**Risk Management Plan**

The Risk Management Plan (RMP) details the elements of risk to a project.

| **Project Name:** | AutoMart |
| --- | --- |
| **Project Number:** |  |
| **Date:** | 08/03/2023 |
| **Prepared by:** | Emiliano Cabrera, developer and Diego Corrales, developer |
| **Project Ownership:** | Gilberto Echeverría Furió |

**Project Contacts**

|  | **Name** | **Title/Position** | **Phone** | **Email** |
| --- | --- | --- | --- | --- |
| Primary | Diego Corrales Pinedo | Developer |  | A01781631@tec.mx |
| Other | Andrew Dunkerley Vera | Developer |  | A01025076@tec.mx |
| Other | Emiliano Cabrera Ruiz | Developer |  | A01015453@tec.mx |
| Other | Andrés Briseño Celada | Developer |  | A01352283@tec.mx |
| Other | Do Hyun Nam | Developer |  | A01025276@tec.mx |

**Version Control**

| **Version Number:** | 1.0 |
| --- | --- |
| **Released:** | 01/03/2023 |
| **Reason/Comments:** | First version of the Risk Management Plan. |

| **Version Number:** | 2.0 |
| --- | --- |
| **Released:** | 06/03/2023 |
| **Reason/Comments:** | Second version of the Risk Management Plan. Applied corrections given by Eduardo. |

| **Version Number:** | 3.0 |
| --- | --- |
| **Released:** | 08/03/2023 |
| **Reason/Comments:** | Third version of the Risk Management Plan. Applied corrections given by Eduardo. |

**Risk Assessment and Management Table**

*This table can be adapted to fit the circumstances of individual projects, including non-IT projects.*

*The project manager should retain the category headings in the RMP template, but change, add and delete table entries within those categories to customize the template to fit the specific project being addressed: project management risks, security risks, resource risks, client risks, technical risks, other risks.*

*Use the algorithm at the end to determine the priority of risk.*

| **Risk** | **Description** | **Likelihood[[1]](#footnote-0)** | **Consequences[[2]](#footnote-1)** | **\*Priority of risk [[3]](#footnote-2)**  \*\*Use algorithm | **Owner of the Risk** | **Control Strategies:**  **Mitigate or Accept** | **Proposed Containment Actions** | **Contingency Plan?**  **(Yes, No)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Project Management Risks** | | | | | | | | |
| Inadequate project definition \* | Unclear or wrong requirements, scope or project plan. | Likely | Major | High | Developers | Mitigate | Establish consistent communication with clients and get validation from clients and advisers after Requirement Phase. | Yes |
| Unrealistic time frames | Deadlines established in unrealistic dates. | Likely | Moderate | Significant | Developers | Mitigate | Prioritize activities based on which cannot be delayed, according to the Critical Route. | Yes |
| Lack of communication \* | Not enough communication between clients, developers and advisers. | Likely | Catastrophic | Very high | Developers and clients | Mitigate | Establish Directive, Executive and Operational committees. These will hold meetings at established intervals with established attendees to make decisions at different levels of the project. | Yes |
| Lack of proper documentation \* | Missing documents, inconsistent or incorrect information. | Likely | Major | High | Developers, advisers and clients | Mitigate | Request weekly feedback from Project Management advisers on the created documentation. | Yes |
| **Security Risks** | | | | | | | | |
| Accuracy and integrity of data and information \* | Information is incorrect and inconsistent across the system. Unauthorized modification of information is allowed. | Unlikely | Catastrophic | High | Developers and clients | Mitigate | Use industry-standard encryption/hashing algorithms and methodologies. Access to the application is session-based. There are different levels of access that are only assigned by administrators. | Yes |
| Principle of least privilege | Users are given access to unintended parts of the system, such as low-privilege final users having access to admin features. | Rare | Catastrophic | Significant | Developers and clients | Mitigate | There are different levels of access that are only assigned by administrators. | Yes |
| **Resource Risks** | | | | | | | | |
| Staff turnover | Development team attendance to class and meetings. | Almost certain | Minor | Significant | Developers | Mitigate | Daily SCRUM meetings. | No |
| Unclear roles and responsibilities | Members of the development team not knowing what their responsibilities are. | Likely | Moderate | Significant | Developers | Mitigate | Establish roles for each developer during the Requirement phase. Monitor and update duties using a Kanban board. | Yes |
| Insufficient funding | Lack of monetary resources for development. | Rare | Insignificant | Trivial | Developers | Mitigate | Create 3 different proposals for a Tech Stack considering different levels of available monetary resources: no money, limited money and unlimited money. | Yes |
| **Client Risks** | | | | | | | | |
| Inadequate business requirements | The client’s requests are unrealistic considering the resources that will be available to the development team. | Rare | Major | Significant | Developers, advisers and clients | Mitigate | Weekly client meetings in Requirement Phase in order to ascertain and narrow requirements to a realistic scope, using a Gantt chart to estimate development time. | Yes |
| **Technical Risks** | | | | | | | | |
| Procurement issues, including tendering | Problems obtaining necessary resources for development. | Rare | Insignificant | Trivial | Developers, advisers | Mitigate | Establish an architecture in the Requirements Phase and have it approved by the PO. This architecture will be based on demand estimates from the PO. | Yes |
| Technical problems | Accidental loss of development resources, such as broken computers. | Unlikely | Major | Significant | Developers | Mitigate | The latest version of the project will be uploaded in an online Github repository available to all developers. Documentation is stored in Google Drive and a Github repository. | Yes |

1 Likelihood = Almost Certain, Likely, Moderate, Unlikely or Rare

2 Consequences = Insignificant, Minor, Moderate, Major or Catastrophic

3 Priority of risk = Very High, High, Significant, Moderate, Low or Trivia

**\*\*Algorithm for Determining Prioritization of Risk**

| **Likelihood** | **Consequences** | | | | |
| --- | --- | --- | --- | --- | --- |
| **Insignificant** | **Minor** | **Moderate** | **Major** | **Catastrophic** |
| **Almost Certain** | **Significant** | **Significant** | **High** | **Very high** | **Very high** |
| **Likely** | **Moderate** | **Significant** | **Significant** | **High** | **Very high** |
| **Moderate** | **Low** | **Moderate** | **Significant** | **High** | **High** |
| **Unlikely** | **Low** | **Low** | **Moderate** | **Significant** | **High** |
| **Rare** | **Trivial** | **Trivial** | **Moderate** | **Significant** | **Significant** |

\* These are the priority risks, which would be presented to the client before the Implementation Phase.

1. Likelihood = Almost Certain, Likely, Moderate, Unlikely or Rare [↑](#footnote-ref-0)
2. Consequences = Insignificant, Minor, Moderate, Major or Catastrophic [↑](#footnote-ref-1)
3. Priority of risk = Very High, High, Significant, Moderate, Low or Trivial [↑](#footnote-ref-2)