rs. 80,000 = Rs. 48,000/month.

Risk Information Sheet:

Risk ID: 3	**Date:** 25/03/2021	**Probability:** 60%	**Impact:** Critical
Description: The application has two modules which help in accurate updation of the schedule by both admin and the user. Error in synchorinisation of the same may lead to incorrect communication between the two modules.			
Refinement/Context: Sub condition 1: Old properties may not have been removed from the platform. Sub condition 2: Such old properties in the database would lead to a lot of time in querying the database depending on the user filters. This would degrade he website performance.			
Mitigation/Monitoring: 1. Making sure two modules communicate under all circumstances. 2. Testing department to conduct various tests.			
Management: RE computed to be Rs. 48,000 per month.			
Current Status: Mitigation steps to be initiated.			
Originator: Yash Dalwani		**Assigned:** Vedant Deshmukh	

Risk Exposure:
Risk: Infiltration of Database
The application will have data of several properties in the database. This can be leaked when infiltrated causing data loss. It can be a crucial threat to the users using the application.

Risk Probability: 50%

Risk Impact:

Malware can cause significant loss and incur substantial costs to organizations. The desire to avoid detection coupled with often lucrative nature of malware development means that there is a high probability that new malware is developed it will likely utilise unknown techniques. This can then lead to loss of user data from the databases once infiltrated. Though it can be mitigated by using some firewalls to prevent malware attacks via input details. This can reduce their attacks by a great margin. The cost can go up to Rs. 40,000 per month.

Risk Exposure:

RE = 0.5 x Rs. 40,000 = Rs. 20,000/month.

Risk Information Sheet:

Risk ID: 4	**Date:** 25/03/2021	**Probability:** 50%	**Impact:** Critical
Description: The application will have data of several properties in the database. This can be leaked when infiltrated causing data loss. It can be a crucial threat to the users using the application.			
Refinement/Context: Sub condition 1: Malware can slow down a user's computer and has the ability to crash some websites. It can infect your computer and use it as a server to broadcast various files or attacks. Sub condition 2: Malware can send emails you did not write getting you or your company in trouble which can result in the company's huge loss. To minimize these attacks firewalls are used.			
Mitigation/Monitoring: 1. Use of antivirus, firewalls and anti-malware software. 2. Monitoring should be in place to verify the security state of: a. Update your operating system, browsers, and plugins. b. Read the emails with eagle eyes. c. Don't believe cold callers. d. Don't call fake tech support. e. Make sure you're on a secure connection. f. Use strong passwords or password managers.			
Management: RE computed to be Rs. 20,000 per month.			
Current Status: Mitigation steps to be initiated.			
Originator: Manav Gandhi		**Assigned:** Yash Dalwani	

Risk Exposure:

Risk: Violation of privacy

In today's world, data is the new oil. Therefore companies, organizations and hackers are always on the lookout for more and more data. This has increased the risk of hackers trying to mine important user data.

Risk Probability: 40%

Risk Impact:

Privacy violation may lead to accounts getting hacked, identity theft, impersonation, targeted ads as well as wrong people seeing the information. This could also harm the reputation of the platform and people would soon lose trust in the application. Information about properties could also be used by other competitors. Contact information about users may be used for marketing purposes.

This can be mitigated by outsourcing cloud security to cloud provider such as Cloudfare. This will cost up to Rs. 20,000 per month.

Risk Exposure:

RE = 0.4 x Rs. 40,000 = Rs. 16,000/month.

Risk Information Sheet:

Risk ID: 5	**Date:** 25/03/2021	**Probability:** 40%	**Impact:** Marginal
Description: In today's world, data is the new oil. Therefore companies, organizations and hackers are always on the lookout for more and more data. This has increased the risk of hackers trying to mine important user data.			
Refinement/Context: Sub condition 1: Hackers may attempt to steal personal information of users such as email addresses and passwords. Sub condition 2: Activity log of the users can also be targeted with the intention to analyse this data and provide targeted ads to the user. This is a serious breach of privacy.			
Mitigation/Monitoring: 1. Creation of automatic backups of the database. 2. Monitoring should be in place to verify the security state of: a. DNS records b. SSL certificates c. Web server configuration d. Application updates e. User access f. File integrity			
Management: RE computed to be Rs. 16,000 per month.			
Current Status: Mitigation steps to be initiated.			
Originator: Vedant Deshmukh		**Assigned:** Manav Gandhi	