RISK PLANNING

- **Consider each risk and develop a strategy to manage that risk**
- **Reactive vs. proactive approach**
- **Avoidance strategies**
  – The probability that the risk will arise is reduced
- **Minimization strategies**
  – The impact of the risk on the project or product will be reduced
- **Contingency plans**
  – If risk arises, contingency plans are to deal with that risk
- **Risk mitigation, risk transfer**

RISK MONITORING

- **Assess each identified risks regularly to decide whether it is becoming less or more probable**
- **Also assess whether the effects of the risk have changed**
- **Each key risk should be discussed at management progress meetings**

Assessing Overall Project Risk

- The following questions have been derived from risk data obtained by surveying experienced software project managers in different parts of the world.
- The questions are ordered by their relative importance to the success of a project.

Questions

- **Have top software and customer managers formally committed to support the project?**
- **Are end users enthusiastically committed to the project and the system/ product to be built?**
- **Are requirements fully understood by the software engineering team and its customers?**
- **Have customers been involved fully in the definition of requirements?**
- **Do end users have realistic expectations?**
- **Is the project scope stable?**
- **Does the software engineering team have the right mix of skills?**
- **Are project requirements stable?**
- **Does the project team have experience with the technology to be implementation**

Questions

- **Is the number of people on the project team adequate to do the job?**
- **Do all customer agree on the importance of the project and on the requirements for the system/product to be built?**

Risk Components and Drivers

Risk components are defined in the following manner:

- ***Risk drivers are the reason which can affect the performance /schedule/cost of the projects***
- ***The project manager identifies the risk drivers that affect the following 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.

Risk Components and Drivers

- ***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 is divided into one of four impact categories—**negligible**, **marginal**, **critical**, or **catastrophic**

Risk Projection

Risk projection, also called ***risk estimation,*** attempts to rate each risk in two ways—

(1) the l**ikelihood or probability** that the risk is real

(2) the **consequences** of the problems associated with the risk, should it occur.

Risk Projection

Risk projection steps:

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. Assess the overall accuracy of the risk projection so that there will be no misunderstandings.

Risk Table

- A risk table provides you with a simple technique for **risk projection.**

- You begin by listing all risks in the first column of the table.
- This can be accomplished with the help of the risk item checklists
- Each risk is categorized in the second column
- The table is sorted by probability and by impact.
- High-probability, high-impact risks percolate to the top of the table, and low-probability risks drop to the bottom.

Risk Projection and 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	
Σ				
Σ				
Σ				

Impact values:
1—catastrophic
2—critical
3—marginal
4—negligible

Risk Category:
PS = Project size risk
BU = Business risk
TE = Technology risk
DE = Development risk
ST = Stakeholder risk
CU =Customer risk

Fig. RISK TABLE

Risk Table and Projection

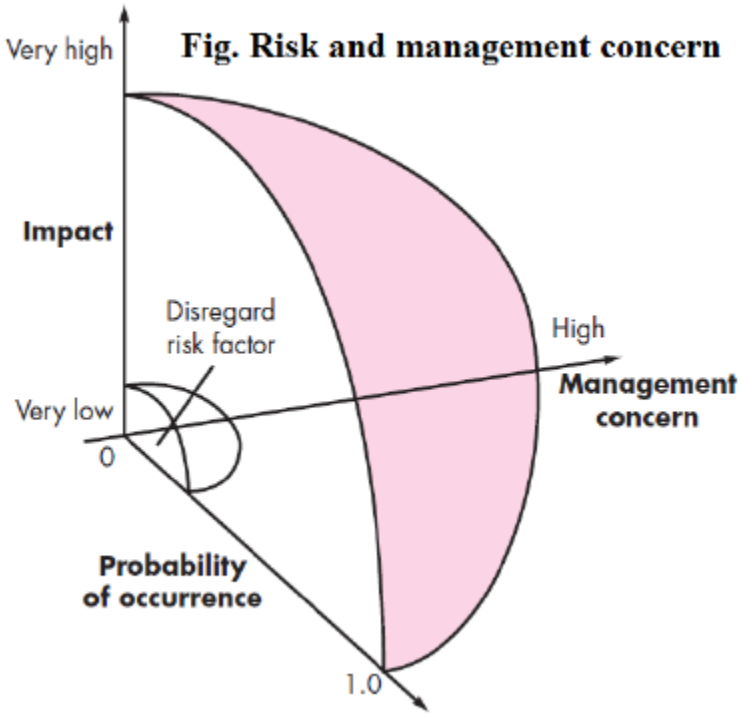

Fig. Risk and management concern

Risk Table and Projection (Management Concern)

- A risk factor that has a high impact, but a very low probability of occurrence should not absorb a significant amount of management time.
- However, high-impact risks with moderate to high probability and low-impact risks with high probability should be carried forward into the risk analysis steps that follow.
- All risks that lie above the cutoff line should be managed.
- The column labeled RMMM contains a pointer into a *risk mitigation, monitoring, and management plan* or, alternatively, a collection of risk information sheets developed for all risks that lie above the cutoff.

Risk Refinement

- Process **of restating the risks as a set of more detailed risks** that will be easier to mitigate, monitor, and manage.
- During early stages of project planning, a risk may be stated quite generally.
- As time passes and more is learned about the project and the risk, it may be possible to refine the risk into a set of more detailed risks, each somewhat easier to mitigate, monitor, and manage.
- One way to do this is to represent the risk in ***condition-transition-consequence*** **(CTC) format.**
- Given that <condition> then there is concern that (possibly) <consequence>.

RISK REFINEMENT

- **Given that all reusable software components must conform to specific design standards and that some do not conform, then there is 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.**
- This general condition can be refined in the following manner:
- **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.
- The consequences associated with these refined subconditions remain the same (i.e., 30 percent of software components must be custom engineered), but the refinement helps to isolate the underlying risks and might lead to easier analysis and response.

RMMM

- Risk **Mitigation, Monitoring, and Management**
- Assessment helps to develop strategy
- An effective strategy must consider three issues: **risk avoidance**, **risk monitoring**, **and risk management and contingency planning**.

RMMM

- All of the risk analysis activities presented to this point have a single goal—to assist the project team in developing a strategy for dealing with risk.
- An effective strategy must consider three issues: risk avoidance, risk monitoring, and risk management and contingency planning.
- If a software team adopts a proactive approach to risk, avoidance is always the best strategy. This is achieved by developing a plan for *risk mitigation*

RMMM

For example, assume that high staff turnover is noted as a project risk

- To mitigate this risk, you would develop a strategy for reducing turnover.

The possible steps to be taken are:

- Meet with current staff to determine causes for turnover (e.g., poor working conditions, low pay, competitive job market).
- Mitigate those causes that are under your control before the project starts.
- Once the project commences, assume turnover will occur and develop techniques to ensure continuity when people leave.
- Organize project teams so that information about each development activity is widely dispersed.

RMMM

- Define work product standards and establish mechanisms to be sure that all models and documents are developed in a timely manner.
- Conduct peer reviews of all work (so that more than one person is “up to speed”).
- Assign a backup staff member for every critical technologist.

Risk Information Sheet

Risk information sheet			
Risk ID: P02-4-32	Date: 5/9/09	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 7/1/09.			
Current status: 5/12/09: Mitigation steps initiated.			
Originator: D. Gagne		Assigned: B. Laster	