Table X: Risk analysis for

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Hazards** | **Is the hazard present? Y/N** | **What is the risk?** | **Risk rating**  **H = High**  **M = Medium L = Low** | **Controls**  **(When all controls are in place risk will be reduced).** | **Is this control in place?** | **Action/to do list/outstanding controls**  **\*Risk rating applies to outstanding controls outlined in this column** | **Person responsible** | **Signature and date completed** |
| Scheduled work Delays | Y | Project Delay | H | Good planning of project | N | Assign project manager to plan work schedule | sania | Sania 22Apr 2024 |
| Rework | Y | Wasted resources | M | Quality Assurance | Y | Review QA process effectiveness | Sania | Sania 22Apr 2024 |
| Excess Cost | Y | Financial loss | H | Legal review of contract | N | Engage legal contract | Sania | Sania 22Apr2024 |
| Change in requirement | Y | Creep scope | M | Clear scope documentation | Y | Regular stakeholder review | Sania | Sania 22/04/2024 |

If there is one or more **High Risk (H)** actions needed, then the risk of injury could be high and immediate action should be taken.

**Medium Risk (M)** actions should be dealt with as soon as possible. **Low Risk (L)** actions should be dealt with as soon as practicable.

Risk Assessment carried out by: Sania Date:22/04/2024 / /

© All Rights Reserved

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Hazards** | **Is the hazard present? Y/N** | **What is the risk?** | **Risk rating**  **H = High**  **M = Medium L = Low** | **Controls**  **(When all controls are in place risk will be reduced).** | **Is this control in place?** | **Action/to do list/outstanding controls**  **\*Risk rating applies to outstanding controls outlined in this column** | **Person responsible** | **Signature and date completed** |
| Technical process risk | Y | Wrongly selected technology stack | H | Senior developer, QA engineers will report changes, modifications. | Y | Project manager, QA engineer | Sania |  |
| Requirement related | Y | Multiple requests, inadequate requests | M | Get user stories in form of SMART Goals  Collecting appropriate user stories for the duration  of the project  Setup Software Requirement Specifications | Y | Project manager, QA engineer | Sania |  |
| Security risk | Y | Involves the potential for loss or damage an organization’s assets, data, and reputation | H | Encrypt data to protect it from unauthorized access. Utilize strong encryption algorithms and ensure that encryption keys are securely managed. Make long security password | Y | IT security engineer | Sania |  |
| Constraint related risks | Y | Environmental factors such as geographical location, climate conditions, or ecological condition may influence project | M | Make a project plan that accounts for all known constraints, including time, budget, resources, technology, regulations, and stakeholder expectations. Ensure that the project plan is realistic, achievable, and aligned with the project's objectives and constraints.  Prioritize project requirements based on their importance to the project's success and their alignment with project constraints | Y | Make a change management process to evaluate and approve changes to the project scope, schedule, or budget. Assess the impact of proposed changes on project constraints and stakeholders, and obtain appropriate approvals before implementing changes.  Keep a flexible and adaptive mindset to respond to changes in project constraints or external factors that may impact the project. | Sania |  |

If there is one or more **High Risk (H)** actions needed, then the risk of injury could be high and immediate action should be taken.

**Medium Risk (M)** actions should be dealt with as soon as possible. **Low Risk (L)** actions should be dealt with as soon as practicable.

Risk Assessment carried out by: Sania Date: 21/4/2024

© All Rights Reserved

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Hazards** | **Is the hazard present? Y/N** | **What is the risk?** | **Risk rating**  **H = High**  **M = Medium L = Low** | **Controls**  **(When all controls are in place risk will be reduced).** | **Is this control in place?** | **Action/to do list/outstanding controls**  **\*Risk rating applies to outstanding controls outlined in this column** | **Person responsible** | **Signature and date completed** |
| UI/UX design elaboration risks | Y | UI/UX designs without optimization for performance can result in slow loading times, unresponsive interfaces | L | User Research and requirement gathering to understand the needs, preferences, and behaviors of the target audiences. Make clear design goals and scope to prevent scope creep and maintain focus throughout the elaboration phase.  Identify potential risks and challenges associated with UI/UX design elaboration.  Maintain comprehensive documentation of the UI/UX design process, including design specifications, wireframes, prototypes, and design iterations |  | UX/UT testing engineer | sania |  |
| Constraint related risks for cost | Y | Allotted budget that must be managed effectively to ensure project success. Risks associated with budgetary constraints include insufficient funding, limited financial resources, or budget cuts imposed by stakeholders | M | Make comprehensive cost estimation during the project planning phase to accurately forecast expenses. Utilize historical data, expert judgment, and industry benchmarks to estimate costs for resources, materials, labor, and other project expenses.  Make a detailed project budget that aligns with the project scope, objectives, and requirements. Allocate funds to different project activities, deliverables, and phases based on their priority and criticality. Make a formal change control process to manage changes to the project scope, schedule, or requirements that could impact project costs |  | Finance manager | sania |  |
| Third-party integration risks | Y | Data breach.  Operational disruption.  Reputational damage | H | Strengthen the security supervision of the system to avoid leakage of important information. Set up machine supervision. | N | IT SECURITY Engineer |  |  |
|  |  |  |  |  |  |  |  |  |

If there is one or more **High Risk (H)** actions needed, then the risk of injury could be high and immediate action should be taken.

**Medium Risk (M)** actions should be dealt with as soon as possible. **Low Risk (L)** actions should be dealt with as soon as practicable.

Risk Assessment carried out by: sania Date:21/4/2024

© All Rights Reserved

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Hazards** | **Is the hazard present? Y/N** | **What is the risk?** | **Risk rating**  **H = High**  **M = Medium L = Low** | **Controls**  **(When all controls are in place risk will be reduced).** | **Is this control in place?** | **Action/to do list/outstanding controls**  **\*Risk rating applies to outstanding controls outlined in this column** | **Person responsible** | **Signature and date completed** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

If there is one or more **High Risk (H)** actions needed, then the risk of injury could be high and immediate action should be taken.

**Medium Risk (M)** actions should be dealt with as soon as possible. **Low Risk (L)** actions should be dealt with as soon as practicable.

Risk Assessment carried out by: Date: / /

© All Rights Reserved