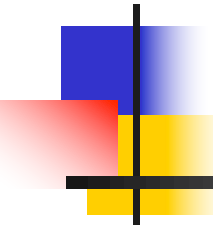
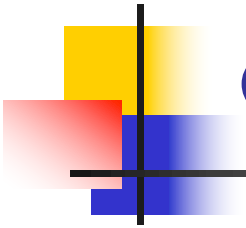


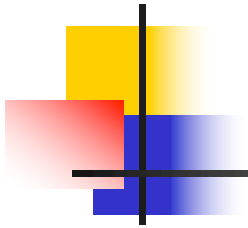
Software Project Management

Risk Management

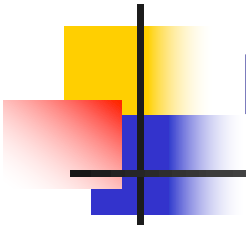


Objectives

- What's Risk?
- Software Risk
- Software Risk Management
- Software Risk Management Process

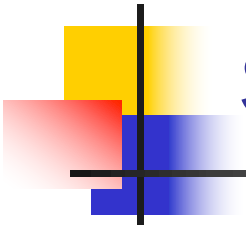


"If you don't actively attack the risks, they will actively attack you" [Gilb-88]



Risk

- "Anything worth doing has risks. The challenge is not to avoid them but to manage them."
- Risk Management is an attempt to minimize the chances of failure caused by unplanned events.
- Risks are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative effect.
  - Defects are not risk. They are almost certain.
  - Risks are probabilistic events.



Software Risk Management

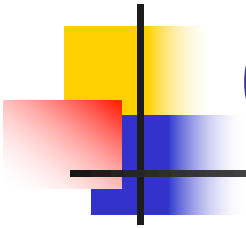
- Although there is a basic component of risk management inherent in good project management, risk management differs from project management in the following ways:

Cont..

Project Management	Risk Management
Designed to address general or generic risks	Designed to focus on risks unique to each project
Looks at the big picture and plans for details	Looks at potential problems and plans for contingencies
Plans what should happen and looks for ways to make it happen	Evaluates what could happen and looks for ways to minimize the damage
Plans for success	Plans to manage and mitigate potential causes of failure

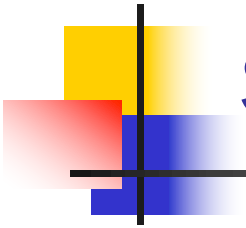
Four Reason implementing SRM

- With risk management the "emphasis is shifted from crisis management to anticipatory management"
- Boehm defines four major reasons for implementing SRM
  1. Avoiding software project disasters,
     - Including run away budgets and schedules, defect-ridden software products, and operational failures
  2. Avoiding rework caused by erroneous, missing, or ambiguous requirements, design or code,
     - which typically consume 40-50% of the total cost of software development



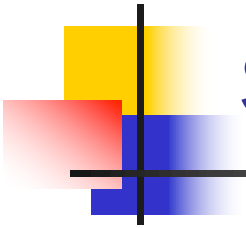
Cont…

3. Avoiding overkill with detection and prevention techniques in area of minimal or no risk
4. Stimulating a win-win software solution where the customer receives the product they need and the vendor makes the profits they expect



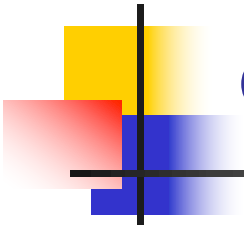
Software Risk

- There are basic risks that are generic to almost all software projects.



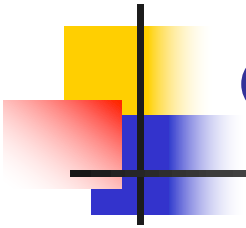
Software Risk

- A software project may encounter various types of risks:
- Technical risks
  - include problems with languages, project size, project functionality, platforms, methods, standards, or processes.
  - These risks may result from excessive constraints, lack of experience, poorly defined parameters, or dependencies on organizations outside the direct control of the project team.



Cont…

- Management risks
  - include lack of planning, lack of management experience and training, communications problems, organizational issues, lack of authority, and control problems.
- Financial risks
  - include cash flow, capital and budgetary issues, and return on investment constraints.
- Contractual and legal risks
  - include changing requirements, market-driven schedules, health & safety issues, government regulation, and product warranty issues.



Cont…

- Personnel risks
  - include staffing lags, experience and training problems, ethical and moral issues, staff conflicts, and productivity issues.
- Other resource risks
  - include unavailability or late delivery of equipment and supplies, inadequate tools, inadequate facilities, distributed locations, unavailability of computer resources, and slow response times.

Risk Management Process

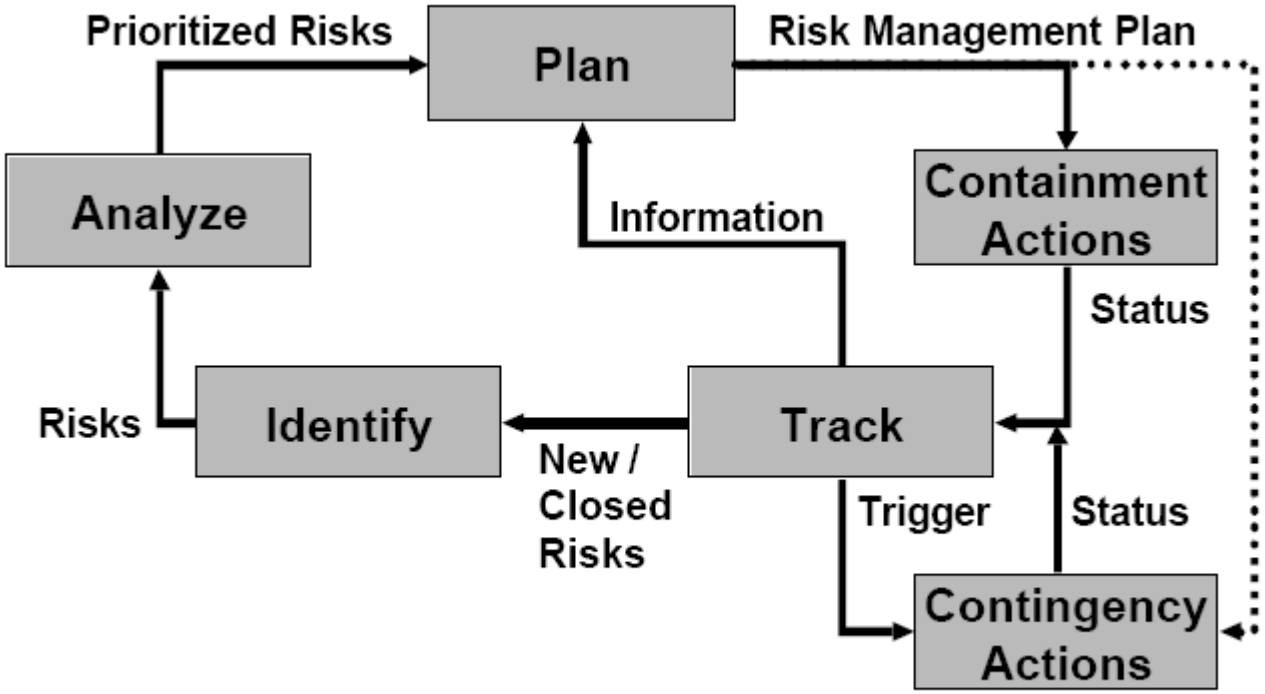
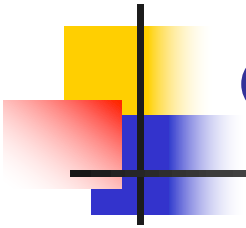
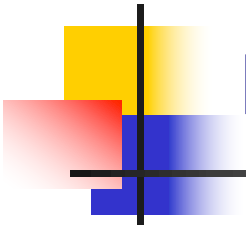


Figure 1 - Risk Management Process



Cont…

- Risk Management can broadly divided
  - Risk Assessment
    - Identification
    - Analysis
    - Prioritization
  - Risk Control
    - Planning
    - Resolution
    - Monitoring
    - Correction (usually considered part of monitoring)



Risk Identification

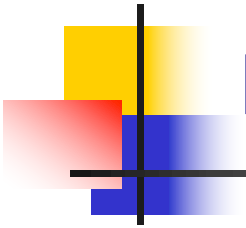
- During the first step in the software risk management process, risks are identified and added to the list of known risks.
- The output of this step is a list of project-specific risks that have the potential of compromising the project's success.
- There are many techniques for identifying risks, including interviewing, reporting, decomposition, assumption analysis, critical path analysis, and utilization of risk taxonomies.

Risk Identification Techniques

- Interviewing/Brainstorming:
  - with project personnel, customers, and vendors.
  - Open-ended questions such as the following can help identify potential areas of risk.
    - What new or improved technologies does this project implement?
    - What interfaces issues still need to be defined?
    - What requirements exist that we aren't sure how to implement?
- Voluntary Reporting:
  - where any individual who identifies a risk is encouraged and rewarded for bringing that risk to management's attention.

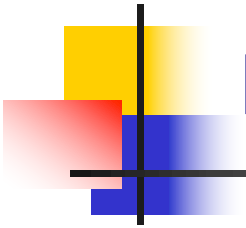
Risk Identification Techniques

- Decomposition:
  - As the product is being decomposed during the requirements and design phases, another opportunity exists for risk identifications. Every TBD ("To Be Done/Determined") is a potential risk.
  - As Ould states, “The most important thing about planning is writing down what you *don’t know*, because what you don’t know is what you must find out” [Ould-90].
  - Decomposition in the form of work breakdown structures during project planning can also help identify areas of uncertainty that may need to be recorded as risks.
- Assumption Analysis:
  - Process and product assumptions must be analyzed. For example, we might assume the hardware would be available by the system test date or three additional experienced C++ programmers will be hired by the time coding starts. If these assumptions prove to be false, we could have major problem



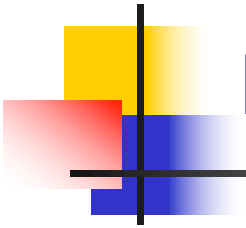
Risk Identification Techniques

- Critical Path Analysis:
  - As we perform critical path analysis for our project plan, we must remain on the alert to identify risks.
  - Any possibility of schedule slippage on the critical path must be considered a risk because it directly impacts our ability to meet schedule.
- Risk Taxonomies:
  - Risk taxonomies are lists of problems that have occurred on other projects and can be used as checklists to help ensure all potential risks



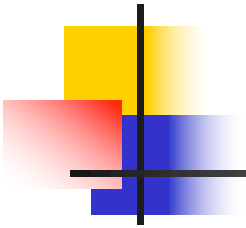
Risk Identification Techniques

- Top software risk items
  - Personnel shortfalls
  - Unrealistic schedules and budgets
  - Developing the wrong functions and properties
  - Developing the wrong user interface
  - Continuing stream of requirements changes
  - Shortfalls in externally furnished components
  - Shortfalls in externally performed tasks
  - Real-time performance shortfalls



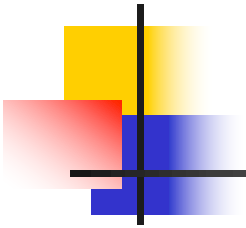
Risk Analysis

- During the risk analysis step, each risk is assessed to determine:
  - Likelihood: the probability that the risk will result in a loss
  - Impact: the size or cost of that loss if the risk turns into a problem
  - Timeframe: when the risk needs to be addressed (i.e., risk associated with activities in the near future would have a higher priority then similar risks in later activities)
  - the interrelationships between risks are assessed to determine if compounding risk conditions magnify losses.



Risk Analysis

- Boehm defines the Risk Exposure equation to help quantitatively establish risk priorities [Boehm-89].
- Risk Exposure measures the impact of a risk in terms of the expected value of the loss.
- Risk Exposure (RE) is defined as the probability of an undesired outcome times the expected loss if that outcome occurs.
  - RE = Probability (UO) * Loss (UO), where UO = Unexpected outcome



Risk Prioritization

- The list of risks is then prioritized based on the results of our risk analysis.
- Since resource limitations rarely allow the consideration of all risks, the prioritized list of risks is used to identify risks requiring additional planning and action.
- Other risks are documented and tracked for possible future consideration. Based on changing conditions, additional information, the identification of new risks, or the closure of existing risks, the list of risks requiring additional planning and action may require periodic updates.

Risk Management Planning

- Taking the prioritized risk list as input, plans are developed for the risks chosen for action.
- Next Fig shows the specific questions that can be asked to help focus on the type of planning required.
- Two Example risks to illustrate the types of actions that might be taken using each risk handling technique:
  - The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications.
  - The interface with the new control device is not defined and as a result its driver may take more time to implement then scheduled.

Risk Management Planning

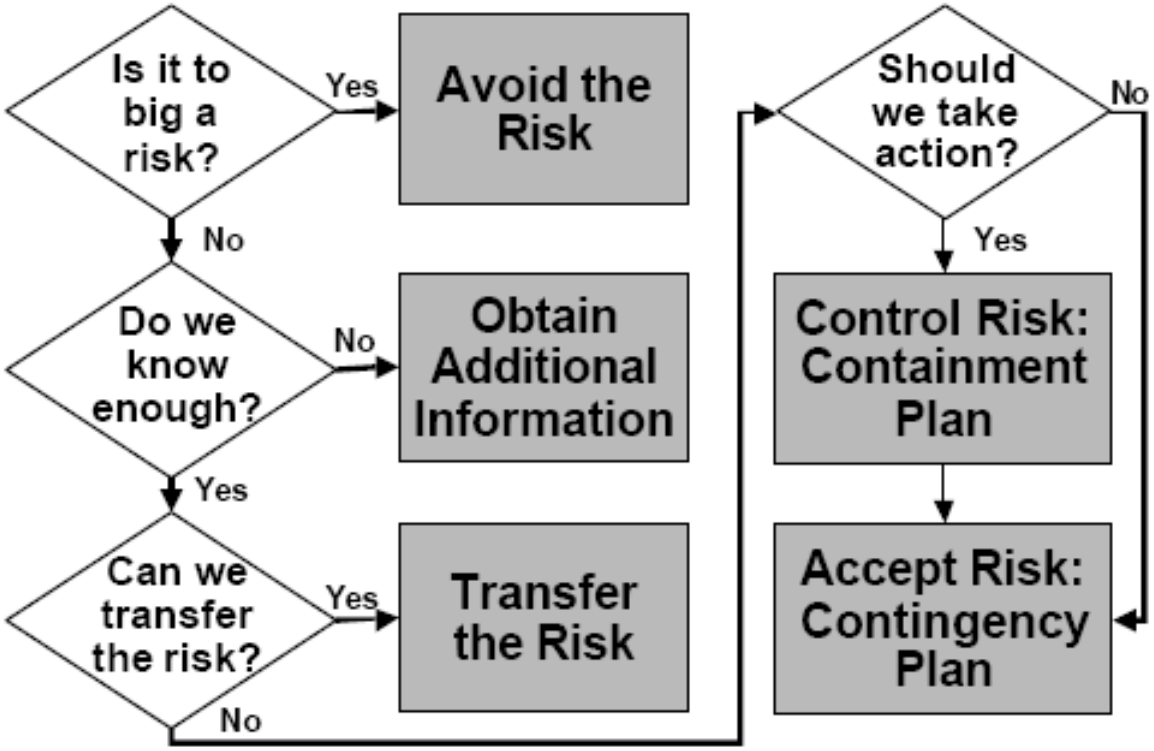
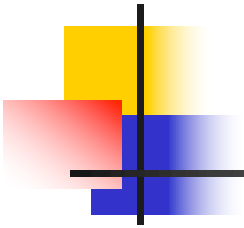


Figure 2 - Techniques for Handling Risks

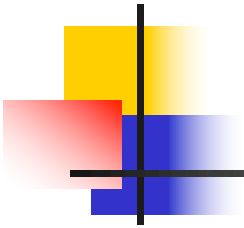


Risk Management Planning

- Is it too big a risk?
  - If the risk is too big for us to be willing to accept,
  - we can avoid the risk by changing our project strategies and tactics to choose a less risky alternate or
  - we may decide not to do the project at all
- Things to remember about avoiding risks include:
  - Avoiding risks may also mean avoiding opportunities
  - Not all risks can be avoided
  - Avoiding a risk in one part of the project may create risks in other parts of the project

Risk Management Planning

Risk	Avoid the Risk
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications.	Develop all software in-house. Switch to a subcontractor with a proven reliability track record even though they are more expensive.
The interface with the new control device is not defined and as a result its driver may take more time to implement then scheduled.	Negotiate with the customer to move the implementation of this control device into a future software release. Replace the selected control device with an older device that has a well-defined interface.

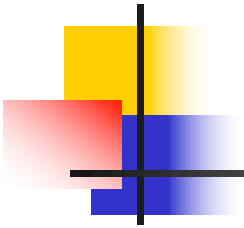


Risk Management Planning

- Do we know enough?
  - If we don't know enough, we can plan to "buy" additional information through mechanisms such as
    - prototyping,
    - modeling,
    - simulation, or
    - conducting additional research.

Risk Management Planning

Risk	Obtain Additional Information
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications.	Perform a capability assessment of the subcontractor. Ask for references from past customers and check on the reliability of previous products.
The interface with the new control device is not defined and as a result its driver may take more time to implement then scheduled.	Establish a communications link with device provider to obtain early design specifications for the device. Research interface specifications for other similar control devices by the same provider.



Risk Management Planning

- Can we transfer the risk?
  - If it is not our risk or if it is economically feasible to pay someone else to assume all or part of the risk, we can plan to transfer the risk to another organization.
  - For example we can contract with a disaster recovery firm to provide backup computer facilities that will allow continuation of the project in case a fire or other disaster destroys the project's work environment.

Risk Management Planning

Risk	Transfer the Risk
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications.	Transfer the risk to the subcontractor by building penalties into the contract for delivered software that does not have the required reliability.
The interface with the new control device is not defined and as a result its driver may take more time to implement then scheduled.	Transfer the risk to the customer by building additional charges to the customer and/or late delivery alternatives into the contract if the customer does not supply the specification by its due date.

Risk Management Planning

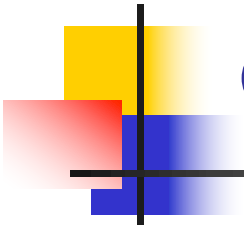
- Should action be taken now?
  - If we decide to attack the risk directly, we typically start with creating a list of possible risk reduction actions that can be taken for the risk.
  - Two major types of risk reduction actions should be considered:
    1. Actions that reduce the likelihood that the risk will occur
    2. Actions that reduce the impact of the risk should it occur
- These may include actions such as establishing a liaison with the customer to insure adequate communications, conducting a performance simulation, or buying additional equipment for the test bed to duplicate the operational environment.

Risk Management Planning

Risk	Control the Risk / Containment Plan
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications.	Assign a project engineer to participate in the requirements & design inspection and to conduct alpha testing at the subcontractor's site. Require defect data reports from the subcontractor on a weekly basis during integration and system test.
The interface with the new control device is not defined and as a result its driver may take more time to implement then scheduled.	Assign a senior software engineer who has experience with similar control devices to the design task. Move the design task later in the schedule and increase its effort estimate.

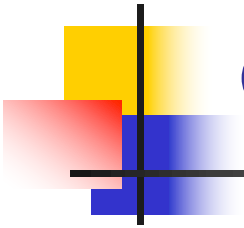
Risk Management Planning

- Contingency plan
  - If immediate risk reduction actions are not taken or if those actions reduce but do not eliminate the risk, it may be appropriate to develop risk contingency plans.
  - plans that are implemented only if the risk actually turns into a problem. Examples of contingency plans include disaster recovery plans, contacting a consulting firm to establish a fallback position if key personnel are not available, or selecting an alternative design approach if the new technology is not delivered as promised.



Cont…

- Each risk that has a contingency plan should also have a trigger.
  - A trigger is a time or event in the future that is the earliest indication that the risk will turn into a problem. For example, if there is a risk that outsourced software will not be delivered on schedule, the trigger could be whether the critical design review was held on schedule.
  - A trigger can also be a relative variance or threshold metric. For example, if the risk is the availability of key personnel for the coding phase, the trigger could be a relative variance of more than 10% between actual and planned staffing levels.



Cont…

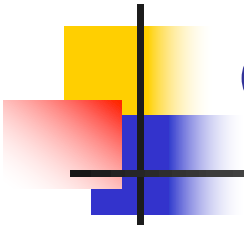
- There are trade-offs in utilizing triggers in risk management.
- We want to set the trigger as early as possible in order to ensure that there is plenty of time to implement risk reduction actions.
- We also want to set the trigger as late as possible because the longer we wait, the more information we have to make a correct decision and not implement unnecessary actions.

Cont…

Risk	Assume the Risk / Contingency Plans
The subcontractor may not deliver the software at the required reliability level and as a result the reliability of the total system may not meet performance specifications.	Risk Assumption: This is the best subcontractor for the job and we will trust them to deliver reliable software. Early Trigger (reassessment of risk indicated): Completion of Critical Design Review (CDR) later than June 1st. Contingency Plan Trigger: More that 2 critical and 25 major defects detected during second pass of system test. Contingency Plan: Assign an engineer to liaison with the subcontractor on defect resolution and implement our regression test plan for maintenance releases from the subcontractor.

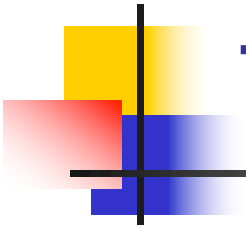
Cont…

The interface with the new control device is not defined and as a result its driver may take more time to implement then scheduled.	Risk Assumption: This new technology will greatly improve the usability of the system. We will assume that the interface definition will be available by the time we are ready to design the driver. Early Trigger (reassessment of risk indicated): Interface definition not received by start of Preliminary Design Review (PDR). Contingency Plan Trigger: Interface definition not received by start of CDR. Contingency Plan: Hold CDR with a "To Be Done" and hold a second CDR for just the subsystem that uses the device.



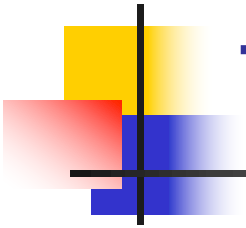
Cont…

- Adjusting the project plan:
  - Each selected action in the risk handling plans must include a description of the action and a list of tasks with assigned responsibilities and due dates.
  - These actions must be integrated into the project plan with effort and cost estimations.
- Project schedules must be adjusted to include these new actions.
  - For example, new tasks such as creating prototypes, doing research or conducting alpha testing at the customer's site must be included in the project plan.



Tracking

- Results and impacts of the risk reduction implementation must be tracked.
  - The tracking step involves gathering data, compiling that data into information, and then reporting and analyzing that information. This includes measuring known risks and monitoring triggers, as well as measuring the impacts of risk reduction activities.
  - The results of the tracking can be:
    - Identification of new risks that need to be added to the risk list.
    - Validation of known risk resolutions so risks can be removed from the risk list because they are no longer a threat to project success.
    - Information that dictates additional planning requirements
    - Implementation of contingency plan



Tracking

- Many of the software metrics typically used to manage software projects can also be used to track risks.
  - For example, Gantt charts, earned value measures, and budget and resource metrics can help identify and track risks involving variances between plans and actual performance. Requirements churn, defect identification rates, and defect backlogs can be used to track rework risks, risks to the quality of the delivered product, and even schedule risks.