Lecture 12

➔ (Week 12 - March 25, 2024)

Week 12: Risk Management and Analysis

Input to Risk Management Planning:

Enterprise Environmental Factors:

- Risk tolerance levels of the organization and stakeholders.
- Risk tolerance signifies the trade-off between benefits and costs.
- Stakeholders weigh benefits against potential losses when considering risks.
- Stakeholders avoid risks if the cost or impact outweighs the benefits.

Organizational Process Assets:

- Existing policies and guidelines defining risk tolerance.

Project Scope Statement:

- Contains crucial information for risk management planning:
    - Project deliverables
    - Project constraints
    - Project assumptions
    - Initial project organization
    - Initial defined risks
- Schedule milestones

Risk Management Planning: Tools & Outputs:

Tools for Risk Management Planning:

- Planning meetings: primary tool involving project manager, project management team, and relevant stakeholders.
- Analysis of project risks and alignment with organizational risk tolerance.

Outputs of Risk Management Planning:

- **Risk Management Plan:** Sole output from the risk management planning process.

Risk Management Plan Content:

Methodology:

- Procedures, methods, tools, and data sources for risk management.

Roles and Responsibilities:

- Identification of team members responsible for managing risks, including risk 'owners'.

Budgeting:

- Allocation of resources and estimation of costs for risk management and associated methods.

Timing:

- Frequency and timing of risk management processes.

Risk Categories:

- Development and review during planning; utilized in risk identification.

Probability and Impact Definitions:

- Detailed discussions in Qualitative Risk Analysis.

Probability and Impact Matrix:

- Detailed discussions in Qualitative Risk Analysis.

Revised Stakeholder Tolerances:

- Changes in stakeholder tolerance resulting from risk planning.

Reporting Formats:

- Describes content and format of risk register and project risk dictionary.

Tracking:

- Documentation of risk activity history and auditing of risk processes.

Risk Categories:

Organizational Risks:

- Resource conflicts due to concurrent projects within the organization.
- Unrealistic scope, time, and cost objectives concerning organizational resources or structure.
- Lack of project funding or diversion of funds to other projects.
- Changes in management oversight.
- Loss of project 'champion'.
- Project 'politics' impacting project dynamics.

External Risks:

- Changes in laws or regulations.
    - Example: Sarbanes-Oxley Act of 2002 necessitates compliance planning and implementation akin to a regular project.
    - Labor issues.
    - Weather-related challenges.
    - Changes in ownership affecting project dynamics.
    - Shifts in foreign policy impacting projects conducted abroad.
- Catastrophic risks (force majeure) beyond the scope of risk management planning, requiring disaster recovery strategies.
    - Examples include earthquakes, meteorites, volcanoes, hurricanes, floods, civil unrest, terrorism, etc.

Risk Breakdown Structure (RBS):

- A visual representation offering hierarchical decomposition of risk categories analogous to a Work Breakdown Structure (WBS).
- Divides risks into categories such as Project, Technical, Project Management, Organizational, and External.
- Provides a structured framework for understanding and managing risks across various dimensions of the project.

Risk Identification:

- Process of determining potential risks impacting the project and profiling them for effective mitigation and response planning.
- Iterative and incremental process involving continuous addition of new risks, elimination of non-risks, and refinement of existing risk profiles as the project progresses.

Where Risks are Found:

- Risks can be identified across various project aspects including budgets/funding, schedules, scope or requirement changes, project plan, management processes, technical issues, personnel matters, hardware, contracts, political and business concerns, legal and environmental factors.

Three Types of Software Risk:

Project Risks:

- Pose threats to the project plan, potentially causing schedule delays and cost overruns.
- Examples include budgetary/funding constraints, schedule issues, personnel challenges, resource limitations, changes in requirements, project complexity, hardware concerns, and environmental risks.

Technical Risks:

- Endanger the quality and timeliness of software deliverables.
- Encompass risks related to design, implementation, interfacing, verification, cutover, maintenance, and security.

Risk Identification: Tools and Techniques

Root Cause Analysis:

- Helps identify the underlying source of risks.
- Involves thorough analysis of identified risks to uncover potential underlying causes.

- Often, the apparent source of risk may not be the true root cause, requiring deeper investigation.

Checklist Analysis:

- Utilizes historical data and past project experiences.
- Risks are compiled into a checklist format.
- Starting point for the checklist can be the lowest level of the Risk Breakdown Structure (RBS).
- Recognizes that checklists cannot be exhaustive due to the uniqueness of each project.

Assumptions Analysis:

- Validates assumptions documented during project planning.
- Assumptions should be accurate, complete, and consistent.
- Assumptions are evaluated based on their strength or validity and potential consequences if they turn out to be false.
- False assumptions are reclassified as risks.

Diagramming Techniques:

- **Cause and Effect Diagram (Ishikawa or Fishbone Diagram):**
    - Illustrates the relationship between the effects of problems and their causes.
    - Depicts all potential causes and sub-causes of a problem along with the effect of proposed solutions.
- **System or Process Flowcharts:**
    - Shows logical steps required to achieve an objective.
    - Demonstrates how elements of a process or system relate to each other.
    - Depicts cause/response relationships.
- **Influence Diagrams:**
    - Primarily showcases causal influences among project variables.
    - May also depict event sequencing.
    - Visually represents risks, uncertainties, or impacts and their interdependencies.

Risk Item Checklist:

- Useful for identifying known and predictable risks across various subcategories:
    - Product size
    - Business impact
    - Customer characteristics
    - Process definition
    - Development environment
    - Technology to be built
    - Staff size and experience

Risk Data Quality Assessment:

- Low-quality data undermines the effectiveness of qualitative risk analysis.
- Assessment examines:
    - Quality, availability, and understanding of data used.
    - Reliability, integrity, and accuracy of data.
- Risk categorizations, such as those in the Risk Breakdown Structure (RBS), aid in identifying project phases and affected elements, facilitating risk assessment.

Risk Urgency Assessment:

- Prioritize risks based on urgency rather than addressing all simultaneously.
- Similar to rolling wave planning, assess when potential risks might occur.
- Develop response plans for imminent risks.
- Focus on actively managing the top ten risks for efficiency.
- Maintain a watch list for remaining risks, replacing those mitigated or resolved.

Outputs: Updates to the Risk Register:

- Update the risk register with:
    - Risk ranking and categorization.
    - Risks requiring immediate responses.
    - Risks for further analysis and response.
    - Watch list for low-priority risks.
    - Trends from qualitative risk analysis for response planning insights.

Risk Response Planning:

- Develops options to mitigate threats and exploit opportunities identified during risk analysis.
- Severity of the risk dictates the level of response planning.
- Responses should be cost-effective and timely.

Strategies for Negative Risks (Threats):

Avoidance:

- Evade or eliminate the risk event or its cause.
- Alter project plans to protect objectives.
- Most suitable in early project stages.
- Example: Eliminating the requirement to interface systems to avoid risks associated with integration complexity.

Risk Transfer:

- Shifts risk and consequences to a third party.
- Transfers responsibility for risk management.
- Effective for financial risks.
- Example: Using insurance to transfer financial risks associated with project activities to an insurance provider.

Strategies for Negative Risks or Threats:

Mitigation:

- Aims to reduce the probability or impact of a risk event to an acceptable level.
- Prioritizes early problem resolution, considering it less costly than addressing it later.
- Examples include performing additional tests, simplifying processes, conducting simulations, or selecting reliable vendors over cheaper alternatives.

Risk Acceptance:

- Acknowledges the risk without taking immediate action unless the risk materializes.
- Suitable when addressing a specific risk is impractical or cost-prohibitive.
- Passive acceptance involves documentation only, while active acceptance involves establishing risk reserves (e.g., funds, time, or resources) for responding to potential risk events.

Risk Contingency Plans:

- Involves planning alternative responses to manage risks should they occur.
- Does not aim to reduce the probability or impact of risks but prepares to respond to them.
- Contingency plans are executed when risk events happen and should be in place well in advance.
- Typically developed for risks with high impact or those with response strategies that may introduce additional risks.
- Examples include disaster recovery plans.

Strategies for Positive Risks or Opportunities:

Exploitation:

- Seeks opportunities for positive impacts.
- Example: Shortening project duration by assigning more experienced resources to critical tasks.

Sharing:

    - Assigns risk ownership to a third party better equipped to utilize the opportunity presented by the risk.
    - Example: Forming a joint venture between a technical software company and a marketing firm.

Sidebar: Residual and Secondary Risks:

- **Secondary Risks:** Arise from implementing risk responses and are inherent in those responses. Planning responses for secondary risks is essential, often involving fallback plans.
- **Residual Risks:** Remain after other risk response plans are executed. Usually addressed through contingency reserves.

Risk Response Planning Outputs:

- Updates to the risk register, including descriptions, impacted project elements, categories, root causes, affected project objectives, risk owners, and triggers.
- Response plans and strategies, with specific actions and fallback plans.
- Cost and schedule activities for implementing responses.
- Contingency plans, reserves, and triggers.
- Lists of residual and secondary risks.
- Probabilistic analysis results from qualitative and quantitative risk analysis processes.