*Software Risk and Software Risk Management*

*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 software development process is called a software risk. 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.*

1. *Internal risk*

*Example: One of the team members is no longer able to contribute to the product.*

*Tip for risk management: In software development, it is important to organize work so that each team member is aware of all tasks, including those of colleagues. This allows one developer to substitute for another.*

1. *External risk*

*Example: Changes in an external provider's policy in each country.*

*Risk management advice: Usually developers in the team evaluate the task of integrating with an external provider, considering potential risks, and consulting with the team that has previously done such integration. This approach lets to determine what might be problematic or pose a problem, as well as our options. Furthermore, if we know that something like that is possible, we focus on the worst-case scenario and plan our next steps in risk analysis.*

1. *Internal and external risks combined.*

*Example: Communication is linked to commitment, which is also an important aspect of software development. And it is multifaceted in this case because it affects everyone involved in the software development process – developers, designers, software testing team, product owners, stakeholders, and, of course, the client. There is a problem if there is a lack of commitment.*

*Risk management advice: A product owner's role is to support, engage, and assist the team and everyone involved in the digital product development process in any way possible. Close collaboration between developers, a UX/UI designer, the client, and stakeholders must be an integral part of any successful digital product.*

***Risk management in software engineering*** *–*

*Risk analysis and management is the process of identifying, addressing, and eliminating potential problems before they have a negative impact on the project.*

*The following tasks are included in risk management:*

* *Determine the risks and the factors that cause them.*
* *All risks should be classified and prioritized.*
* *Create a plan that connects each risk to a mitigation strategy.*
* *Throughout the project, keep an eye out for risk triggers.*
* *If a risk occurs, take the appropriate mitigation measures.*
* *Throughout the project, communicate the status of risks.*

***Risk management is carried out to****:*

* *Identify the risk.*
* *Reduce the impact of risk.*
* *Reduce the probability or likelihood of risk.*
* *Risk monitoring.*

*A project manager has to deal with risks arising from three possible cases:*

* ***Known knowns -*** *are software risks that are facts known to the team as well as to the entire project. For example, not having enough number of developers can delay the project delivery.*
* ***Known unknowns*** *- are risks that the project team is aware of, but it is unknown that such risk exists in the project or not. For example if the communication with the client is not of good level then it is not possible to capture the requirement properly. This is a fact known to the project team however whether the client has communicated all the information properly or not is unknown to the project.*
* ***Unknown Unknowns*** *- are those kind of risks about which the organization has no idea. Such risks are generally related to technology such as working with technologies or tools that you have no idea about because your client wants you to work that way suddenly exposes you to absolutely unknown unknown.*

***Principles of Risk Management in Software Engineering***

* *Global Perspective: In this step of project management, we will go over the overall system description, design, and implementation. We consider the risk and its potential consequences.*
* *Keep an eye on the future: Consider the threat that might appear in the future and make plans to direct the next events.*
* *Open Communication: This allows for the free flow of information between the client and the team members, allowing them to be confident about the risks.*
* *Integrated management: Risk management is integrated into project management in this method.*
* *Continuous process: The risks are tracked constantly throughout the risk management paradigm during this phase.*

*Steps of Risk Management –*

* *Risk Identification - Risk identification entails brainstorming. It also entails the creation of a risk list. Brainstorming is a group discussion technique in which the whole project management is present. Study the project plan properly and check for all the possible areas that are vulnerable to some or the other type of risks. The best ways of analysing a project plan are by converting it to a flowchart and examine all essential areas. In this phase of Risk management, you have to define processes that are important for risk identification.*
* *Risk Assessment and Prioritization*

*It is a procedure within project management that includes the following steps:*

* + - *Identifying the issues that are causing risk in projects.*
    - *Determining the likelihood of a problem occurring.*
    - *Determining the problem's impact.*
    - *Assigning probability and impact values ranging from 1 to 10.*
    - *Determining the risk exposure factor.*
    - *The project manager should make a table with all of the values and rank the risks according to the risk exposure factor.*
* *Software Risk Analysis - Software Risk analysis is a very important aspect of risk management. In this phase the risk is identified and then categorized. After the categorization of risk, the level, likelihood (percentage) and impact of the risk is analyzed. Likelihood is defined after examining what are the chances of risk to occur due to various technical conditions. These technical conditions can be:*
  + - *Complexity of the technology*
    - *Technical knowledge possessed by the testing team.*
    - *Conflicts within the team*
    - *Teams being distributed over a large geographical area.*
    - *Usage of poor-quality testing tools.*
  + *Risk Avoidance and Mitigation - The goal of this technique is to eliminate the occurrence of risks entirely. To avoid risks, reduce the scope of projects by eliminating non-essential requirements. Risk avoidance involves identifying potential risks and then eliminating them as much as possible, or reducing their impact if they cannot be eliminated.*

*Examples of risk avoidance include:*

* + - *Not using certain features in the software due to the potential for bugs or other problems to occur.*
    - *Increase software testing activities using test cases to ensure no bugs exist in a product before it goes live.*
    - *Making sure that any changes made to software are thoroughly tested before they are deployed.*
  + *Risk transfer -*

*This technique is used in software engineering to reduce the risk of a project. Risk transfer is usually used when the scope of a project is too large for any one team to handle, and there is no way to split up the work so that each team can be responsible for its own piece of it. In this case, you have to find an outside company that can take on some portion of your project.*

*For example, if you're working on a video editor app and your team doesn't have enough designers or programmers to make it happen, project management could decide to hire someone else who does have the necessary resources. That way, you don't have to worry about handling all parts of the app yourself and can focus on what's most important--making sure that everything comes together in an enjoyable way!*

*Risk acceptance*

*In software engineering risk acceptance is a technique that involves taking on risks in order to complete the system. It can be a good idea if there is a lot of uncertainty about which features will be required and when they'll be needed. In this case, it makes sense to accept some level of risk in order to have time to figure out what needs to be done and how long it will take. The only way to know whether this will work is by trying it out—you may find that you were right all along, or you may discover that you need more time than expected.*

*6. Risk Monitoring*

*The risk should be continuously monitored by reevaluating the risks, the impact of the risk, and the probability of the risk occurring.*

*This guarantees that:*

* *The dangers have been discovered and reduced.*
* *The magnitude and impact of risk are assessed.*