RISK MANAGEMENT

- A risk is a potential problem – it might happen and it might not

- Conceptual definition of risk
  - Risk concerns future happenings
  - Risk involves change in mind, opinion, actions, places, etc.

- Two characteristics of risk
  - Uncertainty – the risk may or may not happen, that is, there are no 100% risks .
  - Loss – the risk becomes a reality and unwanted consequences or losses occur

- **Reactive Versus Proactive Risk Strategies:-**
- *Reactive risk strategies:-*
- The majority of software teams rely solely on reactive risk strategies.

- “Don’t worry, I’ll think of something!” Never worrying about problems until they happened.

- The team flies into action in an attempt to correct the problem rapidly. This is often called a *fire-fighting mode*.

- *Proactive strategy:-*
- 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.
- The software team establishes a plan for managing risk.

- **Software Risks**
- Risk Categorization:
- **Project risks** threaten the project plan.
  - Project risks identify potential budgetary, schedule, personnel (staffing and organization), resource, stakeholder, and requirements problems and their impact on a software project.

- **Technical risks** threaten the quality and timeliness of the software to be produced.
  - Technical risks identify potential design, implementation, interface, verification, and maintenance problems.

- **Business risks** threaten the viability of the software to be built and often risk the project or the product.

- Sub-categories of Business risks
  - **Market risk** – building an excellent product or system that no one really wants
  - **Strategic risk** – building a product that no longer fits into the overall business strategy for the company
  - **Sales risk** – building a product that the sales force doesn't understand how to sell
  - **Management risk** – losing the support of senior management due to a change in focus or a change in people
  - **Budget risk** – losing budgetary or personnel commitment

- **Risk Identification**
- Risk identification is a systematic attempt to specify threats to the project plan.

- By identifying known and predictable risks, the project manager takes a first step toward avoiding them when possible and controlling them when necessary.

- Generic risks
  - Risks that are a potential threat to every software project

- Product-specific risks
  - Risks that can be identified only by those a with a clear understanding of the technology, the people, and the environment that is specific to the software that is to be built.
  - This requires examination of the project plan and the statement of scope.
  - "What special characteristics of this product may threaten our project plan?"

- One method for identifying risks is to create a risk item checklist.

- Focuses on known and predictable risks in specific subcategories.

- Following generic subcategories:
- **Product size** – risks associated with overall size of the software to be built

- **Business impact** – risks associated with constraints imposed by management or the marketplace

- **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 been defined and is followed

- **Development environment** – risks associated with availability and quality of the tools to be used to build the project

- **Technology to be built** – risks associated with complexity of the system to be built and the "newness" of the technology in the system

- **Staff size and experience** – risks associated with overall technical and project experience of the software engineers who will do the work

- Questionnaire on Project Risk:-

1) Have top software and customer managers formally committed to support the project?
2) Are end-users actively committed to the project and the system/product to be built?
3) Are requirements fully understood by the software engineering team and its customers?

4) Have customers been involved fully in the definition of requirements?
5) Do end-users have realistic expectations?
6) Is the project scope stable?
7) Does the software engineering team have the right mix of skills?
8) Are project requirements stable?
9) Does the project team have experience with the technology to be implemented?
10) Is the number of people on the project team adequate to do the job?
11) Do all customer/user constituencies agree on the importance of the project and on the requirements for the system/product to be built?

- **Risk Components and Drivers**
- The project manager identifies the risk drivers that affect the following 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 is divided into one of four impact levels
  - Negligible, marginal, critical, and catastrophic

- **Risk Projection:-**
- Risk projection (or estimation) attempts to rate each risk in two ways
  - The probability that the risk is real
  - The consequence of the problems associated with the risk, should it occur.

The project planner, managers, and technical staff perform four risk projection steps

1) Establish a scale that reflects the perceived likelihood of a risk (e.g., 1-low, 10-high)
2) Define the consequences of the risk
3) Estimate the impact of the risk on the project and product
4) Note the overall accuracy of the risk projection so that there will be no misunderstandings

- The intent of these steps is to consider risks in a manner that leads to prioritization.

- Be prioritizing risks, the software team can allocate limited resources where they will have the most impact.

- **Developing a Risk Table**
- A risk table provides a project manager with a simple technique for risk projection

- It consists of five columns
  - Risk Summary – short description of the risk
  - Risk Category – one of seven risk categories
  - Probability – estimation of risk occurrence based on group input
  - Impact – (1) catastrophic (2) critical (3) marginal (4) negligible
  - RMMM – Pointer to a paragraph in the Risk Mitigation, Monitoring, and Management Plan

Sample risk table prior to sorting

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

- Developing a Risk Table
- List all risks in the first column (by way of the help of the risk item checklists)
- Mark the category of each risk
- Estimate the probability of each risk occurring
- Assess the impact of each risk based on an averaging of the four risk components to determine an overall impact value
- Sort the rows by probability and impact in descending order
- Draw a horizontal cutoff line in the table that indicates the risks that will be given further attention

- Assessing Risk Impact:-
- Three factors affect the consequences that are likely if a risk does occur
  - **Its nature** – This indicates the problems that are likely if the risk occurs
  - **Its scope** – This combines the severity of the risk (how serious was it) with its overall distribution (how much was affected)
  - **Its timing** – This considers when and for how long the impact will be felt

- The overall risk exposure formula is RE = P x C
  - P = the probability of occurrence for a risk
  - C = the cost to the project should the risk actually occur

- Example
  - P = 80% probability that 18 of 60 software components will have to be developed
  - C = Total cost of developing 18 components is $25,000
  - RE = .80 x $25,000 = $20,000

- **Risk Refinement**
- As time passes and more is learned about the project and the risk, it may be possible to refine the risk.

Given that <condition> then there is concern that (possibly) <consequence>

- **Risk Mitigation, Monitoring, And Management**
- An effective strategy for dealing with risk must consider three issues
  - Risk mitigation (i.e., avoidance)
  - Risk monitoring
  - Risk management and contingency planning

- Risk mitigation (avoidance) is the primary strategy and is achieved through a plan
  - Example: Risk of high staff turnover

Strategy for Reducing Staff Turnover

- 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 our 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

- Define documentation standards and establish mechanisms to ensure that 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

- During risk monitoring, the project manager monitors factors that may provide an indication of whether a risk is becoming more or less likely .

- Risk management and contingency planning assume that mitigation efforts have failed and that the risk has become a reality

- RMMM steps incur additional project cost
  - Large projects may have identified 30 – 40 risks

- Risk is not limited to the software project itself
  - Risks can occur after the software has been delivered to the user

- Software safety and hazard analysis
  - These are software quality assurance activities that focus on the identification and assessment of potential hazards that may affect software negatively and cause an entire system to fail
  - If hazards can be identified early in the software process, software design features can be specified that will either eliminate or control potential hazards

- 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.

- Each risk is documented individually using a *risk information sheet*

- Once RMMM has been documented and the project has begun, risk mitigation and monitoring steps commence.

FIGURE 28.4

Risk information sheet.
Source: [Wil97].

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

- Risk monitoring has three objectives
  - To assess whether predicted risks do, in fact, occur
  - To ensure that risk aversion steps defined for the risk are being properly applied
  - To collect information that can be used for future risk analysis