

Software Engineering

Lecture 11

Risk Analysis and Management



Reactive Risk Management

- Project team reacts to risks when they occur.
- More commonly, the software team does nothing about risks until something goes wrong.
- Then, the team involved into action in an attempt to correct the problem rapidly. This is often called a *fire fighting mode*.
- When this fails, “crisis management” takes over and the project is in real jeopardy.



Proactive Risk Management

- A proactive strategy begins long before technical work is initiated.
- Potential risks are identified, their probability and impact are assessed, and they are ranked by importance.
- Then, the software team establishes a plan for managing risk.
- The primary objective is to avoid risk, but because not all risks can be avoided, the team works to develop a contingency plan that will enable it to respond in a controlled and effective manner.

Software Risks

- Risk always involves two characteristics:
 - *Uncertainty*—the risk may or may not happen; that is, there are no 100% probable risks.
 - *Loss*—if the risk becomes a reality, unwanted consequences or losses will occur
- When risks are analyzed, it is important to quantify the level of uncertainty and the degree of loss associated with each risk.
- To accomplish this, different categories or types of risks are considered.
 - Project Risks
 - Technical Risks
 - Business Risks
 - Known Risks.
 - Predictable Risks
 - Unpredictable Risks

Project Risk

- ***Project risks*** make threats the project plan.
- That is, if project risks become real, it is likely that project schedule will slip and that costs will increase.
- Project risks identify potential budgetary, schedule, personnel (staffing and organization), resource, customer, and requirements problems and their impact on a software project.
- Project complexity, size, and the degree of structural uncertainty were also defined as project risk factors.



Technical risks

- *Technical risks* threaten the quality and timeliness of the software to be produced.
- If a technical risk becomes a reality, implementation may become difficult or impossible.
- Technical risks identify potential design, implementation, interface, verification, and maintenance problems.
- In addition, specification ambiguity, technical uncertainty, and "leading-edge" technology are also risk factors.




Business Risk

- *Business risks* threaten the feasibility of the software to be built.
- Business risks often jeopardize the project or the product.
- Top five business risks are
 - Building a excellent product or 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.
 - Losing the support of senior management due to a change in focus or a change in people (management risk)
 - Losing budgetary or personnel commitment (budget risks)



Known Risk

- *Known risks* are those that can be uncovered after careful evaluation of the project plan, the business and technical environment in which the project is being developed,
- Other reliable information sources (e.g., unrealistic delivery date, lack of documented requirements or software scope, poor development environment).

- 
- *Predictable risks* are generalized from past project experience (e.g., staff turnover, poor communication with the customer, etc).
 - *Unpredictable risks* are the joker in the deck. They can and do occur, but they are extremely difficult to identify in advance.

Risk Identification

- *Risk identification is a systematic attempt to specify threats to the project plan (estimates, schedule, resource loading, etc.).*
- By identifying known and predictable risks, the project manager takes a first step toward avoiding them when possible and controlling them when necessary.
- Two distinct types of risks
 - *Generic risks are a potential threat to every software project*
 - *Product-specific risks can be identified only by those with a clear understanding of the technology, the people, and the environment that is specific to the project at hand.*

Contd.

- To identify product-specific risks, the project Plan and the software statement of scope are examined.
- One method for identifying risks is to create a ***risk item checklist***.
- The checklist can be used for risk identification and focuses on some subset of *known and predictable risks* in the following generic subcategories:
- ***Product size*** —*risks associated with the overall size of the software to be built or modified.*
- ***Business impact*** —*risks associated with constraints imposed by management or the marketplace.*

Risk Item Checklist contd.

- **Customer characteristics** —risks associated with the 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 been defined and is followed by the development organization.
- **Development environment** —risks associated with the availability and quality of the tools to be used to build the product.
- **Technology to be built** —risks associated with the complexity of the system to be built and the "newness" of the technology that is packaged by the system.
- **Staff size and experience** —risks associated with the overall technical and project experience of the software engineers who will do the work.



Risk Components

PM identify the risk drivers that affect software risk components:

- *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.

The impact of each risk driver on the risk component

Components Category		Performance	Support	Cost	Schedule
Catastrophic	1	Failure to meet the requirement would result in mission failure		Failure results in increased costs and schedule delays with expected values in excess of \$500K	
	2	Significant degradation to nonachievement of technical performance	Nonresponsive or unsupportable software	Significant financial shortages, budget overrun likely	Unachievable IOC
Critical	1	Failure to meet the requirement would degrade system performance to a point where mission success is questionable		Failure results in operational delays and/or increased costs with expected value of \$100K to \$500K	
	2	Some reduction in technical performance	Minor delays in software modifications	Some shortage of financial resources, possible overruns	Possible slippage in IOC
Marginal	1	Failure to meet the requirement would result in degradation of secondary mission		Costs, impacts, and/or recoverable schedule slips with expected value of \$1K to \$100K	
	2	Minimal to small reduction in technical performance	Responsive software support	Sufficient financial resources	Realistic, achievable schedule
Negligible	1	Failure to meet the requirement would create inconvenience or nonoperational impact		Error results in minor cost and/or schedule impact with expected value of less than \$1K	
	2	No reduction in technical performance	Easily supportable software	Possible budget underrun	Early achievable IOC

Risk Projection

- *Risk projection*, also called *risk estimation*, attempts to rate each risk in two ways:
 - The likelihood or probability that the risk is real.
 - the consequences (i.e. effect or result) of the problems associated with the risk, should it occur.
- The project planner, along with other managers and technical staff, performs four risk projection activities:
 - Establish a scale that reflects the supposed likelihood of a risk
 - Describe the consequences of the risk,
 - Estimate the impact of the risk on the project and the product,
 - Note the overall accuracy of the risk projection so that there will be no misunderstanding
- The intent of these steps is to consider risks in a manner that leads to prioritization. By prioritizing risks, the team can allocate resources where they will have the most impact.

Developing Risk Table

Risks	Category	Probability	Impact	RMMM
Size estimate may be significantly low	PS	60%	2	
Larger number of users than planned	PS	30%	3	
Less reuse than planned	PS	70%	2	
End-users resist system	BU	40%	3	
Delivery deadline will be tightened	BU	50%	2	
Funding will be lost	CU	40%	1	
Customer will change requirements	PS	80%	2	
Technology will not meet expectations	TE	30%	1	
Lack of training on tools	DE	80%	3	
Staff inexperienced	ST	30%	2	
Staff turnover will be high	ST	60%	2	
•				
•				
•				

Impact values:

- 1—catastrophic
- 2—critical
- 3—marginal
- 4—negligible

Procedure to build risk table

- Listing all risks in first column. This can be accomplished with the help of the risk item checklists
- Each risk is categorized in the second column
- The probability of occurrence of each risk is entered in the next column of the table. Which can be estimated by team members.
- Impact of each risk is assessed. Each *risk component* is assessed using the characterization and an impact categories like *catastrophic, critical, marginal and negligible* are determined.
- Once table is completed, manager will give order of prioritization to the risk. Therefore, the table is sorted by probability and by impact.



Contd.

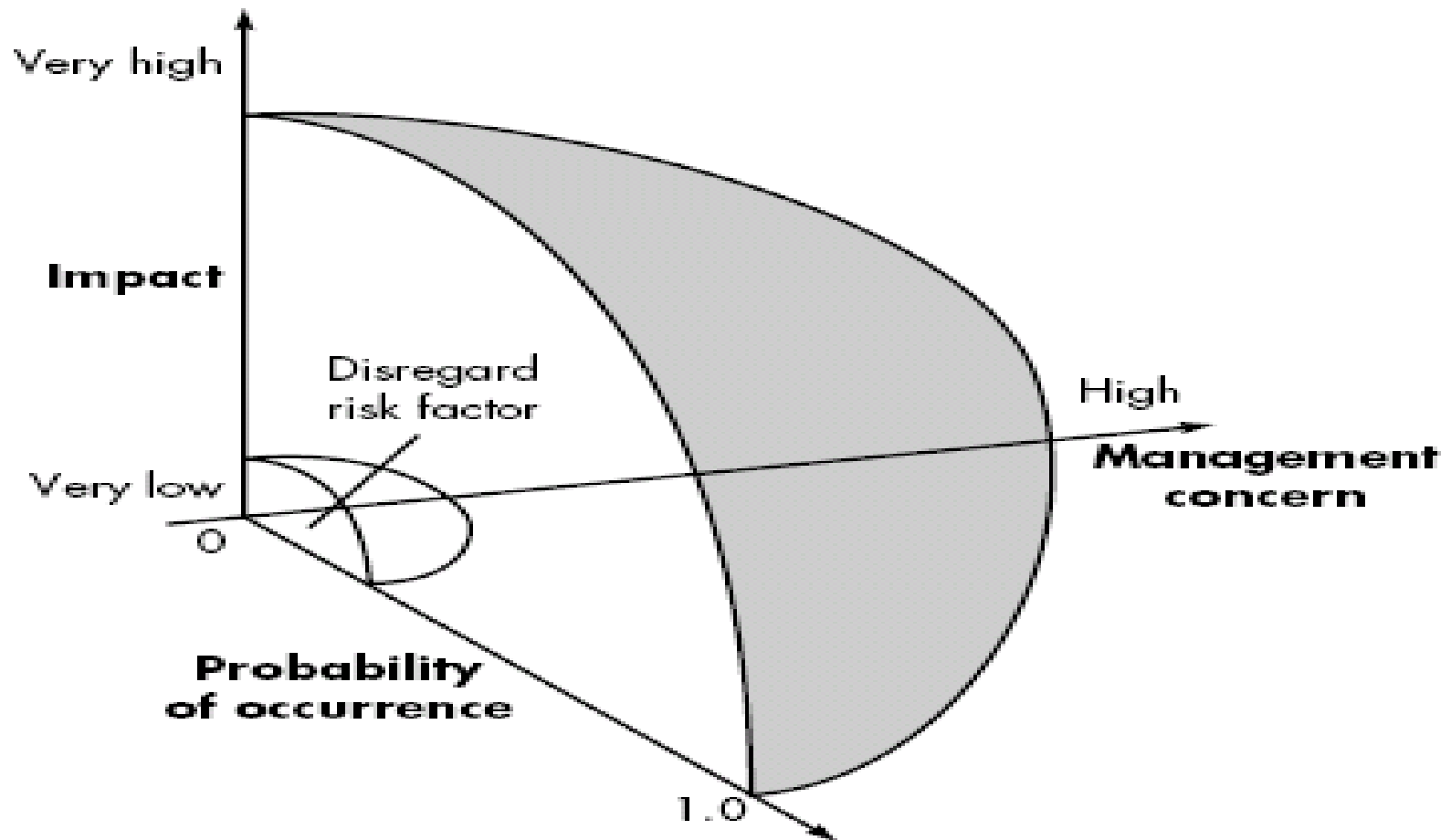
- High-probability, high-impact risks get into the top of the table, and low-probability risks drop to the bottom. (First order prioritization).
- The project manager studies the resultant sorted table and defines a cutoff line.
- The *cutoff line* implies that only risks that lie above the line will be given further attention.
- Risks that fall below the line are considered as second-order prioritization.



Contd.

- Risk impact and probability have a distinct influence on management concern.
- Risk factor that has a high impact but a very low probability of occurrence then management will give little attention or some time no attention.
- But if risk factor that has high impact and high probability of occurrence then management will give high attention.
- All risks that lie above the cutoff line must be managed and specify in last column of the table under RMMM column.

Contd.



Assessing Risk Impact

- Three factors affect the consequences that are likely if a risk does occur:
 - Nature,
 - Scope, and
 - Timing.
- The *nature* of the risk indicates the problems that are likely if it occurs.

For example, a technical risk, development environment change
- The *scope* of a risk combines the strictness with its overall distribution.
- For ex. how much of the project will be affected or how many customers are harmed?
- The *timing* of a risk considers when and for how long the impact will be felt.



To determine the overall consequences of a risk:

- Determine the average probability of occurrence value for each risk component.
- Determine the impact for each component based on the criteria.
- Complete the risk table and analyze the results as described

Now measure, Risk exposure (RE).

$$RE = P \times C$$

P is the probability of occurrence for a risk and C is the cost to the project.

Example- the software team defines a project risk in the following manner


- **Risk Identification** - Only 70 percent of the software components scheduled for reuse and remaining functionality will have to be custom developed.
- **Risk probability.** 80% (likely).
- **Risk Impact** – Assume total no. of component is 60. If only 70 percent can be used, 18 components would have to be developed from scratch.
- Since the average component is 100 LOC and local data indicate that the software engineering cost for each LOC is \$14.00,
- the overall cost (impact) to develop the components would be
$$18 \times 100 \times 14 = \$25,200.$$
- **Risk exposure.** $RE = 0.80 \times 25,200 \sim \$20,200.$


Contd.


- once an estimate of the cost of the risk is derived, compute RE for each risk in risk table.
- The total risk exposure for all risks (above the cutoff in the risk table) can provide a means for adjusting the final cost estimate for a project.
- The project team should revisit the risk table at regular intervals, re-evaluating each risk to determine when new circumstances cause its probability and impact to change.
- As a consequence of this activity, it may be necessary to add new risks to the table, remove some risks that are no longer relevant, and change the relative positions of still others.
- *Compare RE for all risks to the cost estimate for the project. If RE is greater than 50 percent of project cost, the feasibility of the project must be evaluated.*

Risk Mitigation, Monitoring, and Management

- Risk analysis goal - to assist the project team in developing a strategy for dealing with risk. An effective strategy must consider three issues:
 - Risk avoidance or mitigation.
 - Risk monitoring
 - Risk management and contingency planning
- Proactive approach to risk, avoidance is always the best strategy. This is achieved by developing a plan for *risk mitigation*.
- For example, assume that high staff turnover (i.e. revenue) is noted as a project risk.

- 
- To mitigate this risk, project management must develop a strategy for reducing turnover.
 - Steps are:
 - Meet with current staff to determine causes for turnover (e.g., low pay, competitive job market).
 - Mitigate those causes that are under our control before the project starts.
 - Organize project teams so that information about each development activity is widely dispersed.
 - Define documentation standards and establish mechanisms to be sure that documents are developed in a timely manner.
 - Conduct peer reviews of all work
 - Assign a backup staff member for every critical technologist.

- 
- As the project proceeds, *risk monitoring* activities commence.
 - The project manager monitors factors that may provide an indication of whether the risk is becoming more or less likely.
 - In the case of high staff turnover, the following factors can be monitored:
 - General attitude of team members based on project pressures.
 - Potential problems with compensation and benefits.
 - The availability of jobs within the company and outside it.
 - *Risk management and contingency planning* assumes that mitigation efforts have failed and that the risk has become a reality.

- 
- The project is well underway and a number of people announce that they will be leaving. If the mitigation strategy has been followed, backup is available, information is documented, and knowledge has been dispersed across the team.
 - In addition, the project manager may temporarily refocus resources (and readjust the project schedule) to those functions that are fully staffed, enabling newcomers who must be added to the team to “get up to speed.”
 - Those individuals who are leaving are asked to stop all work and spend their last weeks in “knowledge transfer mode.”
 - This might include video-based knowledge capture, the development of “commentary documents,” and/or meeting with other team members who will remain on the project.

RMMM steps incur additional project cost. For example, spending the time to “backup” every critical technologist costs money.

THE RMMM PLAN

- The RMMM plan documents all work performed as part of risk analysis and is used by the project manager as part of the overall project plan.
- Some software teams do not develop a formal RMMM document. Rather, each risk is documented individually using a *risk information sheet* (RIS).
- RIS is maintained using a database system, so that creation and information entry, priority ordering, searches, and other analysis may be accomplished easily.
- Once RMMM has been documented and the project has begun, risk mitigation and monitoring steps commence.

Risk information sheet

Risk ID: P02-4-32

Date: 5/9/02

Prob: 80%

Impact: high

Description:

Only 70 percent of the software components scheduled for reuse will, in fact, be integrated into the application. The remaining functionality will have to be custom developed.

Refinement/context:

Subcondition 1: Certain reusable components were developed by a third party with no knowledge of internal design standards.

Subcondition 2: The design standard for component interfaces has not been solidified and may not conform to certain existing reusable components.

Subcondition 3: Certain reusable components have been implemented in a language that is not supported on the target environment.

Mitigation/monitoring:

1. Contact third party to determine conformance with design standards.
2. Press for interface standards completion; consider component structure when deciding on interface protocol.
3. Check to determine number of components in subcondition 3 category; check to determine if language support can be acquired.

Management/contingency plan/trigger:

RE computed to be \$20,200. Allocate this amount within project contingency cost. Develop revised schedule assuming that 18 additional components will have to be custom built; allocate staff accordingly.

Trigger: Mitigation steps unproductive as of 7/1/02

Current status:

5/12/02: Mitigation steps initiated.

Originator: D. Gagne

Assigned: B. Laster