AIM: Prepare rmmm plan for the project

1) **What is risk and its types ?**

Risk can be defined as the probability of an event, hazard, accident, threat or situation occurring and its undesirable consequences. It is a factor that could result in negative consequences and usually expressed as the product of impact and likelihood.The following are the categories of the risk -

1. Project risk

If the project risk is real then it is probable that the project schedule will slip and the cost of the project will increase.

It identifies the potential schedule, resource, stakeholders and the requirements problems and their impact on a software project.

2. Technical risk

If the technical risk is real then the implementation becomes impossible.

It identifies potential design, interface, verification and maintenance of the problem.

3. Business risk

If the business risk is real then it harms the project or product.

There are five subcategories of the business risk:

1. Market risk - Creating an excellent system that no one really wants.

2. Strategic risk - Creating a product which no longer fit into the overall business strategy for companies.

3. Sales risk - The sales force does not understand how to sell a creating product.

4. Management risk - Loose a support of senior management because of a change in focus.

5. Budget risk - losing a personal commitment.

2) Steps for analysis of risks:

Step 1: Identify hazards, i.e. anything that may cause harm.

Employers have a duty to assess the health and safety risks faced by their workers. Your employer must systematically check for possible physical, mental, chemical and biological hazards.This is one common classification of hazards:

Step 2: Decide who may be harmed, and how.

Identifying who is at risk starts with your organisation's own full- and part-time employees. Employers must also assess risks faced by agency and contract staff, visitors, clients and other members of the public on their premises.Employers must review work routines in all the different locations and situations where their staff are employed.

Step 3: Assess the risks and take action.

This means employers must consider how likely it is that each hazard could cause harm. This will determine whether or not your employer should reduce the level of risk. Even after all precautions have been taken, some risk usually remains. Employers must decide for each remaining hazard whether the risk remains high, medium or low.

Step 4: Make a record of the findings.

Employers with five or more staff are required to record in writing the main findings of the risk assessment. This record should include details of any hazards noted in the risk assessment, and action taken to reduce or eliminate risk.

Step 5: Review the risk assessment.

A risk assessment must be kept under review in order to -

Ensure that agreed safe working practices continue to be applied (e.g. that management's safety instructions are respected by supervisors and line managers); and take account of any new working practices, new machinery or more demanding work targets.

Calculation of Risk Exposure

Risk Description	**Probability**	**Impact**	**Risk Exposure**
Update the dataset with wrong parameters values	20%	3	0.6
Chances of doctor password getting hacked.	40%	5	2.0

Total risk exposure=2.6

3) Identify 2 risks for your project

Risk Information Sheet(RIS)			
Risk ID: POS-001	Date: 26-3-2019	Probability: 40%	Impact: LOW
Description : Update the dataset with wrong parameters values			
Refinement/Context: If the parameter values are wrong then the model will give wrong prediction.			
Mitigation/Monitoring :Thecsv file should be made read only.			
Management/trigger:if someone tries to change the values un the dataset then the admin should get a message.			
Current Status 2-4-2019			
Originator: SS		Assigned: SS	

Risk Information Sheet(RIS)			
Risk ID:101	Date:8/03/2019	Probability: 80%	Impact: Low
Description: Chances of doctor password getting hacked.			
Refinement/Context: Since second step for authentication in our system is password validation there is a huge possibility that it could get hacked.			
Migration/Monitoring: We can use hashing techniques to protect our system from hacking			
Management/Contingency Plan/trigger: If the password gets hacked, the user should immediately change the password.			
Current Status: We will deploy .			
Originator: Developer		Assigned: Developer	

Conclusion:

In this experiment we have successfully identified the risks for our project: Cancer Prediction.