Walkthrough Agenda 3/8/2023 at 1:30 PM in OBT 312

Team Name: C3J

Describe our project as review for the participants in the walkthrough. (2 minutes)

(My explanation)

1:51 is actually doable

1. Our business goals are:
   - Bus-Users: increase userbase and general engagement
   - Bus-Rev: generate revenue
   - Bus-Part: foster partnerships
   - Bus-Educ: promote education and awareness

1a. Are these all of the goals that we want to consider or achieve? (4 minutes)

2:00 Chris reviewing business goals, we wanted to create a different set of values to determine what our business values.

Users are important to our application development process. We want to increase their general experience, not only in the market but also once they have used the app. We want to increase engagement by the leaderboards.

Important is to generate revenue by not being 1 dimensional in how we generate revenue.

Similar is partnership. We want to connect with other companies and key personnel.

Business education- how we can promote education among ourselves and among the users in the collective use of our energy. We want awareness of their energy usage and their emission.

4:10 first question- are there new ids or business goals.

Jacob asks Sigman is there any more goals that we are missing.

Brand and reputation- possibly. We have to prioritize something.

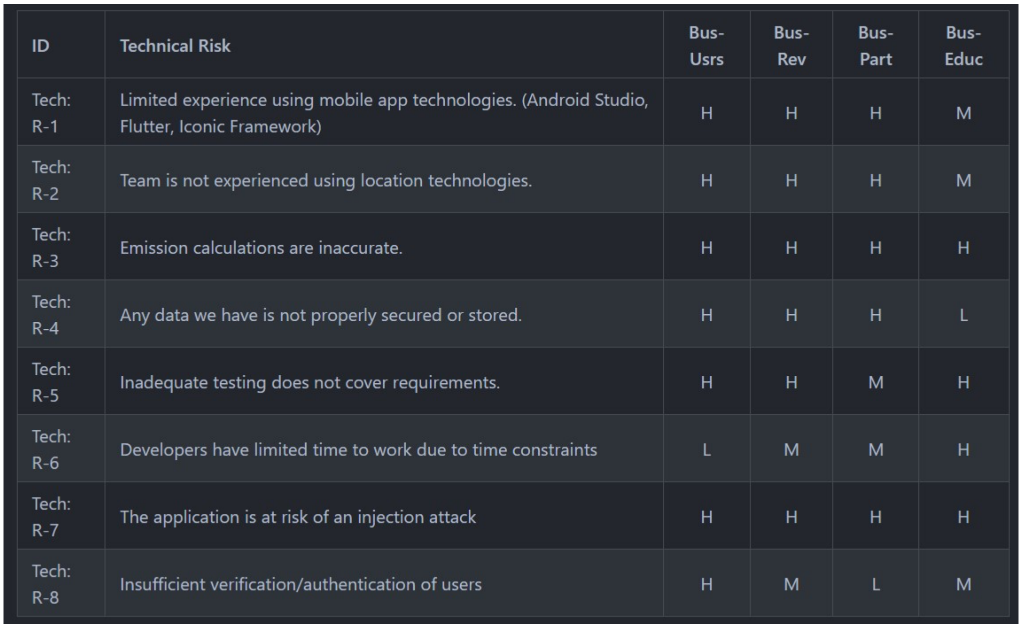
5:06 if we are a for-profit business, could we be a non-profit?

POSSIBLE ADD: We could funnel our revenue into more ways to contribute to the world, education resources, we could be non-profit while still generating revenue.

6:20 We don't have to balance out to zero as a non-profit, based on Sigman's experience. "We still have years where we don't spend all that we take in". "Consortion covered it back so we are a 5013C non-profit".

7:51 would being a non-profit fit us better?

2. We have 8 risk potential technical risks:



ID	Technical Risk	Bus-Usrs	Bus-Rev	Bus-Part	Bus-Educ
Tech: R-1	Limited experience using mobile app technologies. (Android Studio, Flutter, Iconic Framework)	H	H	H	M
Tech: R-2	Team is not experienced using location technologies.	H	H	H	M
Tech: R-3	Emission calculations are inaccurate.	H	H	H	H
Tech: R-4	Any data we have is not properly secured or stored.	H	H	H	L
Tech: R-5	Inadequate testing does not cover requirements.	H	H	M	H
Tech: R-6	Developers have limited time to work due to time constraints	L	M	M	H
Tech: R-7	The application is at risk of an injection attack	H	H	H	H
Tech: R-8	Insufficient verification/authentication of users	H	M	L	M

8:20- we have identified 8 primary risks.

1- Limited experience using mobile app technology, team currently has no experience professionally. High risk overall, no one wants to advertise on a poorly built application
2- Same risks as we mentioned beforehand, could lead to negative experience
3- Emission calculations is the highest risk we have since this is the core of our application if it's inaccurate it will impact all our goals since no one will want to use or be affiliated with it. If calculations aren't correct, we can't provide this education to others.
4- Improperly secured data, this could be a large risk to our users, revenue, could lead to potential lawsuits, not good for the brand/working with other companies.
5- (10:41) improper testing leading to bad experience for the users, less downloaded if testing is not done properly

6- Limited time constraints since it won't affect the users as much, but the project will be delayed. Medium impact on goals since it will make some impact.

7- Risk of an injection attack, also high like the emission attack. Could impact all goals, since when a user attempts to use our app, they could be at risk as well.

8- Mainly impacting the user itself, waterfalling down to the other goals. If we don't properly secure each account it will lead to negative user experience if we have loss of progress and data.

2a. Should the severity of these technical risks be reevaluated compared to Business IDs?

12:50 questions posed. Explain the user data, that could be usernames, emails, password, GPS data.

13:48 is the data significant enough to be listed as high? GPS makes it high. The minute we put GPS data, this is very high-risk data since it tracks the user.

14:33 Risk 7- ADD MORE DETAIL? - application is at risk of an injection attack. I assume SQL injection attack, SQL injection attack. Jacob answer- In the user sign up form, log in form, emission part, typing miles if not formatting right could lead to injection. Finding a backdoor to create a group.

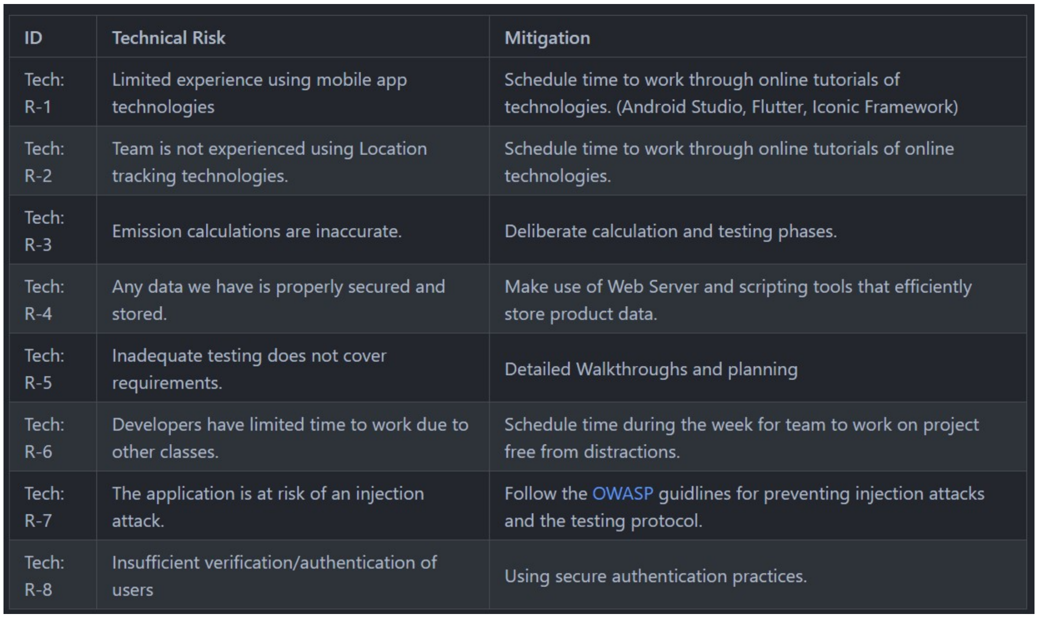
16 Yes, you've convinced me that it should be listed as high. XSS could be added to that risk.

2b. Are there any risks that should be removed or added? (7 minutes)

3. We have 8 methods to mitigate the previously mentioned risks.

16:52 Jace- we have devised mitigation methods for each of these risks

1- Straight forward mitigation, ways to learn these technologies sufficient enough to build this app, using Udemy and Youtube tutorials.
2- Same thing, set aside enough time for everyone on the team to learn these independently. Documentation can be used to learn these.
3- Deliberate calculation and testing phases in the creation of these formulas to calculate the users emissions. ADD: using external resources to create these formulas, since none of us have experience in environmental science calculations.
4- (18:44) Mitigation- using a secure server, and database, using things like hasing of passwords.
5- Inadequate testing does not get requirements, straightforward make sure it's tested enough.
6- (19:43) Limited time, we need to make sure that we schedule time during the week to work.
7- Injection attack, follow OWASP guidelines for injectinon attacks, filtering our inputs that interact with the databases.
8- (20:19) using secure authentication practices such as 2FA or email sent.



ID	Technical Risk	Mitigation
Tech: R-1	Limited experience using mobile app technologies	Schedule time to work through online tutorials of technologies. (Android Studio, Flutter, Iconic Framework)
Tech: R-2	Team is not experienced using Location tracking technologies.	Schedule time to work through online tutorials of online technologies.
Tech: R-3	Emission calculations are inaccurate.	Deliberate calculation and testing phases.
Tech: R-4	Any data we have is properly secured and stored.	Make use of Web Server and scripting tools that efficiently store product data.
Tech: R-5	Inadequate testing does not cover requirements.	Detailed Walkthroughs and planning
Tech: R-6	Developers have limited time to work due to other classes.	Schedule time during the week for team to work on project free from distractions.
Tech: R-7	The application is at risk of an injection attack.	Follow the OWASP guidlines for preventing injection attacks and the testing protocol.
Tech: R-8	Insufficient verification/authentication of users	Using secure authentication practices.

3a. Are the listed mitigation techniques sufficient?

Questions posed at 20:48 – Sigman said that these are good. Let me throw out some ideas, such as 1 and 2, it's obvious that we have limited experience, since all we have is what we've already learned in class. Maybe alongside that, we need to also bring in someone with experience. How do we do that? (22) POSSIBLE ADD: Hire someone to teach us mobile. If we do non-profit, make it an open-sourced project, if they like to contribute to a humanitarian type of project. So maybe listing the project as open-sourced. We have a bunch of different approaches.

ADD: These have to be in literature some where of how to calculate carbon emission. There must be calculations that are accurate in literacture, start a LITERATURE SEARCH. Depending on what we find there are data sets available. Someone on the team may have the background to use dataset and calibrate models from exisintg data set. Maybe you don't want formulas, maybe we want a deep learning set. Testing phases are importate, calibration of the model ADD for a mitigation factor.

24:51 ADD establishing a detailed testing strategy that is complete that is not just walkthroughs, but also unit testing, required regression testing, established acceptance testing. We have to plan for those things.

26 minute Number 8- ADD thing about hiring or planning penetration testing. As software engineers we do not do this typically. Use cyber security experts that can do penetration for us, finding someone that would be willing to help.

It's a wonderful list but there's more mitigations that we haven't thought of yet but that's okay because we are doing this for the first time.

> 3b. What do we as individuals need to work on to learn map/mobile technologies? (7 minutes)

Ended at 26 minutes and 29 seconds.

Sigman, my only concern. Technical risks are mapped to business objectives. But there's a missing step here: we start with looking at identifying our business objectives, where are our business risks, how do these relate to our business objectives. ADD BUSINESS RISKS: Technical risks map to business risks that map to business goals/objectives.