Software Risk Management

Former US Deputy Assistant Secretary of the Air Force Lloyd Mosemann said:
“Software is so vital to military system that, without it, most could not operate at all. Its importance to overall system performance, and the generally accepted notion that software is always inadequate, makes software the highest risk item and must be steadfastly managed...Failure to address risk has been the downfall of many DoD acquisition programs. The system component with the greatest inherent risk has historically been software.”

Defining Risks and Problems

What is a risk? The state of being exposed to injury, pain, or loss

What is a problem? Something requiring thought and skill to arrive at a proper conclusion or decision

Risks and problems are not the same. Problems often arise from unmanaged risk

Risk Can Be Quantified

Risk is the probability of failing to achieve particular costs, performance, and schedule objectives, and the consequences of failing to meet those objectives.

Risk Exposure = Prob(Loss) x Size(Loss)

But precise quantification is difficult for software projects

Why Isn’t Software Risk Managed (or at Least Discussed)?

Our culture has evolved such that owning up to risks is often confused with defeatism.

Many managers will not admit that risk exists

Doing risk management makes good sense, but talking about it can expose you to legal liabilities. if a project fails, the existence of a formal risk plan...can compromise the producer’s legal position.

View of Tim Lister (*IEEE Software*, May/ June 1997)

To practice risk management:

- Identify your risks
- Determine the odds of each risk manifesting a prob-lem
- Estimate your exposure in the risks occur (time, money, effort spent)
- Determine which risks to manage
- Take action on risks you have control over
- Plan contingency for those beyond immediate action

But is Risk Management for Everyone? Views of Marvin Carr (*IEEE Software*, May/June 1997)

Effective risk management consists of two activities:

- Make informed decisions about risk
- Take appropriate action to minimize the effects of those risks

Why Risks are not Managed

As simple as it sounds, many organizations are unable to manage risks effectively for any of the following three reasons

- A risk-averse culture
- An inadequate infrastructure to support effective risk management
- A lack of a systematic and repeatable method to identify, analyze and plan risk mitigation

Acknowledging risk can cancel a project is forbidden.

Risk Aversion

A risk-averse culture rewards crisis management and punishes those who identify why the project might not succeed.

If executive management is averse to risk, that value permeates to all levels, so no one sounds an alarm when risk perceived

Deficient Infrastructure

Lack of an infrastructure makes risk management a one-shot activity, sometimes called “risk management season.” However, what management sees as risks are really problems needing attention. Thus, projects manage their Top 10 problems, rather than looking to future risks. When mitigation strategies are in place, they are usually abandoned during a crisis.

Systematic Infrastructure

Systematic methods ensure that:
All aspects f the project have been examined for risks
The project is periodically reexamined to identify new risks

This requires the culture be risk-aware at all levels

Implementing Risk Management (from E. Conrow and P. Shishido, *IEEE Software*, May/June 1997)

Recent survey of 365 respondents and 8,380 commercial software-intensive project indicated that 53%of the projects were “challenged:” They were over budget, behind schedule, or had fewer features and functions than originally specified, and 31% were canceled. Average cost increases were 189% and average schedule slippage was 222%. Completed projects had only 61% of planned functionality.

Risk Groupings

Project risk can be viewed along dimensions of:

- Project level
- Project attributes
- Management
- Engineering
- Work environment
- Other

Project Level Risk Factors

- Excessive, immature, unrealistic, or unstable requirements
- Lack of user involvement
- Underestimates of project complexity or dynamic nature

Project Attributes Risk Factors

- Performance shortfalls (includes errors and quality)
- Unrealistic cost or schedule (estimates and/or allocated amounts)

Management Risk Factors

- Ineffective project management (multiple levels possible)

Engineering Risk Factors

- Ineffective integration, assembly and test, quality control, specialty engineering, or systems engineering (multiple levels possible
- Unanticipated difficulties associated with user interfaces

Work Environment Risk Factors

- Immature or untried design, process, or technologies selected
- Inadequate work plans or configuration control
- Inappropriate methods or tool selection or inaccurate metrics
- Poor training

Other Risk Factors

- Inadequate or excessive documentation or review process
- Legal or contractual issues (such as litigation, mal-practice, ownership)
- Obsolescence (includes excessive schedule length)
- Unanticipated difficulties with subcontracted items
- Unanticipated maintenance and/or support costs

Sources of Project Risk - 1

- Using a performance-dominated requirements generation process that begins before you formally start the development process
- Starting a project with a budget and schedule that is inadequate for the desired performance level
- Using performance-driven design and development process
- Establishing a design that is near the feasible limit of achievable performance

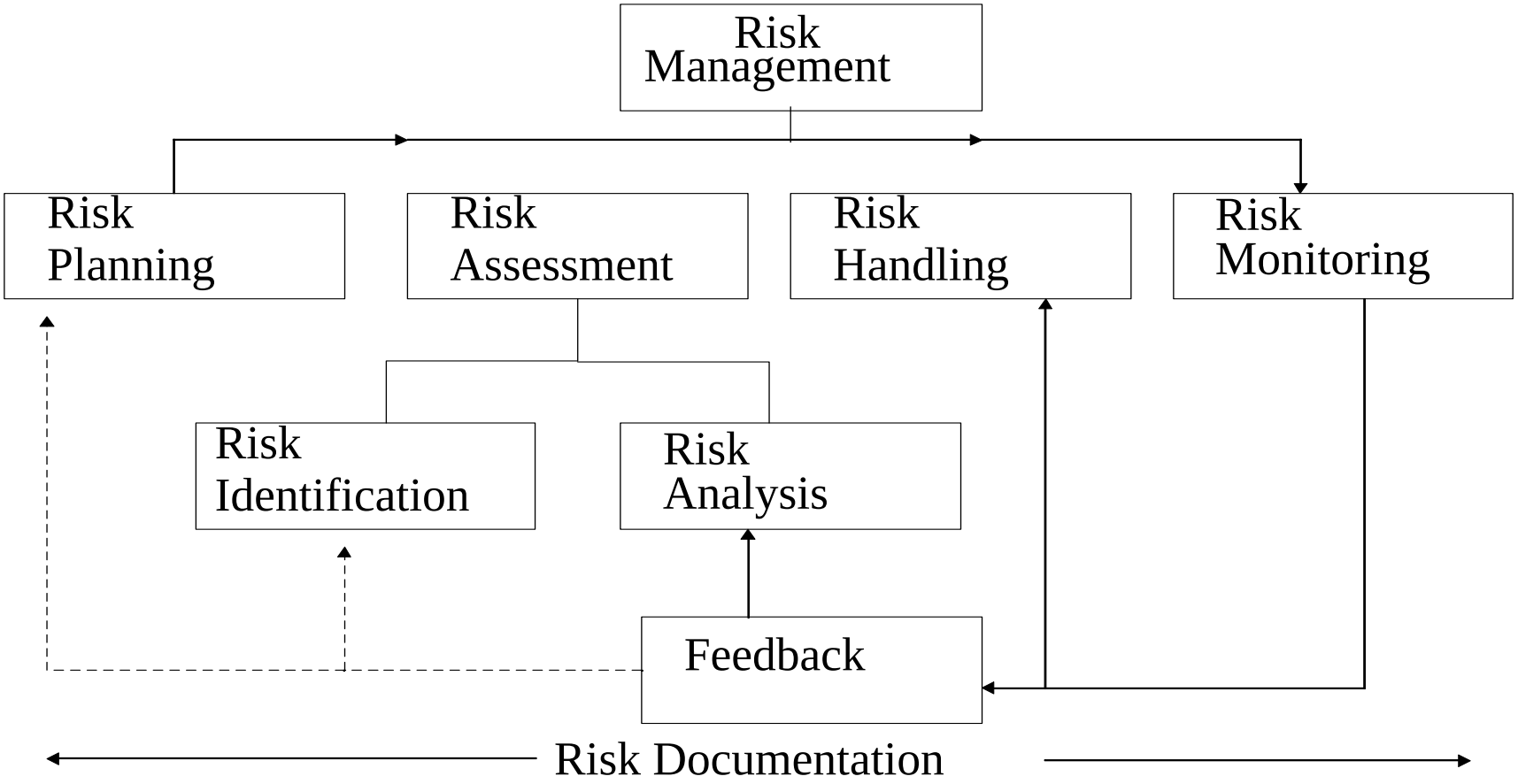
Sources of Project Risk - 2

- Being overly optimistic in assessing the limits of performance achievable for a given budget and schedule
- Making major project design decisions before the relationships between cost, performance, and schedule is understood

Results of Risk Sources

- Each of these items generally contributes to
- Overoptimism in establishing and estimating adequate project costs and schedule
- Underestimation of cost and schedule risk
- An eventual increase in project cost and schedule during development

Risk Management Paradigm



Recognizing and Controlling Risk

Establish a Risk Review Board (RRB) led by the project manager. Representatives from each of the functional and support areas. Risks are documented and include a short description of the risk type (cost, schedule, technical); severity (low, moderate, high); risk management plan; and status of risk mitigation activity.

Underlying steps are: Identification, Assessment, Mitigation planning, and Status and Control

Risk Management: Moving Beyond Process (A. Gremmer, *IEEE Computer***, May 1997)**

Effective risk management requires obtaining functional behavior, not just following a process or having diverse sources of information.

Successful risk management involves three elements:

- Repeatable process
- Widespread access to adequate knowledge
- Functional behavior

Why Functional Behavior?

Some people think functional behavior follows naturally from the first two elements. This is a fallacy. Following repeatable processes may mean we are just systematically managing risk poorly. Having adequate sources of information doesn’t mean people use them correctly

Cultural Rules/Observed Behaviors - 1

- View each person’s decision-making capability as invariant - Don’t forget people’s failures
- View uncertainty as negative Believe the team can’t fail
- Don’t ask for information - Shoot the messenger
- Don’t bring forward risks or problems without solutions - Expect problems or risks to be already solved
- Be risk averse - Don’t make decisions until the outcome is guaranteed

Cultural Rules/Observed Behaviors - 2

- Make decisions based on emotion, not logic - Don’t reach closure on difficult issues
- Make commitments without determining the probability of success - Always plan for the best-case scenario
- Be reactive - “I’ll deal with it when it happens”
- Reward heroes - Reward hard work, not smart work; glorify the comeback

Functional Behaviors - 1

- Manage risk as an asset
- Treat decision-making as a skill that can be taught
- Create a pull for risk information--actively seek it
- Seek diversity in perspectives and information sources
- Minimize uncertainty in time, control, and information
- Recognize and minimize bias in perceiving risk
- Plan for multiple futures--best case, worst case, and likely case

Functional Behaviors - 2

- Be proactive - Act before things go wrong
- Make timely, well-informed decisions and commitments
- Reward those who identify and manage risk early, even if the risks become problems

Risks, Opportunities, and Problems

A **risk** is the probability of unwanted consequences of an event and decision

An **opportunity** is the probability of exceeding expectations. A risk is the probability of failing to meet expectations

A **risk** is **not** a **problem**. A risk is a potential problem over which we have some choice.

Discuss Risk Intelligently

- Distinguish between risks, opportunities, and problems
- Distinguish between uncertainty and probability
- Make explicit the causes of risks (uncertainty in time, control, or information)
- Detail the characteristics of a risk (probability, impact, time frame, and coupling)
- Devise a strategy for dealing with the risk (mitigate, avoid, transfer, accept)

Causes of Risks

Uncertainty in Time - Uncertainty about when certain evens may occur or the ability to react to them

Uncertainty in control - Inadequate authority to make or influence decisions

Uncertainty in information - Inadequate or inaccurate information on which to base decisions

Characteristics of Risks - 1

Impact - The nature and magnitude of a risk's consequences

Probability - The likelihood that a risk's consequences will be realized if the risk is allowed to continue

Time frame - The time during which the team can exercise proactive choices associated with a risk

Characteristics of Risks - 2

Coupling - The effect a risk’s consequences would have on other risks or opportunities

Uncertainty - Lack of understanding about the nature of a risk’s probability distribution function or how it may vary over time

Risk-Handling Strategies

- Mitigate - Reduce the probability ad/or impact of the risk
- Avoid - Eliminate the possibility of a specific risk by choosing an alternative path. May mean swapping one risk for more acceptable ones
- Transfer - Get someone else to share or assume the risk
- Accept - Plan a contingency, track the risk, and enact if it becomes a problem

Formal Risk Management (from T*he Program Manager's Guide to Software Acquisition Best Practices)*

Formal risk management requires corporate acceptance of risk as a major consideration for software program management, commitment of program resources, and formal methods for identifying, monitoring, and managing risk.

Risk Management Essentials - 1

- Identify risk
- Decriminalize risk
- Plan for risk
- Formally designate a risk officer (senior person)
- Include in the budget and schedule a calculated Risk Reserve Buffer of time, money, and other key resources
- Compile a database of all non-negligible risks
- Prepare a profile of each risk consisting of probability and consequences

Risk Management Essentials - 2

- Include risks over full life-cycle (not just your watch)
- Do not expect to avoid risk actualization
- Keep risk resolution and workarounds off the critical path by identifying and resolving risk item as early as possible

Risk Management Essentials - 3

- Provide frequent Risk Status Report to project management that include:
- Top ten risks
- Number of risk items resolved to date
- Number of new risk items since last report
- Number of risk items unresolved
- Unresolved risk items on critical path
- Probable cost for unresolved risk vs. risk reserve