Risk Management in Software Engineering

An overview of technology and its practice

Jyrki Kontio

Nokia Telecommunications jyrki.kontio@nokia.com	Helsinki University of Technology http://wwwseg.cs.hut.fi	R & D-Ware Oy http://www.rdware.com

Main Messages

- Ad hoc risk management is not enough
- Risk is an abstract and subjective concept, communicate clearly
- Most current risk mgmt approaches have
- overhead
  - u plus, it is easy to start with small steps

Risky Business

- Any human endeavor is inherently risky
- Software development often involves
  - vague requirements
  - new technologies
  - new ideas or concepts
  - new personnel
  - changing situations and priorities
  - unrealistic plans
- ➡ Software development is particularly risky

.. but without risks there is no reward

Why Manage Risks?

- All projects have risks and some risks will occur
- Risk management is an investment into the future:
  - It is often cheaper to avoid a potential problem than fix an occurred one
  - If you only fix problems as they surface, the flow of future problems will continue to keep you busy
- It is important to know where the risks are to focus on essential areas in risk
- Intuitive risk management is seldom sufficient in complex, large projects
- Improve predictability and control of projects
- Consistent understanding of risks throughout the organization
- Learn from the risks that occurred

Obstacles to Risk Management

"If risk management is so hot, how come hardly anyone is using it?"

- Difficult (impossible?) to measure success in risk management
- Risk management is new, people do not know the possibilities
- Risk is an abstract phenomenon, it is difficult understand
- Some organizations have an internal culture that supports risk taking and discourages analytical approach to risk.
- Most project managers do manage risks but do not make it an issue.... but maybe they should?
- Most organizations do not even have their management act together ("chaotic processes")

What is Risk?

"We don't have a lot of experience in GUI" "Requirements are unstable"
"Excessive time may be spent on GUI development" "Requirements may change"
"We may have to rework the GUI" "Extra development effort may need to be spent due to requirements change"
"Project may be late and over budget"
"There is a 50% risk that Joe will quit before system testing phase"
"The use of CASE tool XXX is a risk in the project" "It would be a risk to deliver the prototype too early"

What is Risk?

"We don't have a lot of experience in GUI" "Requirements are unstable"	*Things that contribute to risk* **Risk factors**
"Excessive time spent on GUI development" "Requirements change"	*Things that happen* **Risk events**
"GUI reworked" "Extra development effort due to requirements change"	*Consequences of things that happened* **Risk outcomes**
"Project may be late and over budget"	*Effects of things that happen on valued characteristics* **Risk effects on goals**
"There is a 50% risk that Joe will quit before system testing phase"	*Probabilities of things that could happen* **Risk event probability**
"The use of CASE tool XYZ is a risk in the project" "It would be a risk to deliver the prototype too early"	*Anything associated with risk* **Action, person or object that is associated to risk**

What is Risk

Are these risks?

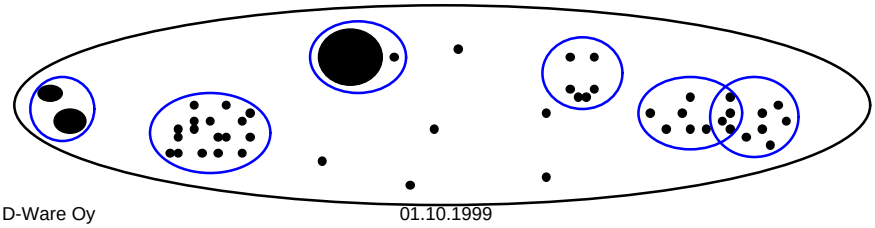
- Frequent, but uncertain small problems (e.g., some days will be lost to sick leave)
- Almost certain events (e.g., some requirements will change)
- Risks that do not effect your project (e.g., HW budget is exceeded)

Technically yes, but..

- Too minor to receive special focus, to be managed by "normal" management
- consider them problems
- delegate them to someone else

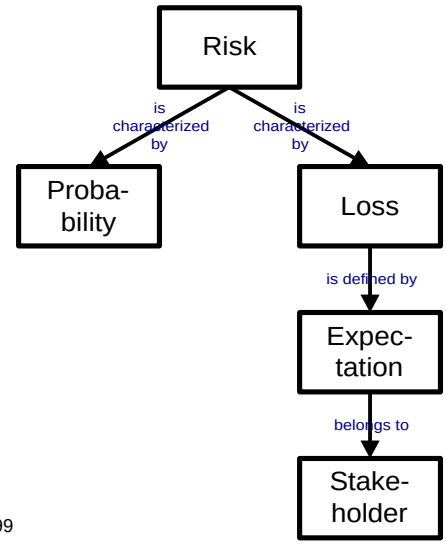
Levels of Abstraction and Risk

- There is an indefinite number of possible future outcomes
  - All of them cannot be modeled
- What is the right level of abstraction
  - "John will quit on Friday 13th at 13:13 hrs"
  - "something goes wrong in the project"
- **A key in risk management is to find right abstractions of future outcomes:**
  - detailed enough to provide focus
  - general enough so that their volume does not overwhelm you



Goals and Stakeholders

- From the concept of loss two additional attributes can be derived:
  - **goals** or expectations: without them the definition of loss is vague or does not exist
  - **stakeholder**: goals and expectations are associated to some interested party, a person or an organization
- The Riskit method uses more precise terms to decompose risk into different elements

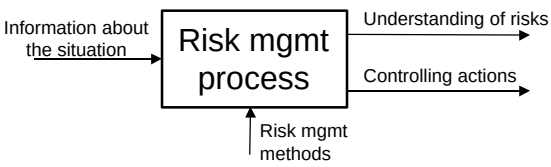


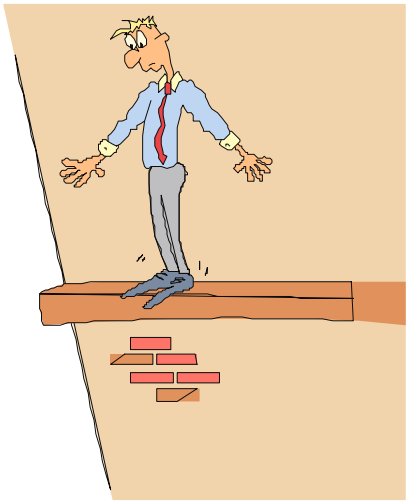
Definitions of Probability

- Classic probability
  - u Future outcomes are decomposed into atomic, equally probably components
- Frequency-based probability
  - u Ratio of a certain event in an infinite series of identical trials
- **Subjective probability**
  - u A person's subjective belief of the likelyhood of an event occurrence

Risk Management

- ***Risk management*** refers to a systematic and explicit approach used for identifying, analyzing and controlling risk.
- The risk management process produces two main outputs:
  - u Understanding about risks
  - u Controlling actions



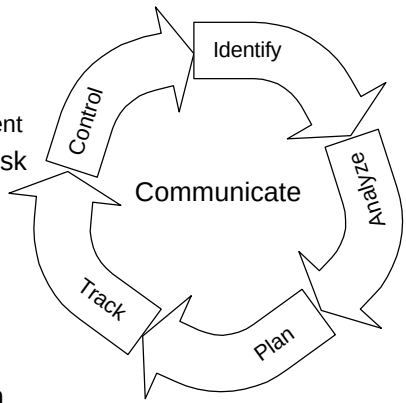


Main Risk Management Approaches

- Barry Boehm's risk management tutorial and spiral model, late 1980's
- Charette's risk management books and risk helix model, late 1980s to early 1990's
- SEI's risk management methods: risk taxonomy and guidebook, 1990's
- Hall's risk management principles, 1998
- Increased industry awareness and improved practice

SEI's Risk Management Approach

- The Software Risk Evaluation Method
  - u The risk taxonomy model
    - – a questionnaire for risk assessment
  - u A complete, defined process for risk management
  - u Team risk management
- Mainly targeted for initial risk evaluation but can also be applied on continuous basis
- A database of risk identification results has been collected



SEI's Continuous Risk Management

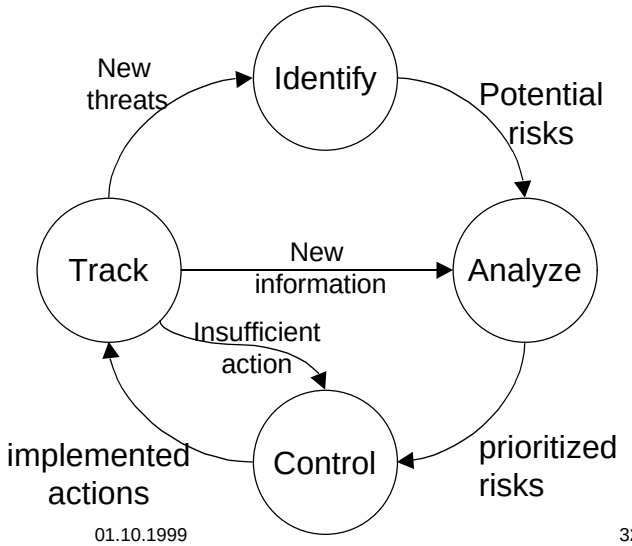
- Contains detailed process, guidelines and techniques
- A portfolio of of techniques for
  - brainstorming and teamwork
  - structuring information
  - documenting risks
  - analyzing and prioritizing risks
- Open issues
  - Does not discuss underlying assumptions and limitations
  - May lead to large risk management processes

SEI's Team Risk Management

- Main principles
  - Shared product vision
  - Effective teamwork through a defined process
  - Integrated into the continuous risk management process
- Open issues with SEI's team risk management
  - What if a shared product vision cannot be reached?
  - Hidden agendas and confidential targets?
  - Different priorities and objectives?

A Generic Risk Management Process

Practically all risk management methods have a similar generic process model



Risk Identification

- Identification of potential threats
- Needs to be done frequently
- Requires a different mental attitude:
  - not problem solving but free association

Techniques:
- brainstorming
- checklists
- questionnaires
- history data (lessons learned, data)
- critical path analysis
- goal review

Risk Identification Checklists

- SEI Taxonomy (Carr et al. 1993)
  - a comprehensive checklist with a questionnaire
- VTT survey (Laitinen et al. 1993)
  - a survey done in Finland, definitions normalized
- Barki's survey (1993)
  - 35 risk variables and their impacts
- Moynihan's personal risk constructs
  - How experienced project managers identify risks
- Capers Jones (1994)
  - Describes 60 most common risks
- Ropponen's survey (1993)
  - Survey/interviews in Finland

 01.10.1999 34

A. Product Engineering
- **1. Requirements**
  - a. Stability
  - b. Completeness
  - c. Clarity
  - d. Validity
  - e. Feasibility
  - f. Precedent
  - g. Scale
- **2. Design**
  - a. Functionality
  - b. Difficulty
  - c. Interfaces
  - d. Performance
  - e. Testability
  - f. Hardware Constraints
  - g. Non-Developmental Software
- **3. Code and Unit Test**
  - a. Feasibility
  - b. Testing
  - c. Coding/Implementation
- **4. Integration and Test**
  - a. Environment
  - b. Product Integration
  - c. System Integration
- **5. Engineering Specialties**
  - a. Maintainability
  - b. Reliability
  - c. Safety
  - d. Security
  - e. Human Factors
  - f. Specifications

B. Development Environment
- **1. Development Process**
  - a. Formality
  - b. Suitability
  - c. Process Control
  - d. Familiarity
  - e. Product Control
- **2. Development System**
  - a. Capacity
  - b. Suitability
  - c. Usability
  - d. Familiarity
  - e. Reliability
  - f. System Support
  - g. Deliverability
- **3. Management Process**
  - a. Planning
  - b. Project Organization
  - c. Management Experience
  - d. Program Interfaces
- **4. Management Methods**
  - a. Monitoring
  - b. Personnel Management
  - c. Quality Assurance
  - d. Configuration Management
- **5. Work Environment**
  - a. Quality Attitude
  - b. Cooperation
  - c. Communication
  - d. Morale

C. Program Constraints
- **1. Resources**
  - a. Schedule
  - b. Staff
  - c. Budget
  - d. Facilities
- **2. Contract**
  - a. Type of contract
  - b. Restrictions
  - c. Dependencies
- **3. Program Interfaces**
  - a. Customer
  - b. Associate Contractors
  - c. Subcontractors
  - d. Prime Contractor
  - e. Corporate Management
  - f. Vendors
  - g. Politics

The SEI Risk Taxonomy

Checklists vs. Brainstorming

Checklists	Brainstorming
● Pros u Fast and easy to use u Standardize results u Cover a broad area u May prompt thinking new risks ● Cons u Cause fatigue u Do not encourage creativity u May be biased due to a different domain u Do not encourage finding situation specific risks	● Pros u Fast and easy to use u Leverages local expertise and insight u Keeps participants active u Develops commitment ● Cons u Require facilitation or training u Meeting dynamics may bias results u Dependent on participants experience

Risk Identification Guidelines

- Start with open brainstorming
  - u Learn and use an effective technique
- Perform focused brainstorming
  - u by project area, stakeholder, goal, technical area, etc.
- Use checklists to ensure sufficient coverage
  - u Use as discussion points
  - u May also be used after meeting to produce off-line risk lists
  - u **Accumulate your experience to customize your checklists !**

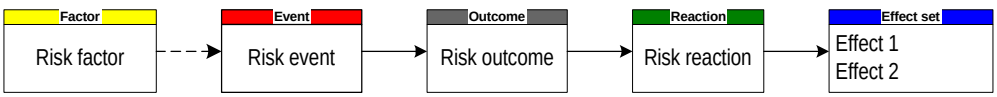
Risk Analysis

- Understanding (describing) risks
  - Risk tracking tables
  - Risk information forms
  - Visualization of risk dependencies
- Ranking of risks
  - Risk exposure (I.e., probability * loss)
  - Risk reduction leverage
  - Urgency

Understanding Risks: Riskit Analysis Graphs

Riskit Analysis Graphs

- Structure risk information
- Visualize links between risk elements
- Can link different risk scenarios and their interactions
- Can be used in textual form
- Can be used in a simple form or scale up when details are required



Risk Documentation Guidelines

- Templates standardize communications
- Use an approach that matches your needs
- Develop a path to refine the information
  - you often start with an abstract description and add details later
- Do not fill in information that you do not know: empty fields act as flags to others
- Archive past data
  - useful for learning from experience

Risk Prioritization

- Key attributes in prioritization:
  - Probability and loss determine how severe (=big) the risk is
  - Urgency indicates whether you still have time to wait
- Two main approaches for ranking risks:
  - Expected value of loss = prob(event) * loss(event)
  - Ranking through tables
    - ordinal rank multiplication
    - prearranged ranking tables for ordinal probability and loss estimates
    - risk factor ranking tables
- Both approaches have some problems ...

Expected Value Calculations

- Probability
  - In a changing environment the real probabilities of events are not only difficult to estimate, **they are unknowable**!
  - Probability is defined as *subjective probability*, a person's degree of belief that an event will occur
  - "Probability estimates are probably inaccurate, but that's all we've got"
- Ranking of losses is non-trivial
  - How to deal with multiple goal effects?
  - Use of direct metrics can lead to incorrect risk rankings

Let's Play a Game ...

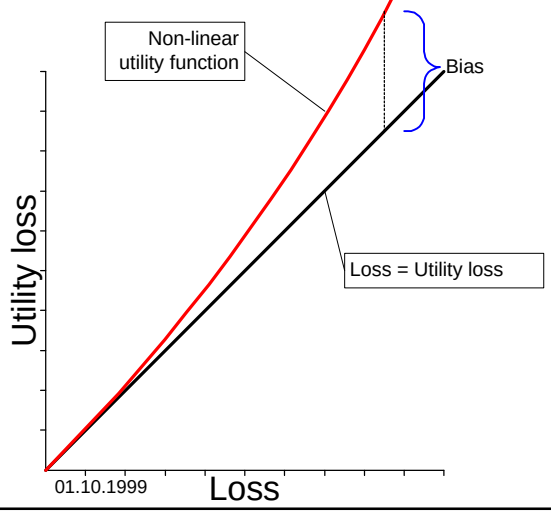
- You must choose between two gambles:
  - 100% probability of losing $20 — 100% * -$20 = -$20
  - 1% probability of losing $2,000 — 1% * -$2,000 = -$20

Will you play?

- How about this game:
  - 100% probability of losing $20 — 100% * -$20 = -$20
  - 1% probability of losing $1,900 — 1% * -$1,900 = -$19
- Last bid:
  - 100% probability of losing $20 — 100% * -$20 = -$20
  - 1% probability of losing $800 — 1% * -$800 = -$8

Utility Theory

- Expected loss cannot account for non-linear utility function
- Most fields assume non-linear utility functions
- Riskit evaluates expected utility loss



Risk Control Planning

- Two main steps
  - u Defining potential risk controlling actions
    - –what techniques can be used
  - u Selecting risk controlling actions to be implemented
    - –What strategies can be used in selection

Defining Risk Controlling Actions

- Brainstorming
  - u Open or focused
- Strategies (Hall, 1997)
- Checklists (Riskit)
- Risk element review (Riskit)
  - u analyze risk elements to identify what actions could be taken
- Experience
  - u Personal experience and insights

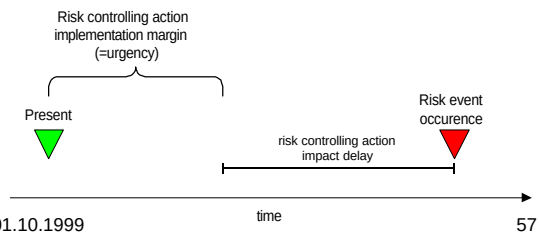
Acceptance
Avoidance
Protection
Reduction
Research
Reserves
Transfer

Selecting Risk Controlling Actions

- Control high-risk scenarios
- Effectiveness of risk controlling action

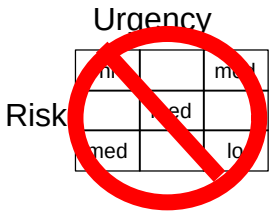
$$\text{risk reduction leverage} = \frac{\text{Expected utility loss}_{before} - \text{Expected utility loss}_{after}}{\text{Cost of risk controlling action}}$$

- Project constraints
- Stakeholder priority
- Urgency of risk controlling action



Dealing with Probability, Loss and Urgency

- Probability and (utility) loss characterize the magnitude of risk
- Urgency is a function of risk and controlling actions
- Urgency prompts a decision about a controlling action, it does not prioritize risks per se
  - è Risk & timeframe ranking tables are misleading



Conclusions on Risk Management Process

- Deploy a portfolio of techniques
- Be aware of assumptions and problems with various techniques
- The process itself is as important as the outputs
- Start simple and scale up and refine information as required

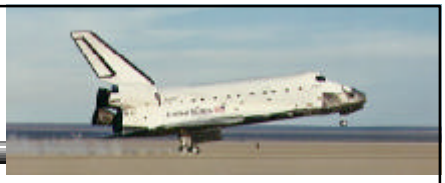
Levels of Risk Management

Invisible RM	There is no evidence of risk management activities taking place in projects, all risk management is intuitive and implicitly included in project management.
Ad hoc RM	Project managers occasionally perform risk management activities out of their own initiative.
Suggested RM	There are templates for documenting the output of risk management activities, such as a risk management section in the project plan or risk list section in project progress report. However, these sections are not required in actual plans or reports.
Required RM	The output of risk management activities is formally required and tracked from projects: a risk management plan is required and risk lists are frequently reported, updated and tracked.
Supported RM	There exists a defined process for performing risk management in an organization, including methods, tools, guidelines and supporting infrastructure.
Improving RM	There exists a systematic process for capturing risk management experience and improving risk management practices based on this experience.

Steps Towards Success: What Should You Do?

- Provide risk mgmt training to your project and line managers
- Make sure that your project plan templates have a detailed section on risk management (process, risks, actions)
- Make sure that your progress reports include a list of top n risks and their controlling actions
- Make sure that an explicit risk identification session is held for each project
  - Introduce brainstorming techniques
  - Find and customize a checklist
- Introduce a systematic method and support
- Enforce the process
- Accumulate experience

Summary



- Risk management will
  - avoid some, not all, of the potential problems
  - make participants understand project goals and risks more realistically
- Risk management needs to be supported to
  - guarantee that it is done frequently enough
  - maintain consistency in risk management
- Many existing approaches have built-in biases
  - they may work on practice but be aware of these limitations, some limitations are serious
- Select the methods according to your needs
  - start simple, gain experience
  - scale up as your needs and experience grows

Recommended Books

- Peter L. Bernstein. *Against the Gods*, New York:John Wiley & Sons, 1996.
- *Continuous Risk Management Guidebook*, Pittsburgh, PA:Software Engineering Institute, 1996.
- Elaine M. Hall. *Managing Risk: Methods for Software Systems Development*, Reading:Addison-Wesley Pub Co., 1998.
- Barry W. Boehm. *Tutorial: Software Risk Management*, IEEE Computer Society Press, 1989.
- Robert N. Charette. *Software Engineering Risk Analysis and Management*, New York:McGraw-Hill, 1989.
- Robert N. Charette. *Applications Strategies for Risk Analysis*, New York:McGraw-Hill, 1990.

Main References

H. Barki, S. Rivard, and J. Talbot, *Toward an Assessment of Software Development Risk* Journal of Management Information Systems, vol. 10, pp. 203-225, 1993.

V. R. Basili. *Software Modeling and Measurement: The Goal/Question/Metric Paradigm*. Computer Science Technical Report Series. College Park, MD:University of Maryland. CS-TR-2956, 1992.

B. W. Boehm. *Tutorial: Software Risk Management*, B.W. Boehm (Ed). IEEE Computer Society Press, 1989.

M. J. Carr, S. L. Konda, I. Monarch, F. C. Ulrich, and C. F. Walker. *Taxonomy-Based Risk Identification*, SEI Technical Report SEI-93-TR-006, Pittsburgh, PA: Software Engineering Institute, 1993.

R. N. Charette. *Software Engineering Risk Analysis and Management*, New York: McGraw-Hill, 1989.

C. Jones. *Assessment and Control of Software Risks*, Englewood Cliffs: Yourdon Press, 1994.

J. Kontio, *The Riskit Method for Software Risk Management, version 1.00* 1997. Computer Science Technical Reports. University of Maryland. College Park, MD.

Main References (cont.)

J. Kontio and H. Englund, *Experiences from an Exploratory Case Study with a Software Risk Management Method* 1996. Computer Science Technical Reports. University of Maryland. College Park, Maryland.

L. Laitinen, S. Kalliomäki, and K. Känsälä. *Ohjelmistoprojektien Riskitekijät, Tutkimusselostus N:o L-4*, Helsinki: VTT, Tietojenkäsittelytekniikan Laboratorio, 1993.

F. W. McFarlan, Portfolio approach to information systems, *Harvard Business Review*, vol. pp. 142-150, 1974.

T. Moynihan, How Experienced Project Managers Assess Risk *IEEE Software*, vol. 14, pp. 35-41, 1997.

G. Pandelios, T. P. Rumsey, and A. J. Dorofee, *Using Risk Management for Software Process Improvement*, 1996. Proceedings of the 1996 SEPG Conference. SEI. Pittsburgh.

J. Ropponen, *Risk Management in Information System Development* TR-3, 1993. Computer Science Reports. University of Jyväskylä, Department of Computer Science and Information Systems. Jyväskylä.

W. D. Rowe. *An Anatomy of Risk*, New York: John Wiley & Sons, 1977.