**Aim:** Risk Analysis for SMS/Email Spam Detection System.

**Theory:**

**1.What is Risk and types?**

Risk is an expectation of loss, a potential problem that may or may not occur in the future. It is generally caused due to lack of information, control or time.A possibility of suffering from loss in the software development process is called a software risk. Loss can be anything, increase in production cost, development of poor quality software, not being able to complete the project on time. Software risk exists because the future is uncertain and there are many known and unknown things that cannot be incorporated in the project plan. A software risk can be of two types: (a) internal risks that are within the control of the project manager and (2) external risks that are beyond the control of project managers. Risk management is carried out to:

**Types Of Risks**

**1.Schedule / Time-Related / Delivery Related Planning Risks:**

Project schedule gets slip when project tasks and schedule release risks are not addressed properly. Schedule risks mainly affect a project and finally on the company economy and may lead to project failure.

**Schedules often slip due to the following reasons:**

Wrong time estimation

Resources are not tracked properly. All resources like staff, systems, skills of individuals, etc.

 Failure to identify complex functionalities and time required to develop those functionalities.

Unexpected project scope expansions.

**2.Budget / Financial Risks:**

These are the monetary risks which are associated with budget overruns.

Some of the reasons for such risks are

  a.Improper Budget Estimation

  b.Cost Overruns due to underutilization of resources

  c.Expansion of Project Scope

  d.Improper Tracking of Finances

  e.Underutilization of resources especially happens when resources are shared between projects                because it becomes difficult to effectively manage such resources and a certain amount of productivity may go waste.

  f.Further, unexpected expansion of project scope (due to addition of features by clients, etc) may lead to budget overruns as such expansions may not have been factored into the original estimates.

  g.Delay of projects may also have certain penalty costs associated with it e.g. construction projects

**3.Operational / Procedural Risks:**

Risks of loss due to improper process implementation failed system or some external events risks.

Causes of Operational Risks:

Failure to address priority conflicts

Failure to resolve the responsibilities

Insufficient resources

No proper subject training

No resource planning

No communication in the team.

**4.Technical / Functional / Performance Risks:**

Technical risks generally lead to failure of functionality and performance.

Causes of Technical Risks are:

 1. Continuous changing requirement.

 2. No advanced technology available or the existing technology is in the initial stages.

 3. The product is complex to implement.

 4. Difficult project modules integration.

**5.Other Unavoidable Risks:**

These are the external risks beyond the operational limits.

These are all uncertain risks that are outside the control of the program.

These external events can be:

Running out of the fund, Market development,Changing customer product strategy and priority,Government rule changes.

**2.Steps for Risk Analysis**

**A.Risk Identification**

**Product size**—risks associated with the overall size of the software to be built or modified.

**Business impact**—risks associated with constraints imposed by management or the marketplace.

**Customer characteristics**—risks associated with the sophistication of the customer and the developer's ability to communicate with the customer in a timely manner.

**Process definition**—risks associated with the degree to which the software process has been defined and is followed by the development organization.

**Development environment**—risks associated with the availability and quality of the tools to be used to build the product.

**Technology to be built**—risks associated with the complexity of the system to be built and the "newness" of the technology that is packaged by the system.

**Staff size and experience**—risks associated with the overall technical and project experience of the software engineers who will do the work.

**B.Risk Assessments**

Risk impact assessment is the process of assessing the probabilities and consequences of risk events if they are realized.

The results of this assessment are then used to prioritize risks to establish a most-to-least-critical importance ranking.

Ranking risks in terms of their criticality or importance provides insights to the project's management on where resources may be needed to manage or mitigate the realization of high probability/high consequence risk events.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Category** | **Probability** | **Impact** | **RMMM** |
| Customer will change requirements | PS | 60% | 2 | 1.1 |
| Lack of Training on Tools | DE | 80% | 3 | 1.2 |
| Technology will not meet expectations | TE | 40% | 1 | 1.3 |
| Lack of Testing on Mobile Phones | DE | 60% | 2 | 1.4 |
| Predicting wrong Output | TE | 20% | 2 | 1.5 |
| End users resist system | BU | 70% | 3 | 1.6 |
| Computer Crash | TE | 70% | 1 | 1.7 |
| Website Hacked | TE | 40% | 1 | 1.8 |

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK INFORMATION SHEET** | | | |
| Risk ID: 1.5 | Date: 25/03/2020 | Probability: 20% | Impact: 2 |
| **Description:**  There is good amount of probability that the training algorithm used for machine learning can predict wrong output and which has to be taken care of. | | | |
| **Refinement/Context:**  The website is made to predict if the message is spam or not and if the prediction is wrong then there is no use of using this website as a preventive measure to stay away from cybercrimes. | | | |
| **Mitigation/Monitoring:**  1.Prepare better algorithm for training the machine learning model.  2.Monitor the predictions of the website and try to understand if the prediction is correct as per human thinking of a cyber security expert. | | | |
| **Management/contingency plan/trigger:**  Get a new training algorithm for the website so the users get better predictions. | | | |
| **Current status:**  29/03/2020: Website is being monitored for predictions | | | |
| Originator: Harsh Oza | | Assigned: Shelton Pinto | |

|  |  |  |  |
| --- | --- | --- | --- |
| **RISK INFORMATION SHEET** | | | |
| Risk ID: 1.8 | Date: 25/03/2020 | Probability: 40% | Impact: 1 |
| **Description:**  Every software built is viable of being hacked, so to handle this risk some precautions are already take into consideration. | | | |
| **Refinement/Context:**  The website has user credentials stored, if the website is hacked there is a probability of data leaks. | | | |
| **Mitigation/Monitoring:**  1.Contact third-party network professionals for penetration testing.  2.Build proper hashed user credentials to be safe from normal brute-force attacks. | | | |
| **Management/contingency plan/trigger:**  Shut Down the website if found being hacked to prevent the data leaks | | | |
| **Current status:**  29/03/2020: All steps completed | | | |
| Originator: Harsh Oza | | Assigned: Darrel Noronha | |

**CONCLUSION:**

From this experiment, we learn about risk analysis in software engineering.We understood the concept of risk tablea amd risk information sheet(RIS) where in risk table we will list all the potential risks of the software with category of the risk, probability,impact of the risk and RMMM number. Risk information Sheet will have the Context, mitigation, monitoring, management plans of RMMM is that risk occurs.We implemented the same for our project software.