

Software Project Management

Ali Ameer Gondal

Assistant Professor

University of Engineering & Technology

Taxila, Pakistan

ali.ameer@uettaxila.edu.pk

17th Nov. 2011

Software Project Management

Lecture # 9

Risk Analysis & Management

Outline

- What is Risk Management?
- Risk Management Strategies
- Software Risks
- Risk Categories
- Risk Management Principles
- Risk Identification
- Risk Projection
- Risk Refinement
- RMMM?

Risk Management - Introduction

- **What is a Risk?**

- A risk is a potential problem which may or may not happen

- **What is Risk Analysis and Management?**

- It is a series of steps that help the software team to understand and manage uncertainty. It involves
 - Identifying risks
 - Assessing the probability of risks' occurrence
 - Estimating risks' impact

What is Risk Management? (Contd.)

- Ranking risks by probability and impact
 - Establishing a contingency plan to manage risks if they actually occurs
-
- **Who is responsible for Risk Analysis and Management?**
 - Everyone involved in the software process – managers, software engineers, stakeholders

Reactive Vs. Proactive Risk Strategies

- Reactive Risk Strategy
 - A reactive strategy monitors project for likely risks
 - Resources are set aside to deal with them
 - Commonly the software team does nothing about risks until something goes wrong
 - Then the team flies into action to correct the problem (fire-fighting mode)
 - When this fails, crisis management takes over and the project is in real trouble

Reactive Vs. Proactive Risk Strategies

- Proactive Risk Strategy
 - A more intelligent strategy which begins long before technical work is initiated
 - Potential risks are identified, probability and impact are assessed, ranked by importance and a plan is established

Software Risks

- There has been a considerable debate on proper definition of software risks but there is a general agreement that risk always has two characteristics
 - *Uncertainty* – the risk may or may not happen, i.e., there are no 100% probable risks*
 - *Loss* – if a risk becomes a reality, unwanted consequences or losses will occur

* A 100% probable risk = Project Constraint

Categories of Risks

- **Project risks**

- Threaten project plan, i.e., if they occur, project schedule will slip and costs will increase
- They identify potential budgetary, schedule, personnel, resource, stakeholder, and requirements problems & their impact on project

- **Technical risks**

- Threaten the quality and timeliness of software to be produced, if they occur implementation may become difficult or impossible
- They identify potential design, implementation, interface, verification and maintenance problems

Categories of Risks

- **Business risks**

- Threaten the viability of the software to be built

- Top five business risks are:

- Building an excellent product/system that no one really wants (market risk)
 - Building a product that no longer fits into the overall business strategy for the company (strategic risk)
 - Building a product that the sales force doesn't understand how to sell (sales risk)
 - Losing the support of senior management due to change in focus or change in people (management risk)
 - Losing budgetary or personnel commitment (budget risk)

Categories of Risks

- Another general categorization of risks (proposed by Charette):
 - Known risks
 - those that can be uncovered after careful evaluation of the project plan, the business and technical environment and other reliable information sources
 - Predictable risks
 - Those that can be extrapolated from past project experience (e.g., staff turnover, poor comm. with customer)
 - Unpredictable risks
 - They can and do occur
 - They are extremely difficult to identify in advance

7 Principles of Risk Management

- SEI has identified 7 principles for effective risk management
 - *Maintain a global perspective*
 - View software risks within the context of system in which it is a component and the business problem that it is intended to solve
 - *Take a forward-looking view*
 - Think about the risks that may arise in future, e.g., due to changes in software; establish plans so that future events are manageable

7 Principles of Risk Management

– *Encourage open communication*

- Consider a potential risk even if stated informally. Encourage all stakeholders and users to suggest risks at any time.

– *Integrate*

- A consideration of risk must be integrated into the software process

– *Emphasize a continuous process*

- The team must be vigilant throughout the software process, modifying identified risks as more information is known and adding new ones as better insight is achieved

7 Principles of Risk Management

– *Develop a shared product vision*

- If all the stakeholders share the same vision of the software, it is likely that better risk identification & assessment will occur

– *Encourage teamwork*

- The talent, skills, and knowledge of all stakeholders should be pooled when risk management activities are conducted

Risk Identification

- It is a systematic attempt to specify threats to the project plan
- By identifying known and predictable risks, the project manager takes a first step towards avoiding them when possible and controlling them when necessary
- There are two types of risks for each of the categories (already discussed)
 - Generic risks
 - Product-specific risks

Risk Identification

- **Generic risks**
 - Potential threats to every software project
- **Product-specific risks**
 - these can be identified only by those having a clear understanding of the technology, the people, and the environment specific to the software being developed.
 - To identify product-specific risks, the project plan and the software statement of scope are examined and an answer to the following is developed:
“what special characteristics of this product may threaten our project plan?”

Risk Identification (Contd.)

- **A Risk Identification Method:**

One method to identify risks is to create a risk item checklist.

- This checklist focuses on some subset of known and predictable risks in the following generic subcategories:

- Product size

- Risks associated with the overall size of software to be built or modified

- Business impact

- Risks associated with constraints imposed by management or the market place

Risk Identification (Contd.)

- Customer Characteristics
 - Risks associated with 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 to be defined and followed by the development organization
- Development environment
 - Risks associated with availability and quality of the tools to be used in product development

Risk Identification (Contd.)

- Technology to be built
 - Risks associated with complexity of the system to be built and the “newness” of technology that is packaged by the system
- Staff size and experience
 - Risks associated with the overall technical & project experience of the software engineers who will do the work

Risk Identification (Contd.)

- The risk item checklist can be organized in different ways.
- Questions relevant to each of the topics in checklist can be answered so that the planner can estimate risk impact
- A short list of questions can be used to provide preliminary indication of whether a project is “at risk”

Assessing Overall Project Risk (1)

- The following questions have been derived based on risk data obtained from experienced project managers around the world
(Their listing order is according to their relative importance to the success of a project)
 - Have top software and customer managers formally committed to support the project?
 - Are the end users enthusiastically committed to the project and the system/product to be built?
 - Are the requirements fully understood by the software engineering team and the customers?

Assessing Overall Project Risk (2)

- Have customers been involved fully in the definition of requirements?
- Do end-users have realistic expectations?
- Is project scope stable?
- Does the software engg team have the right mix of skills?
- Are project requirements stable?
- Does the project team have experience of the technology to be implemented?
- Is the no. of people on the team adequate to do the job?
- Do all customer/user constituencies agree on the importance of the project and on the requirements for the system/product to be built?

Assessing Overall Project Risk (3)

- If any of these questions has negative answers, mitigation, monitoring and management steps should be instituted.
- The degree to which a project is at risk is directly proportional to the number of negative responses to these questions

Risk Components and Drivers (1)

- The U.S. Air force has published an excellent guideline for software risk identification and abatement.
- Their approach requires project manager to identify risks drivers that affect software risk components
- Following are the Risk Components
 - Performance
 - Cost
 - Support
 - Schedule

Risk Components and Drivers (2)

- These risk components are defined as follows in context of these guidelines:
 - Performance risk
 - The degree of uncertainty that the product will meet its requirements and be fit for its intended use
 - Cost risk
 - The degree of uncertainty that the project budget will be maintained
 - Support risk
 - The degree of uncertainty that the resultant software will be easy to correct, adapt and enhance
 - Schedule risk
 - The degree of uncertainty that the project schedule will be maintained and that the product will be delivered on time

Risk Components and Drivers (3)

- The impact of each risk driver on the risk component is determined. This impact can be any of these four impact categories
 - Negligible
 - Marginal
 - Critical
 - Catastrophic

Risk Projection (1)

- Risk Projection is also known as Risk Estimation
- Risk projection rates each risk in two ways:
 - the probability that the risk is real and
 - the consequences of the problems associated with the risk, should it occur
- 4 Risk projection steps performed by project planner along with other managers & tech staff
 1. Establish a scale that reflects the perceived likelihood of a risk
 2. Delineate the consequences of the risk
 3. Estimate the impact of the risk on the project and the product
 4. Note overall accuracy of the risk projection so that there will be no misunderstandings

Risk Projection (2)

- The aim of these steps is to eventually determine prioritization of the risk
- By prioritizing risks, the software team can allocate resources where they will have the most impact.

Developing a Risk Table (1)

- A risk table provides a project manager with a simple technique for risk projection (estimation)
- The risk table can be implemented as a spread sheet model (enabling easy manipulation & sorting of entries)
- The table has the following content:
- **1st column:** list of all risks
- **2nd column:** categorization of risks, e.g., PS (Project Size risk), BU (Business risk)
- **3rd column:** probability of risk occurrence
- **4th column:** risk impact category
 - determined by averaging the impact categories of the 4 risk components – performance, support, cost, schedule)

Developing a Risk Table (2)

- After the first four columns are completed, the table is sorted by probability and by impact.
- High probability and high impact risks move to the top of the table and low ones drop to bottom
- Project Manager studies the resultant (1st order risk prioritization) table and defines a *cutoff line*.
- Risks above the *cutoff line* must be managed
- Risks below *cutoff line* are reevaluated for 2nd order prioritization.
- **5th column:** contains a pointer into a Risk Mitigation, Monitoring and Management Plan (RMMM) or alternatively, a collection of risk information sheets developed for all risks above the *cutoff*

Assessing Risk Impact

- If a risk does occur, then the consequences (that are likely) are affected by 3 factors
 - nature of risk
 - scope (severity & its distribution) of risk
 - timing of risk
- Following are the recommended steps to determine overall consequences of risk
 - Determine the avg probability of occurrence value for each risk component
 - Using impact assessment, determine impact for each component based on the criteria.
 - Complete the risk table & analyze the results as earlier.
- The overall risk exposure RE is determined using the following relationship:
 - **$RE = P \times C$**
 - where P = probability of occurrence for risk
 - C = cost to the project, if risk occurs

Risk Refinement (1)

- During early stages of the project, a risk is stated generally
- As time passes, learning about project work and related risks improves
- Hence, risks stated earlier can be refined, making them more detailed so that they are easier to handle
- Risk can be represented in *condition-transition-consequence* (CTC) format
 - *Given that <condition> then there is a concern that (possibly) <consequence>*

Risk Refinement (2)

- Example:
 - Given that all reusable components must conform to specific design standards and that some do not conform, then there is a concern that possibly only 70 percent of the planned reusable modules may actually be integrated into the as-built system, resulting in the need to custom engineer the remaining 30 percent of components
- Refinement:
 - Subcondition1
 - Certain reusable components were developed by a third party with no knowledge of internal design standards
 - Subcondition2
 - The design standard for component interfaces has not been solidified and may not conform to certain existing reusable components
 - Subcondition3
 - Certain reusable components have been implemented in a language that is not supported on target environment
- The consequence (of custom engg of 30% components) remains same for all refined subconditions but refinement helps in easy risk analysis

What is RMMM?

- RMMM = Risk Mitigation, Monitoring and Management
- An effective strategy to deal with risks must consider issues such as:
 - Risk avoidance
 - Risk monitoring
 - Risk management and contingency planning
- RMMM steps incur additional project cost

Example Scenario of a RISK...

- **Scenario**

- Assume that high staff turnover is a project risk r_1 .
- Based on past history, the likelihood l_1 , of high turnover is estimated to be 0.70 (70%)
- The impact x_1 , is projected as critical
- So, high turnover will have a critical impact on project cost and schedule

- **Steps to mitigate r_1 :**

- Meet the staff to find the causes of turnover (poor working conditions, low pay, etc.)
- Try to reduce the causes of turnover (if possible) before project starts
- Once project starts, assume turnover will occur and develop techniques to ensure continuity when people leave

Example Scenario of a RISK...

- Organize project teams so that information about each development activity is widely dispersed.
 - Define documentation standards & establish mechanisms to ensure that documents are timely developed.
 - Conduct peer reviews of all work.
 - Assign backup staff member for every critical technologist.
- **Risk Monitoring for r_1 :**
 - As project proceeds, risk monitoring activities commence to find indications whether the risk is becoming more or less likely.
 - Following factors are considered for r_1 :
 - General attitude of team members based on project pressures.
 - The degree to which the team is jelled.

Example Scenario of a RISK...

- Interpersonal relationships among team members.
- Potential problems with compensation and benefits.
- The availability of jobs within or outside the company.

- **Risk Management & Contingency Planning:**

This stage comes into play when mitigation efforts have failed and risk has become a reality.

- Considering again scenario for r_1 .
- The project is underway and a number of people announce that they will be leaving.
- If mitigation strategy has been followed, backup is available, information is documented and knowledge is dispersed across the team.

Example Scenario of a RISK...

- Project manager may refocus resources to those functions that are fully staffed and re-adjust schedule accordingly.
- The newcomers can “get up to speed” in the mean time.
- Individuals who are leaving are asked to stop all work and spend their last weeks in “knowledge transfer mode”.
- This may include
 - video-based knowledge capture,
 - development of “commentary documents”,
 - And / or meeting with other team members who will stay on the project team

Example Scenario of a RISK...

- **Cost/benefit analysis:**

- Since RMMM steps incur additional cost, the project managers & planners must consider if the benefit of these steps are outweighed by costs associated in implementing them.
- If risk management steps are projected to increase costs by 5% and duration by only 3%, then there is no harm in putting them in place.
- If these steps increase both project cost and duration by 15%, then they may not be undertaken.

Risk Management

- For a large project, 30 to 40 risks can be identified. If between 3 & 7 risk management steps are identified for each risk, risk management may become a project itself!
- For this reason, we adapt the **Pareto 80-20 rule** to software risks
 - Experience indicates that 80% of overall project risk (potential for failure) can be accounted for by 20% of the identified risks (the critical 20 risks with highest project priority).

Risk Management

- Risks can even occur after the software has been successfully developed & delivered to the customer.
- *Software safety and hazard analysis* (SQA activities) focus on identification & assessment of potential hazards that have negative affect and may cause entire system to fail.

The RMMM Plan

- The RMMM plan documents all work performed as part of risk analysis.
- It is used by project manager as part of overall project plan.
- Some software teams do not develop formal RMMM document. Rather, each risk is documented individually using a risk information sheet (RIS).
- In most cases, RIS is maintained using a database system so that creation & information entry, priority ordering, searches, and other analysis may be accomplished easily.

The RMMM Plan

- RIS contains the following information
 - Risk ID, Date, Probability & Impact
 - Description
 - Refinement/context
 - Mitigation/monitoring
 - Management/Contingency Plan/trigger
 - Current Status
 - Originator & Assigned (to whom) information
- Once RMMM has been documented & project has begun, risk mitigation and monitoring steps commence.

The RMMM Plan

- Risk mitigation is problem avoidance activity
- Risk monitoring has three main objectives:
 - To assess whether predicted risks do, in fact, occur
 - To ensure that risk aversion steps defined for the risk are properly applied
 - To collect info that can be used for future risk analysis
- A part of monitoring is to find causes (origin) of risks.

References

- Today's lecture contents were taken from the book:
 - “Software Engineering, A Practitioner's Approach”
by Roger Pressman