Risk [week-4 theory]

Risk

- 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.
- Risk is a measure of the potential inability to achieve overall program objectives within defined cost, schedule and technical constraints.

Risk Management

- Risk management is defined as the process of identifying, monitoring and managing potential risks in order to minimize the negative impact they may have on an organization.
- Examples of potential risks include security breaches, data loss, cyberattacks, system failures and natural disasters.
- Risk Management is the system of identifying addressing and eliminating these problems before they can damage the project.

Characteristics of risk

1) **Situational:** Changes in a situation can result in new risks. Such changes include replacing a team member, undergoing a reorganization, changing the scope of the project.

2) **Time-based:** In this case, the probability of the risk occurring at the beginning of the project is very high (due to the unknown factor), and diminishes along as the project progresses. In contrast, the impact (cost) from a risk occurring is low at the beginning and higher at the end.

3) **Interdependence:** Within a project, many tasks and deliverables are interdependent on each other. These delays in these tasks will have a cascading effect on the other related tasks, and the result could be a domino effect.

4) **Magnitude Dependent:** The relationship between probability and impact is not linear in this case, and the magnitude of the risk makes a lot of difference.
For example, consider the risk of spending $1 for a 50/50 chance to win $5 versus the risk of spending $1000 for a 50/50 chance of winning $5000. Since the probability of loss is the same in both cases (50%), the opportunity cost of losing is much greater in the latter case.

5) **Value-Based:** The risk may be affected by personal, corporate or cultural values. For example, completing a project on schedule may be dependent on the time of the year and the nationalities or religious beliefs of the work team. Projects being done in international locations where multiple cultures are involved may have a higher risk than those done in a single location with a similar kind of workforce.

Categories of risk

There are 3 main categories of risk:

1. **Project risk**
   - If the project risk is real then it is probable that the project schedule will slip and the cost of the project will increase.
   - It identifies the potential schedule, resource, stakeholders and the requirements problems and their impact on a software project.

2. **Technical risk**
   - If the technical risk is real then the implementation becomes impossible.
   - It identifies potential design, interface, verification and maintenance of the problem.

3. **Business risk**
   - If the business risk is real then it harms the project or product.

There are 5 sub-categories of the business risk:

1. **Market risk**
   - Creating an excellent system that no one really wants.
2. **Strategic risk**
   - Creating a product which no longer fit into the overall business strategy for companies.
3. **Sales risk**
   - The sales force does not understand how to sell a creating product.
4. **Management risk**
   - Loose a support of senior management because of a change in focus.
5. **Budget risk**
   - losing a personal commitment.

Other risk categories

1. **Known risks**
   - These risks are unwrapped after the project plan is evaluated.
2. **Predictable risks**
   - These risks are estimated from previous project experience.
3. **Unpredictable risks**
   - These risks are unknown and are extremely tough to identify in advance.

Why risk management is critical?

- Critical risks are defined as: **"threats or hazards that pose the most strategically signification risk"** because of their probability of occurrence and consequence.
- These can include earthquakes, industrial accidents, terrorist attacks, pandemics, illicit trade and organized crime.

Other risks:

- ✓ Failure to use appropriate risk metrics
- ✓ Mismeasurement of known risks

- ✓ Failure to take known risks into account
- ✓ Failure in communicating risks to top management
- ✓ Failure in monitoring and managing risks

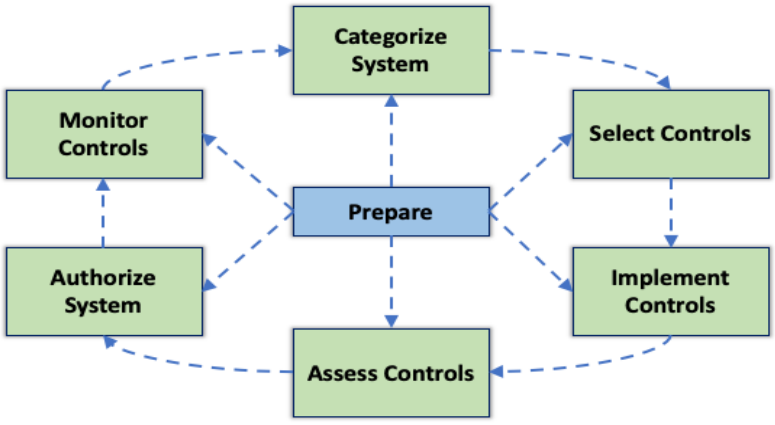
1) A lack of risk decision making structure and lack of accountability for risk decisions in an organization.
   For example, a project manager may accept a large information security risk that can lead to compliance and reputational issues simply because they only thing they get incentivized on is getting the new product out the door. However, the executive in charge of the business unit, accountable for sustained results may make a very different decision.

2) The lack of meaningful risk assessment process. In terms of risk assessment effectiveness, organizations who take a control-based approach to risk assessment are often missing the business context required to make the right decisions.
   A true, goals-based risk management strategy facilitates a more effective allocation or risk mitigation resources and sometimes even saves money!

3) A lack of an open, risk -ware culture. In order to build a culture where business managers are willing to be transparent to their executives, the executives have to be careful to craft the kind of culture that fosters this transparency.

Risk Management Framework

- The Risk Management Framework is a template and guideline used by companies to identify, eliminate and minimize risks.
- It was originally developed by the National Institute of Standards and Technology to help protect the information systems of the United States government.



The RMF steps include:

1) Prepare to execute the RMF by establishing a context and priorities for managing security and privacy risk at organizational and system levels.

2) Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.

3) Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as

needed based on an organizational assessment of risk and local conditions. If any overlays apply to the system they will be added in this step.

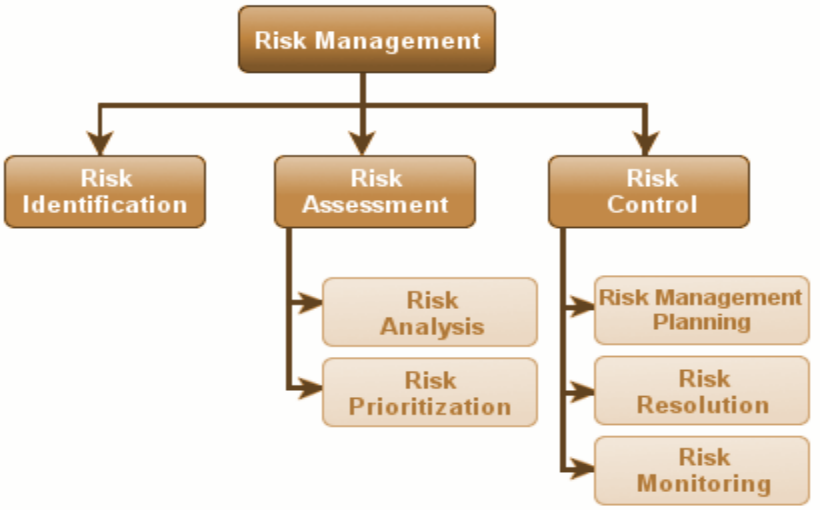
4) **Implement** the security controls identified in step 2.

5) **Assess** a third party assesses the controls and verifies that the controls are properly applied to the system.

6) **Authorize** the information system is granted or denied an Authorization to Operate (ATO), in some cases it may be postponed while certain items are fixed. The ATO is based on the report from the Assessment phase. ATO is typically granted up to 3 years and the process needs to be repeated at the end of the period.

7) **Monitor** the security controls in the information system continuously in a pre-planned fashion as documented earlier in the process.

Risk Management Activities



Risk Management

In the field of software engineering, risk management is a methodology or a mechanism, carried out throughout the development process to identify, manage and control risks evolved before and during the development process.

Basically, three types of activities are covered under the risk management process.

- ✓ Risk Identification.
- ✓ Risk Analysis.
- ✓ Risk Control.

1. Risk Identification

It is the first step of a risk management process, which involves the identification of potential risks that may affect a software product or a development project, and accordingly documenting them along with their characteristics.

It is a constant process, which is carried out throughout the development due to the fact that as the development process progresses, the more we get to know about the software product and based on it, we may able to explore and identify more unvisited or hidden risks.

Generally, this phase helps in identifying the two types of risks, product risk and project risk.

1) Product risk

Risks pertaining to a software product or application, which may arise, due to its inefficiency, to function, desirably, to meet the expectation of the users.

2) Project risk

These risks involve any sort of uncertain or unexpected event or action, which may likely to occur and degrade the progress of a project.

In this phase, usually client, stakeholders, business manager, project manager and test manager, collaborate and participates in brainstorming or small sessions, study and analyse the project documentation plan, etc., to make out the probable list of risks associated with the software development.

Some commonly known techniques to identify risks may include risk templates, project retrospective, Failure Mode and Effect Analysis (FMEA), Failure Mode Effect and Criticality Analysis (FMECA), etc.

2. Risk Assessment

The next stage of a risk management process is risk analysis, which involves the assessment of the risks identified during the risk identification stage.

1) Risk Analysis

This stage usually involves the analysis and prioritization of the risks, i.e., possible outcomes of each identified risk is being assessed based on which risks are categorized and accordingly, prioritized.

2) Risk Prioritization

Based on the degree of impact, possessed by each risk, they are being assigned severity levels, namely ‘High’, ‘Medium’ and ‘low’. And based on their severity, they are prioritizing i.e., High risks are considered as top priority whereas the low risk is regarded for the bottom most priority.

3. Risk Control

During this stage, risks are managed, controlled and mitigated, based on their priority so as to achieve the desired results. It is generally divided into three activities which may be seen below.

1) Risk Management Planning

It involves a proper and effective plan to deal with the each identified risk.

2) Risk Resolution

It refers to the execution of the plans, outlined during the risk management planning stage so as to either remove or fix identified risks.

3) Risk Monitoring

It involves, regular monitoring and tracking, the development progress, in the direction, of resolving risk issues, which may include revaluation of the risks, their likelihood to occur, etc., and taking and implementing necessary & appropriate actions, wherever necessary.

Principles of risk management

1) **Maintain a global perspective -** View software risks in the context of a system and the business problem planned to solve.

2) **Take a forward-looking view -** Think about the risk which may occur in the future and create future plans for managing the future events.

3) **Encourage open communication -** Encourage all the stakeholders and users for suggesting risks at any time.

4) **Integrate -** A consideration of risk should be integrated into the software process.

5) **Emphasize a continuous process -** Modify the identified risk than the more information is known and add new risks as better insight is achieved.

6) **Develop a shared product vision -** If all the stakeholders share the same vision of the software, then it is easier for better risk identification.

7) **Encourage teamwork -** While conducting risk management activities pool the skills and experience of all stakeholders.

Risk Mitigation

- Risks are inevitable in business. Businesses must reduce their exposure to risks and find ways to mitigate them to remain competitive in business.
- Identification and acknowledgement of risks that affect the operations, profitability, security, or reputation of the business is the first step.
- Developing strategies to mitigate these risks is the next and the most essential step! Risk mitigation is an important step in risk management that includes identifying the risk, assessing the risk, and mitigating the risk.

Definition:

Risk mitigation can be defined as taking steps to reduce or minimize risks. When you devise a strategy for reducing prospective risks and working with an action plan, it is important that you choose a strategy that relates to your company's profile and nature of business.

Need and importance of risk mitigation

- A robust risk mitigation plan helps establish procedures to avoid risks, minimize risks, or reduce the impact of the risks on organizations.
- It guides organizations on how they can bear and control risks. This helps a business in achieving its objectives.
- The ability to understand and control risks makes an organization more confident and helps in making the right business decisions.
- It increases the stability of the organization and reduces its legal liability.
- It protects people involved and company from any potential harm.