Risk Management

Ashima Tyagi
Assistant Professor
School of Computer Science & Engineering

Outline

- Risk Management
- Types
- Process
- Risk Analysis and Assessment
- Risk Strategies
- Risk Monitoring and Control
- Risk Response and Evaluation

Risk Management

A risk is a probable problem; it might happen, or it might not. There are main two characteristics of risk.

- **Uncertainty:** the risk may or may not happen which means there are no 100% risks.
- **Loss:** If the risk occurs in reality, undesirable results or losses will occur.

What is Risk Management?

Risk Management is a systematic process of recognizing, evaluating, and handling threats or risks that have an effect on the finances, capital, and overall operations of an organization.

These risks can come from different areas, such as financial instability, legal issues, errors in strategic planning, accidents, and natural disasters.

The main goal of risk management is to predict possible risks and find solutions to deal with them successfully.

IMPORTANCE

Risk management is important because it helps organizations to prepare for unexpected circumstances that can vary from small issues to major crises.

By actively understanding, evaluating, and planning for potential risks, organizations can protect their financial health, continued operation, and overall survival.

Let's Understand why risk management important with an example.

Suppose In a software development project, one of the key developers unexpectedly falls ill and is unable to contribute to the product for an extended period.

One of the solution that organization may have , The team uses collaborative tools and procedures, such as shared work boards or project management software, to make sure that each member of the team is aware of all tasks and responsibilities, including those of their teammates.

An organization must focus on providing resources to minimize the negative effects of possible events and maximize positive results in order to reduce risk effectively.

Organizations can more effectively identify, assess, and mitigate major risks by implementing a consistent, systematic, and integrated approach to risk management.

Types of Risk

There are mainly 3 classes of risks that may affect a computer code project:

1. Project Risks
2. Technical Risks
3. Business Risks

1. Project Risks:

Project risks concern various sorts of monetary funds, schedules, personnel, resources, and customer-related issues. A vital project risk is schedule slippage. Since computer code is intangible, it's tough to observe and manage a computer code project. It's tough to manage one thing that can not be seen. For any producing project, like producing cars, the project manager will see the merchandise taking form.

For example, see that the engine is fitted, at the moment the area of the door unit is fitted, the automotive is being painted, etc. so he will simply assess the progress of the work and manage it. The physical property of the merchandise being developed is a vital reason why several computer codes come to suffer from the danger of schedule slippage.

2. Technical Risks:

Technical risks concern potential style, implementation, interfacing, testing, and maintenance issues. Technical risks conjointly embody ambiguous specifications, incomplete specifications, dynamic specifications, technical uncertainty, and technical degeneration. Most technical risks occur thanks to the event team's lean information concerning the project.

3. Business Risks:

This type of risk embodies the risks of building a superb product that nobody needs, losing monetary funds or personal commitments, etc.

Classification of Risk in a project

Example: Let us consider a satellite-based mobile communication project. The project manager can identify many risks in this project. Let us classify them appropriately.

- What if the project cost escalates and overshoots what was estimated? – **Project Risk**
- What if the mobile phones that are developed become too bulky to conveniently carry? **Business Risk**
- What if call hand-off between satellites becomes too difficult to implement? **Technical Risk**

Risk Management Process

Risk management is a sequence of steps that help a software team to understand, analyze, and manage uncertainty.

Risk management process consists of

Risks Identification.

Risk Assessment.

Risks Planning.

Risk Monitoring

Risk Identification

Risk identification refers to the systematic process of recognizing and evaluating potential threats or hazards that could negatively impact an organization, its operations, or its workforce. This involves identifying various types of risks, ranging from IT security threats like viruses and phishing attacks to unforeseen events such as equipment failures and extreme weather conditions.

Risk analysis

Risk analysis is the process of evaluating and understanding the potential impact and likelihood of identified risks on an organization. It helps determine how serious a risk is and how to best manage or mitigate it. Risk Analysis involves evaluating each risk's probability and potential consequences to prioritize and manage them effectively.

Risk Planning

Risk planning involves developing strategies and actions to manage and mitigate identified risks effectively. It outlines how to respond to potential risks, including prevention, mitigation, and contingency measures, to protect the organization's objectives and assets.

Risk Monitoring

Risk monitoring involves continuously tracking and overseeing identified risks to assess their status, changes, and effectiveness of mitigation strategies. It ensures that risks are regularly reviewed and managed to maintain alignment with organizational objectives and adapt to new developments or challenges.

Risk Assessment

- Risk assessment is a systematic process of evaluating potential risks that may be involved in a projected activity, undertaking, or business decision.
- It aims to identify, analyze, and evaluate the likelihood and impact of risks to determine appropriate measures to mitigate or manage them effectively.
- A broader process that includes **risk analysis** and adds **risk evaluation**.
- **Risk analysis:** Think of it as the "*What could go wrong?*" phase.
- **Risk assessment:** Think of it as "*Should we be worried, and what should we do about it?*"

Objective of Risk Assessment

The objective of Risk Assessment is to rank the risks in terms of their harm inflicting potential. For risk assessment, initial every risk ought to be rated in 2 ways:

- The chance of a risk coming back true (denoted as r).
- The consequence of the issues related to that risk (denoted as s).

Based on these 2 factors, the priority of every risk is computed:

$$p=r*s$$

Where p is the priority with which the danger should be handled, r is the likelihood of the danger changing into true, and s is the severity of harm caused by the danger changing into true. If all known risks are prioritized, then the foremost probably and damaging risks are handled initial and a lot of comprehensive risk abatement procedures are designed for these risks.

Risk Assessment Steps

The risk assessment process typically involves several key steps to ensure that risks are properly identified, evaluated, and managed:

- **Identify Risks:** The first step is to identify potential risks that could affect the project or organization. This involves gathering information from various sources, such as stakeholder input, historical data, and expert opinions, to recognize possible threats or vulnerabilities.
- **Analyze Risks:** Once risks are identified, they are analyzed to determine their potential impact and likelihood. This step involves evaluating how these risks could affect objectives and what the consequences might be. The analysis helps in understanding the severity and urgency of each risk.
- **Evaluate Risks:** In this step, risks are prioritized based on their potential impact and likelihood. This evaluation helps to determine which risks are the most significant and need immediate attention. It often involves comparing risks to established criteria or benchmarks.
- **Mitigate Risks:** After evaluating risks, strategies are developed to manage or mitigate them. This can include avoiding the risk, reducing its impact, transferring it to another party, or accepting it if it is within acceptable limits.
- **Monitor and Review:** The final step involves continuously monitoring risks and reviewing the effectiveness of the mitigation strategies. This ensures that risk management efforts remain relevant and effective as conditions change.

How to Use a Risk Assessment Matrix

A risk assessment matrix is a tool used to evaluate and prioritize risks based on their likelihood and impact. It is typically represented as a grid, where the x-axis represents the probability of a risk occurring, and the y-axis represents the potential impact of the risk.

How to Use It:

- **Plot Risks:** Identify and plot each risk on the matrix according to its likelihood and impact.
- **Categorize Risks:** Risks are categorized into different levels, such as low, medium, or high, based on their position on the matrix.
- **Prioritize Actions:** The matrix helps prioritize which risks require immediate attention and which can be monitored over time. High likelihood and high impact risks are addressed first, while low likelihood and low impact risks may require less urgent responses.

Risk Analysis

- Software risk analysis in Software Development involves identifying which application risks should be tested first.
- Risk is the possible loss or harm that an organization might face.
- Risk can include issues like project management, technical challenges, resource constraints, changes in requirements, and more
- **Finding every possible risk and estimating are the two goals of risk analysis.**
- Think about the potential consequences of testing your software and how it could impact your software when creating a test plan.
- Risk detection during the production phase might be costly.
- Therefore, risk analysis in testing is the best way to figure out what goes wrong before going into production.

Types of risk analysis

In risk management, you can perform two types of risk analysis:

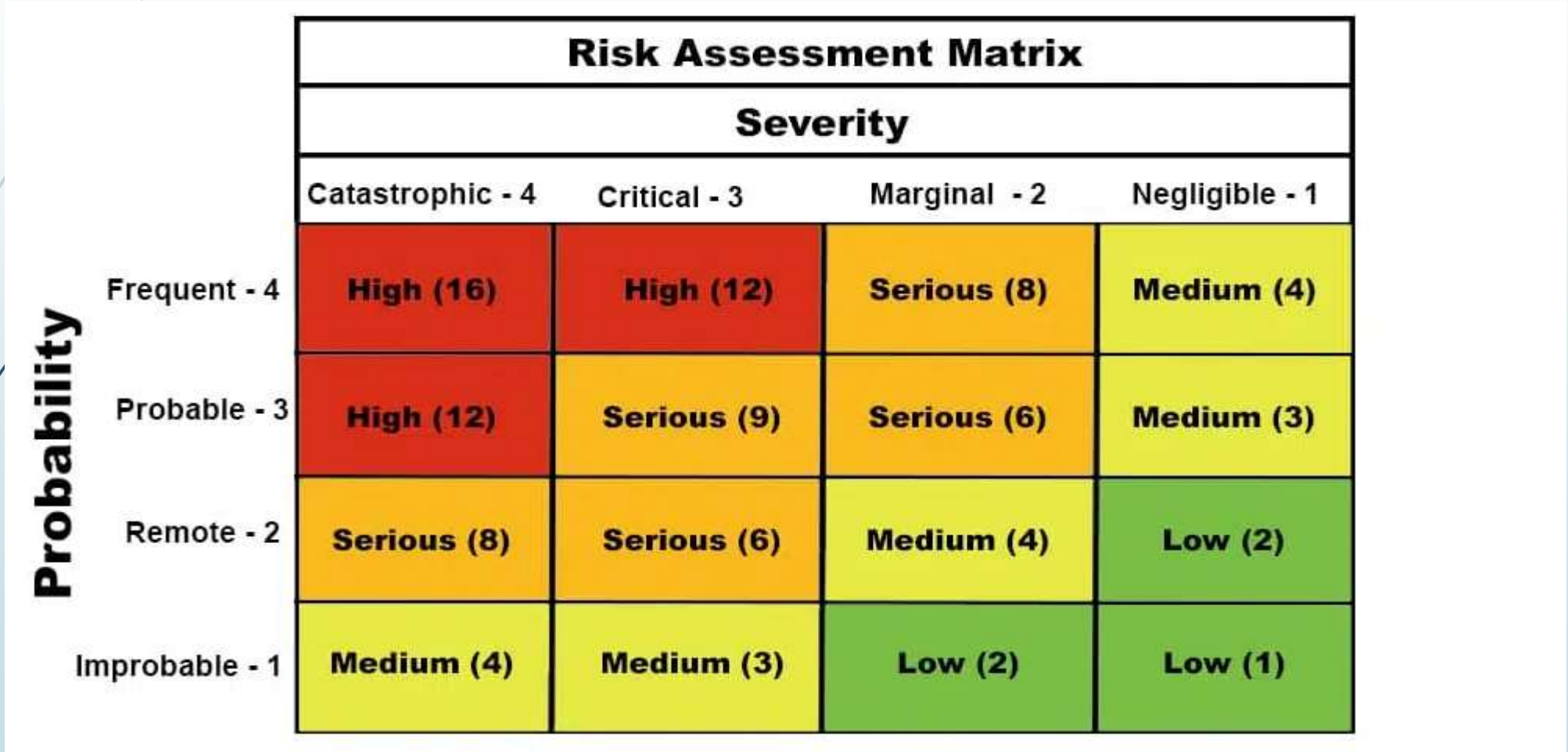
Qualitative Risk Analysis

Quantitative Risk Analysis

1. Qualitative Risk Analysis:

- In qualitative risk analysis, you will examine risks for severity and likelihood of occurrence during the project.
- Afterward, you will find the risk ratings using **the risk assessment matrix**. The risk rating can be high, serious, medium, and low.
- The risk assessment matrix is a great communication tool to communicate the risk information to stakeholders to decide on the next action.

As shown below, you will order the risks on a risk assessment matrix.



Risk Assessment Matrix				
	Severity			
Probability	Catastrophic - 4	Critical - 3	Marginal - 2	Negligible - 1
Frequent - 4	High (16)	High (12)	Serious (8)	Medium (4)
Probable - 3	High (12)	Serious (9)	Serious (6)	Medium (3)
Remote - 2	Serious (8)	Serious (6)	Medium (4)	Low (2)
Improbable - 1	Medium (4)	Medium (3)	Low (2)	Low (1)

To provide a better understanding, let's take a look at the below risk register that is created during identify risks process. This risk register includes both positive and negative risks.

Risk ID	Risk Description	Probability	Impact	Risk Score
01	Insufficient Amount of Coders	2	4	8
02	Delayed Delivery	2	2	4
03	Need for Advanced Testing to Eliminate Defects	3	5	15
04	Reuse of Existing Testing System	4	5	20

As shown in the table above, in qualitative risk analysis, probability and impact values are determined for each risk and the risk score is calculated by multiplying them. Depending on the risk scores, you prioritize each risk and establish risk response strategies for both positive and negative risks if the score exceeds risk tolerance limits.

2. Quantitative Risk Analysis:

- After performing a qualitative risk analysis, the quantitative risk analysis process is carried out. Organizations utilize this procedure for significant and complicated initiatives since it demands resources and time.
- Calculating risk using objective data is known as quantitative risk analysis.
- During this process, you will use verifiable data to examine the potential impact of risks on your project objectives, such as schedule baseline, cost baseline, scope baseline, etc.

In the below table, we will perform quantitative risk analysis by assigning monetary values for the impact of each risk and percentages for their probability of occurrence.

Risk ID	Risk Description	Probability	Impact	Expected Monetary Value (EMV)
01	Insufficient Amount of Coders	40%	$30.000	$12.000
02	Delayed Delivery	40%	$40.000	$16.000
03	Need of Advanced Testing to Eliminate Defects	60%	$25.000	$15.000
04	Reuse of Existing Testing System	80%	$45.000	$36.000

Qualitative Risk Analysis	Quantitative Risk Analysis
Risk level	Project level
Easy to perform	Time-consuming
Does not require a software tool	Software tools facilitate the process
Subjective evaluation of probability and impact	Objective/numeric evaluation of probability and impact
Should be done first	Should be done after performing qualitative analysis
Analyzes the effects of individual project risks	Analyzes the combined effects of risks as a whole to specify an overall project risk.
Useful in all-size projects	Useful in especially in large and sophisticated projects
Risk scale and scores are qualitative	Risk scale and scores are quantitative -often specified in monetary and duration terms
Not Applicable	Determines the amount of Contingency Reserve
Provides quick information	Provides detailed information

Risk Strategies

- Risk strategies define how you will handle a risk once it is identified and assessed. They are part of the Risk Response Planning phase in Risk Management.

Risk Management Strategies:

- Risk Avoidance
- Risk Reduction
- Risk Sharing
- Risk Transfer
- Contingency Planning

1. Risk Avoidance

- Risk Avoidance is one of the simplest risk management strategies.
- It involves completely avoiding activities that could lead to risk.
- For example, a business might decide not to enter a highly volatile foreign market to avoid the risk of financial loss.
- The main advantage of risk avoidance is that it eliminates the possibility of facing negative outcomes from the avoided activities.
- However, this strategy also means missing out on potential opportunities that taking the risk might have provided.

When to use it?

The best time to use risk avoidance is when the potential risks far outweigh the expected benefits.

It's particularly useful when the consequences of a risk could be catastrophic to the business or project.

Although risk avoidance can seem like a conservative approach, it's a prudent choice when dealing with risks that can have severe legal, financial, or health-related repercussions.

Pros:

Completely eliminates specific risks.

Reduces uncertainties and potential costs.

Cons:

Limits opportunities for growth or profit.

Can lead to stagnation if overused.

Example:

A tech company might avoid storing sensitive user data to circumvent the risks associated with data breaches and the resultant legal consequences.

2. Risk Reduction

Example: A construction company using high-quality materials and strict safety protocols to reduce the risk of structural failures and worker injuries.

3. Risk Sharing

- Risk Sharing is a collaborative tactic among risk management strategies where risk is distributed among multiple parties.
- By sharing risks, for instance through partnerships or outsourcing, companies can leverage external expertise and reduce their own exposure to potential losses.
- This is common in projects that are too large or complex for a single entity to manage alone.

When to use it?

- The strategy is particularly effective when engaging in new or innovative projects where the risks are high and uncertain. It is a smart choice for businesses that need to mitigate potential financial losses or when specialized knowledge is required to manage specific risks.

Pros:

Spreads and mitigates risks across parties.

Leverages collective resources and expertise.

Cons:

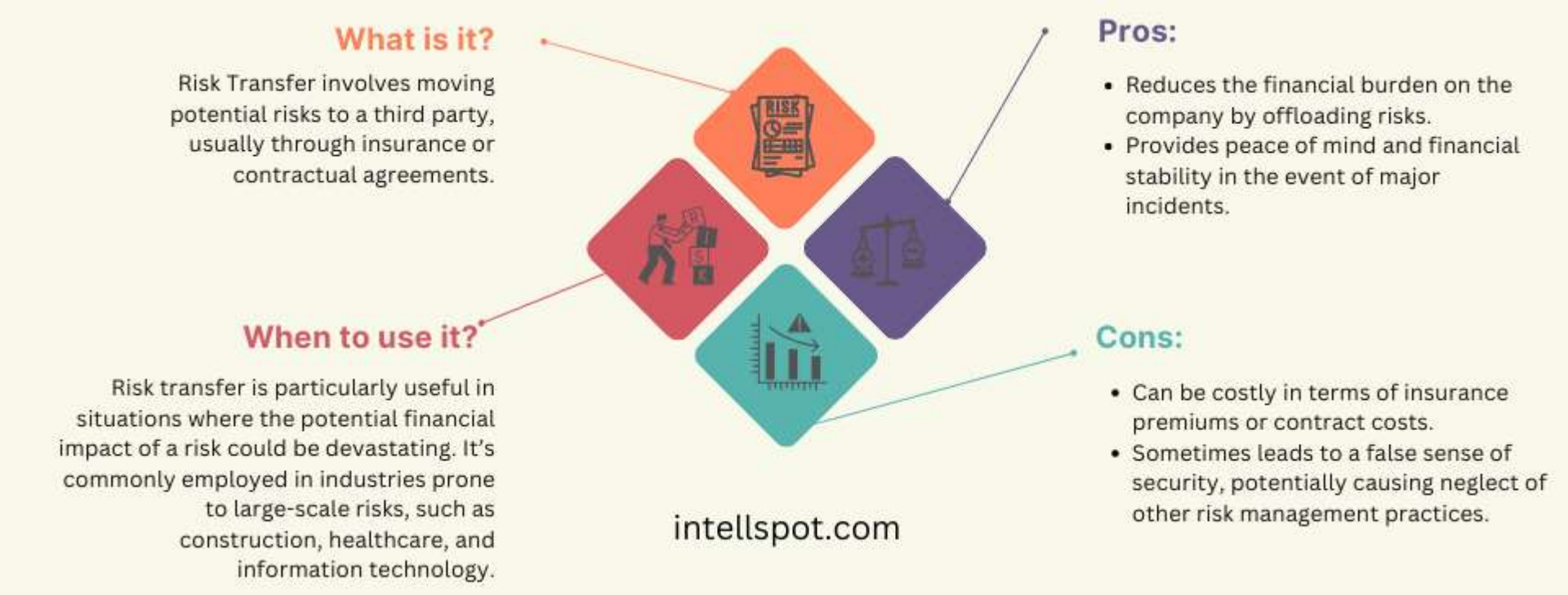
Can lead to dependencies on other parties.

May result in reduced control over project outcomes.

Example:

A small tech firm partnering with a larger company to co-develop a new software product, sharing the financial risks involved in its development and market introduction.

4. Risk Transfer



Example:

A tech startup might use a cloud service provider to host data, thereby transferring the risk of data center management and potential downtime to the provider.

5. Contingency Planning

- Contingency Planning involves preparing alternative action plans that can be implemented if initial plans fail due to unforeseen risks.
- This strategy is about readiness and flexibility, ensuring that a business can continue operations under various scenarios.
- It often includes developing detailed recovery plans, backup operations, and maintaining reserves of essential resources.

When to use it?

Contingency planning is crucial for businesses in environments where sudden changes can occur, such as natural disasters, economic instability, or technology failures. It allows organizations to react quickly and effectively, minimizing downtime and operational losses.

Pros:

- Enhances organizational resilience against unexpected events.
- Helps maintain business continuity during crises.

Cons:

- Requires significant time and resources to develop effective contingency plans.
- May not be used if no crisis occurs, leading some to view resources spent on contingency planning as non-productive.

Example:

- A bank might have contingency plans for IT system failures that include manual transaction processing methods and secondary data centers to ensure continuous customer service.

Risk Monitoring and Control

Risk monitoring and control begins at the start of projects when all potential and known risks are identified, and then just as importantly, continues throughout a project as those initial risks are continuously tracked while new risks are also identified as work continues, changes and progress.

Activity	Description
Reviewing risk triggers	Check for early signs that a risk may occur.
Tracking residual risks	Monitor risks that remain after mitigation.
Reassessing risks	Regularly re-analyze and re-prioritize risks.
Identifying new risks	Watch for emerging risks throughout the project.
Evaluating risk response	Assess whether mitigation or contingency plans are working.
Updating the Risk Register	Log changes in status, ownership, or strategies.
Communicating risk status	Share updates with stakeholders and project team.

Tools for Monitoring and Controlling Project Risks

•**Risk Assessment:** It involves checking for the past identified risks and new risks, and generating risk responses.

•**Risk Audits:** The effectiveness of risk responses applied should be documented. These documents are needed in scheduled meetings to discuss the project's progress.

•**Variance and Trend Analysis:** The performance of the project in terms of the risks incurred, responses taken instead of that, the progress of the project, etc. should be monitored. This analysis helps in predicting the output of the project in the future.

•**Technical Performance Measurement:** Technical aspects of the project should be measured by testing the achievement of the project till that time. It determines the technical success of the project.

•**Reserve Analysis:** Reserves of the risk should be analyzed for deciding on their adequacy in the complete project tenure.

•**Status Meetings:** Regular team meetings should be conducted for all the issues and achievements of the project.

Outputs for Monitoring and Controlling Project Risks

•**Work Performance Information:** It includes a record of risks occurring in the project throughout the term and whether a response is needed for the same or they can be ignored. It also includes schedule progress, deliverables status, costing, the requirement of resources, etc.

•**Organizational Process Assets Updates:** They involve templates for risk planning, risk breakdown structure, and lessons learned from previous issues and errors.

•**Change Requests:** They involve modifications in the project plan as per the need, such as adding the extra budget, extending the schedule, including more resources, etc. for dealing with emergency purposes.

Risk Response and Evaluation

Risk response planning is the final step in the risk management process. In this process, risk responses are developed. The risk response can be drawn based on three categories of risks, viz. controllable known risks, uncontrollable known risks, and unknown risks. While risk responses can be developed for known risks, no response can be developed for unknown risks.

Now let us study how a risk response is created for controllable and uncontrollable known risks.

- Controllable Known Risks
- Uncontrollable Known Risks

Controllable Known Risks

Risk response for controllable known risks involves risk prevention. Risk prevention can be achieved in two ways, which are:

Risk Avoidance

As the name suggests, the risk avoidance approach is all about eliminating risks and not taking them at all. The simplest way of avoiding a risky project is not to take that project.

Risk Mitigation

It involves taking measures for reducing the probability of the occurrence of a risk and its impact on the overall project. It is not meant to eliminate the risk, but to reduce the risk exposure. Providing safety training and safety gear to construction workers on a site is for mitigating the risk of injury or accident. It does not eliminate the risk, but it certainly reduces the probability or impact of risk. Similarly, some risks are not mitigated within a project but are transferred to others.

Uncontrollable Known Risks

Risk response for uncontrollable known risks involves reactive response after a risk event has occurred. It may be done through contingency planning, where a contingency budget is set aside to take care of the risk event.

- For example, assume that 2% of the inventory will get damaged, destroyed, or stolen and will have to be purchased again. However, the budget for the additional 2% inventory can be set aside as a contingency budget if, in case, the inventory damage exceeds the quantity already factored in.
- The other possibility, concerning dealing with effects, is that you may simply “accept” the risk if it occurs and not respond. It can be for two extreme reasons:

❑ If the loss in case of a risk event is too trivial, you may not want to respond to such a risk since planning the response for it might be costlier.

❑ If the loss in case of a risk event is massive and beyond control, the only option is to “accept” the risk.

Several risk response strategies are being developed in the planning process and the one best suited for the risk applied at that time to deal with risks.

The risk response actions are based on the 4Ts:

•**Terminate**: Risk termination is done by changing the project plan to terminate the impact of risk on the project. If the termination of the risk is not possible, it may be avoided by taking pre-emptive actions.

•**Treat**: Treatment involves reducing the probability of risk by taking actions in advance at an early stage. it may require extra resources, an extra schedule, and modification in a plan to minimize risks.

•**Tolerate**: Tolerance doesn't ask for any changes in the project plan. Risks are borne as no strategies can be applied to that.

•**Transfer**: A third party is hired to deal with the risk and therefore, the project risk is transferred to them

Thank You