Risk Planning and Management

Farid Ahmadi

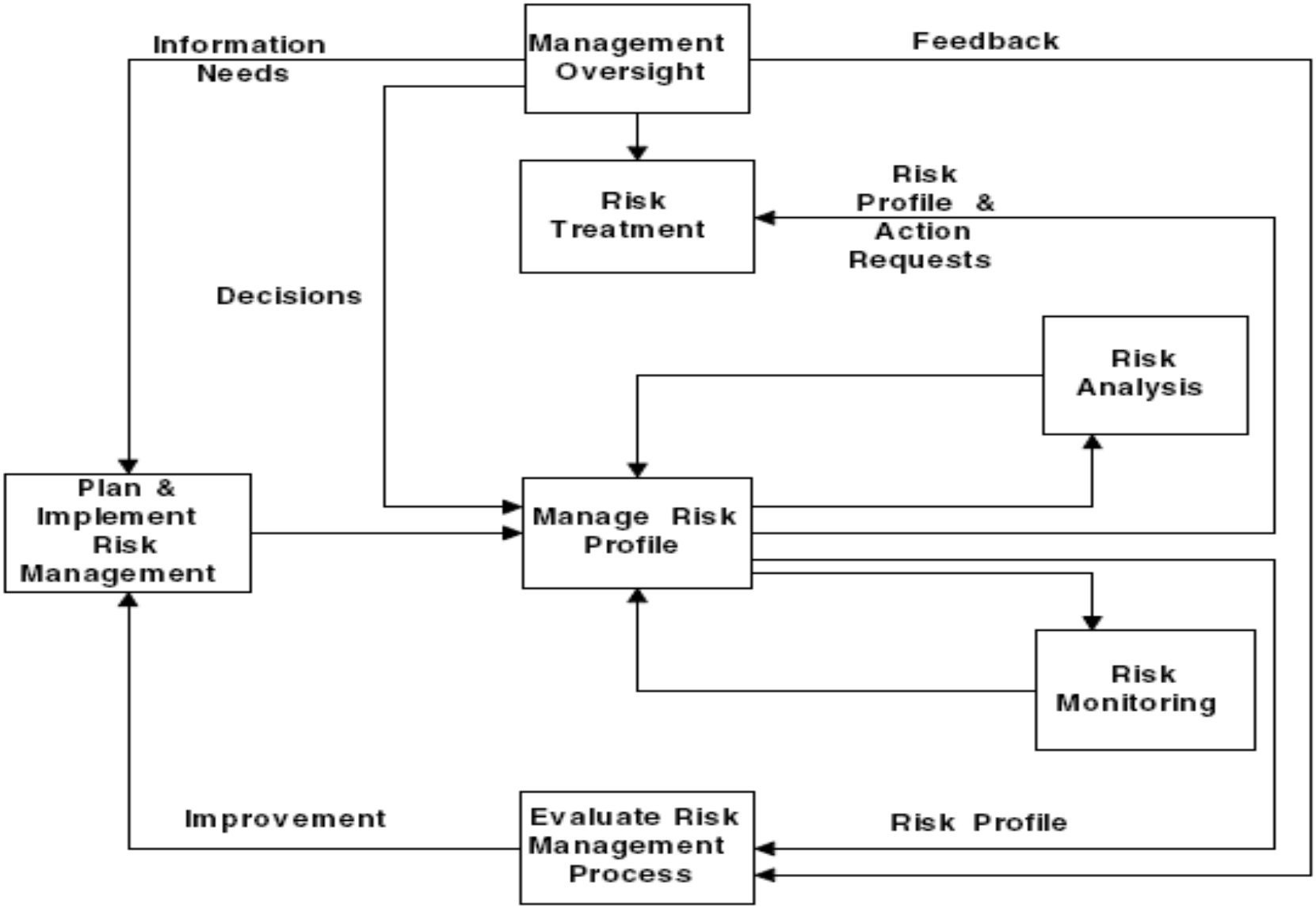
Risk

- Risk is the possibility of suffering loss. In IT, the loss may involve increased costs, longer completion times, reduced scope, reduced quality, reduced realization of proposed benefits, or reduced stakeholder satisfaction.
- *Risk and opportunity are different sides of the same coin. Some IT projects advance the state of the art, and as such are more risky than those that do not. The opportunity for significant advancement cannot be done without significant risk.*
- we must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunity.

Risk management standards

- The ISO/IEC 17799-1:2000 Code of Practice provides a sequencing of the risk management process into sub processes for context identification, risk identification, risk analysis, risk evaluation, and risk treatment.
- The IEEE 1540 standard on software risk management is being merged with the corresponding ISO/IEC standard. Figure shows the IEEE 1540:2001 overall risk management process.

IEEE 1540:2001 risk management process



Risk Management

As The Project Management Institute (PMI; 2000) Risk Management Processes are:

- Risk identification
- Risk quantification
- Risk response development
- Risk response control

Risk Management

- Risk management involves making plans and decisions in the face of uncertainty, and uncertainty is a state of nature, typified by the absence of information on a desired outcome.
- A *risk event is a particular occurrence that could affect a project for good or* bad.
- *Risk analysis is the combination of risk identification and risk quantification.*
- Therefore, *risk management is the processes involved with identifying, analyzing, and* handling risk. It includes maximizing the results of positive risk events and minimizing the consequences of adverse events.

Risk *context identification*

- Risk *context identification is a step in the ISO risk-management processes. This context* identification establishes the strategic, organizational, and risk-management environment.
- Context identification is made through familiar business models like:

  - *SWOT: Strengths, weaknesses, opportunities, threats*
  - *Context: Describes the system capabilities, as well as its goals and objectives and* the strategies that are in place to achieve them
  - *Target: Describes the goals, objectives, strategies, scope and parameters of the* activity, or system to which the risk management processes being applied
  - *Assets: Describes the identified assets and their dependencies*
  - *Security Requirements: Describes the security requirements needed to preserve* the identified assets

Risk Identification

- Ideally, risk identification should start during project initiation and should finish during project planning. In practice for IT projects, however, a risk analysis is typically done after project planning and before the final costing of the project.
- Risk identification cannot be fully completed until the WBS is created and most work, staff, and procurements have been specified. Then risks are further identified as the project proceeds and as change orders come in.

Risk identification

- Project critical success criteria and factors were discussed previously in this book. In a broader sense, risk identification should start with these critical success factors of the project. These factors can be used to identify critical sources of risks that may arise from our satisfaction criteria and completion criteria. The critical success factors were determined by considering all stakeholders for a project, and risk source identification should also consider all stakeholders.

Major risks in IT projects

- For large IT projects that will create products that will significantly change organizations (such as how business processes are performed and the "balance of power" within an organization), the major risks may involve satisfaction criteria more than the completion criteria.
- "Business based project failures come from such things as not having new workflow processes [to go with the new product], not adapting the structure of the organization to the new ways of working, not revising incentives and rewards to emphasize the new goals, and keeping the old cultural practices in place even when they impede the new ways of working"

Difference between a hazard and a threat

- *The threats posed to people by these hazards are death or injury from inundation, fire, heat, missile impact, lightning strike, and ash ingestion.*
- *The threats to infrastructure, lifelines, and property are destruction, damage, route obstruction, structural collapse, electrical malfunction, and pollution.*

The sources of risk

- Risks/hazards are often separated by such categories as:
  - *Business Risk: Risk of a gain or loss*
  - *Pure (Insurable) Risk: Risk of a loss only*

The sources of risk are further classified as:

- *Internal: Project variables (including managing the "normal" trade-offs in the* project schedule, cost, quality, scope) and other factors inside a organization
- *Technical: Technology uncertainty or change*
- *External: Factors outside of the organization*
- *Unforeseeable: Only 10% of risks fall into this category*

Internal and external risks

- Internal and technical risks are often quantified at the WBS level for projects, whereas external and unforeseeable risks are quantified at the overall project level.
- A PM is generally responsible for issues dealing with the customer are internal and technical types of risk events. Sometimes classified as external, and sometimes they are classified as internal depending upon whether the customer (benefiting organization) is internal or external to the company. The same situation may be true of procurement.

indicators of potential internal risks

- Some indicators of potential internal risks would be related to:
  - *Investment Size: Size of project cost versus budget of benefiting or performing* department (i.e., IT department)
  - *Project Size: Time length of project compared to "cycle" time in that industry*
  - *Impact Analysis: How broadly project results may impact organization, customers,* industry
  - *Business Risks: New corporate organization, merger, new employees, new vendors/*contractors
  - *Political Risks: Who internally cares about the project and their corporate* influence and power
  - *Performing Organization Risks: Staff and management uncertainties*

Technical risks

- Some technical risks in IT projects would possibly be:
  - New type of project
  - New area of application
  - New methodology
  - New technology (platforms, languages, tools, algorithms, methods, etc.)
  - New standards
  - “Going where no project in this company has gone before”

External and unforeseeable risks

- External and unforeseeable risks are not usually the responsibility of the PM. Unforeseeable risks include natural hazards (such as weather events, earthquakes, etc.), market fluctuations, riots, fires, crime, war, and the like. Only about 10% of risks are unforeseeable (PMI, 2000).
- Some indicators of external risks would be related to:

  - *Benefiting Organization (Customer) Risks: Management and contact uncertainties*
  - *Procurement Risks: Vendor issues*
  - *Political Risks: Those who externally cares about the project and their political* power
  - *Compatibility Risks: Alignment to current and new standards*
  - *Economic Risks: Flexibility to changes in local, national, and global economic* factors

standard industry checklist For risk identification

- One good way to start to identify risks is with a standard industry checklist or questionnaire. One such questionnaire from Pearlson and Saunders (2004) is:
- Are we doing the right things?
- Are project objectives clear?
- Will the proposed solution support business activities?
- What changes should be considered? • Are we doing it the best way?
- Have alternative ways been explored?
- Are there new or emerging ways we should consider?
- What changes would increase the likelihood of success?
- How do we know how we are doing?
- What are the performance standards?
- Is there regular progress reporting?
- How will the staff give feedback?
- What impacts are we having on the business?
- To what extent have project objectives been achieved?
- Are the project clients satisfied?
- Is satisfaction improving or declining?
- Is support for the project improving, stable, or declining?
- Is the project cost effective?
- What significant business costs are influenced by this project?
- What is the trend of these costs?
- What significant variances from budget have occurred?
- Is there clear accountability for the project?
- Are the right people involved?
- Are lines of responsibility clear?
- Is senior management supportive?
- Is performance monitored and on track?
- Do all those involved with the project understand their roles?
- Are key assets protected?
- Will the IT infrastructure handle the deployment of this application?
- Is IT security adequate?
- Are risks identified and monitored?
- How are incidents reported and analyzed?”

- A widely used checklist was given by Wideman (1992) who listed common general project risks and then specific risks by category: external unpredictable, external predictable, internal nontechnical, technical, and legal.

standard industry checklist For risk identification

- Sommerville (2003) identified common risks to software development: staff turnover, management change, hardware unavailability, requirements change, specification delays, size underestimation, CASE tool underperformance, technology change, and product competition.

Marchewka method

- Another way to identify risk is via a framework. One such framework, defined by Marchewka (2003), began by examining risks involving project scope, quality, or budget.
- It then viewed risk influences for these items in terms of people, legal, process, and so forth. It then considers whether the risk is internal or external, what is known about the risk(frequency and impact), and where in the project timeline the risk will occur:
- Scope
- Quality
- Schedule
- Budget
- People
- Legal
- Process
- Environment
- Technology
- Organization
- Product
- Other
- Internal
- External
- Known risks (frequency and impact known)
- K-U risks (frequency known, impact unknown)
- Unknown risks (frequency and impact unknown)
- Project conceptualization
- Charter and plan
- Execute and control
- Closeout
- Evaluation

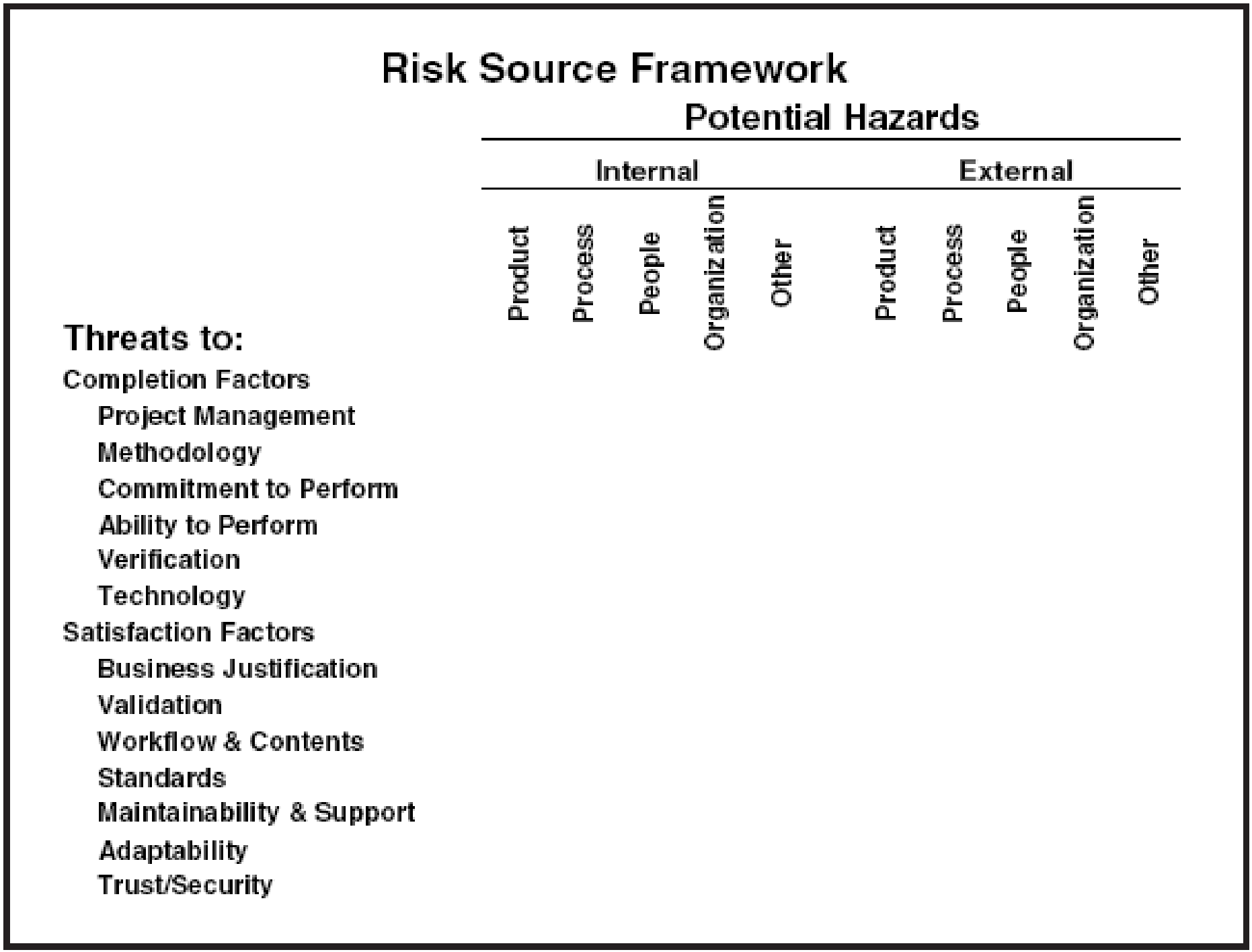
The IEEE framework

- The IEEE framework (taxonomy) is based upon identifying risk in three areas: product engineering, development engineering, and program constraints. Each category has subcategories, and each subcategory has specific areas (Carr, 1993):
- Product engineering
  - Requirements
  - Design
  - Code and unit test
  - Integration and test
  - Engineering specialties
- Development engineering
  - Development process
  - Development system
  - Management process
  - Management methods
  - Work environment
- Program constraints
  - Resources
  - Contract
  - Program interface

General Framework

- A more general framework suggested herein for IT projects is based upon the critical success criteria and factors introduced early in this book. Figure shows a template for this risk source identification template.
- Each cell in our framework table (intersection of a hazard and a threat) is a risk source arena. There may be more than one risk source in each cell. In practice, each cell is analyzed to identify sources of risk, and for each risk identified, a set of specific symptoms is listed. These symptoms are early warning signals that a risk event may be about to occur. Thus, the PM, project team, and line management can watch for these symptoms during the project execution.

Risk Source Framework



Risk Quantification

- After the risks and their symptoms are identified, those risks need to be quantified and the stakeholders' risk tolerance levels determined. The risk quantification process will result in a list of opportunities to pursue, threats to respond to, opportunities to ignore, and threats to accept.
- Risk quantification may utilize several models, including
  - *Hazard Frequencies: Describes frequency estimates for the identified hazards*
  - *Threat Frequencies: Describes frequency estimates for the identified threats*
  - *Consequence Estimates: Describes consequence estimates for the identified* hazards
- The formal analysis of risk includes the following risk factors:
  - The probability that the risk event(s) will occur
  - The economic impact (money at stake)
  - When the risk event(s) may occur (timing)
  - How often are they likely to occur (frequency)
- The first step in the analysis is determining the probability and impact. The two methods are commonly used are
- • *Qualitative: Expert opinion, project historical data, educated guess*
- • *Quantitative: Parametric formulas, simulation, industry and/or application statistical* data

EMV

- The most common quantitative method is the expected monetary value (EMV) calculation.
- Probability and impact are used to calculate the EMV as:

EMV = Probability * Impact

The impact is typically in money or person hours.

EMV

- A single impact number may be used in the previous formula, or the impact may be calculated from a maximum impact (total loss) times the probability of that maximum value (Pi):

  Impact = max Impact * Pi

- EMV = Pe * Pi * maxImpact (where Pe is the event probability)
- Calculation of management reserves involves summing up the EMV for all the identified threats and opportunities.

EMV determination

Risk/Opportunity	Impact	Probability	EMV
Threat 1			
…			
Threat N			
Opportunity 1			
…			
Opportunity N			
Total	-----	-----	**xxx**

less precise quantitative method

- A less precise quantitative method uses the base formula but expresses both impact and event probability on a scale (such as from 1 to 10) or as a rough percentage. This method, though less precise, may be more applicable, particularly in IT projects in which impact and probability are harder to estimate in an absolute sense.
- The impact for each risk is the fraction of the project overall budget that is directly affected by that risk. A relative EMV is calculated for each risk by multiplying the probability of the risk by the impact (amount of the budget at risk). The relative EMVs may be summed to calculate a management reserve for risk mitigation:
- Management Reserve = Σ Probabilityi * Impacti

SAPMLE

- For example, if there are two risks, and the first risk affects 50% of the project budget with a probability of 20%, and the second risk impacts 30% of the project budget, with an probability of 15%, then he management reserve would be 14.5%.

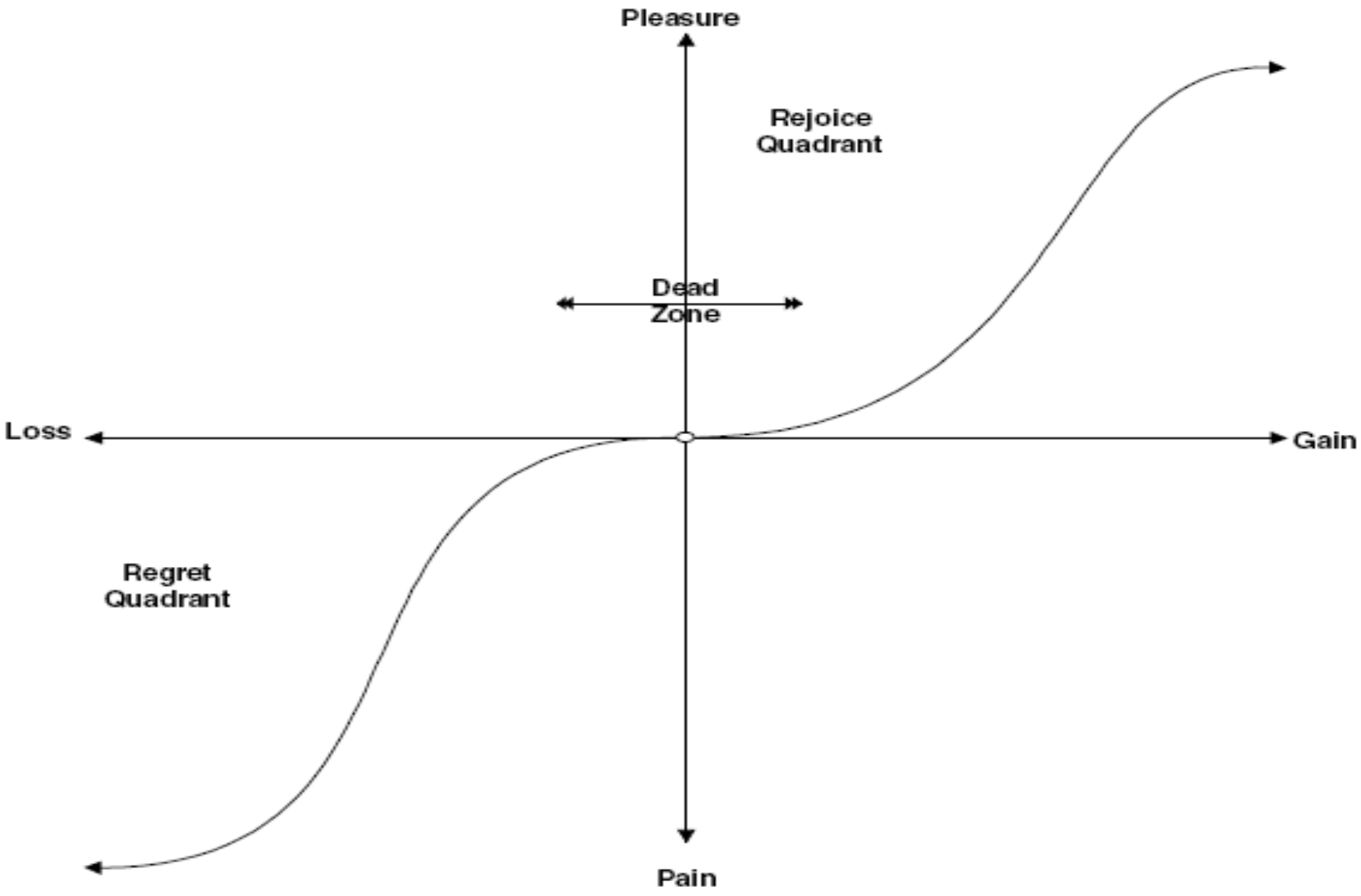
Risk grading

	Impact		
Probability	Low	Medium	High
Low	1	2	3
Medium	2	3	4
High	3	4	5

Risk utility function

- Piney (2003) defined different zones for the utility function graph that indicate different ways risks may need to be analyzed to determine stakeholder tolerance. The dead zone indicates threats and opportunities for which no response is developed. A table or spreadsheet may be prepared listing threats and opportunities for which responses need to be developed, as is shown in figure

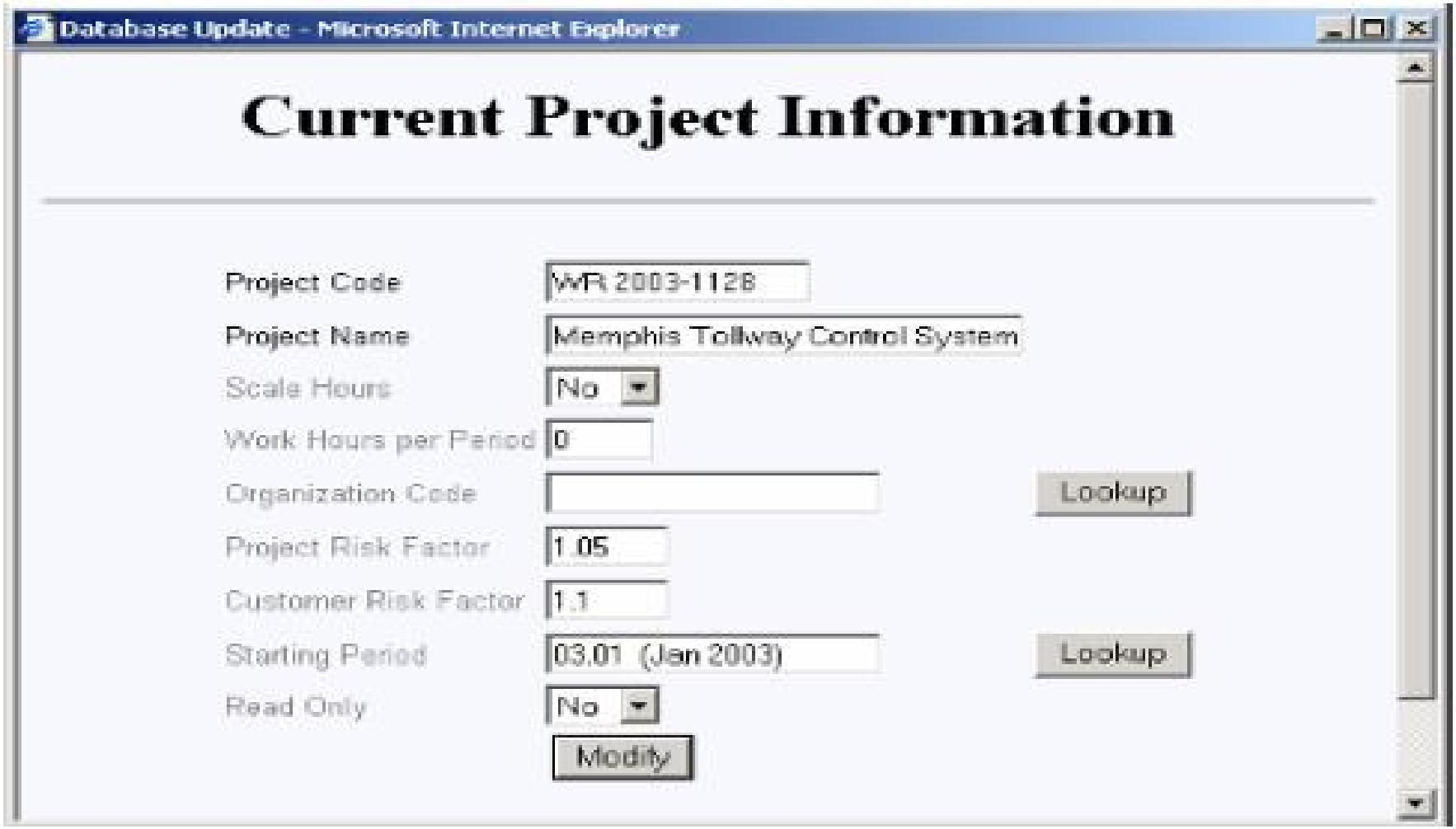
Risk utility function



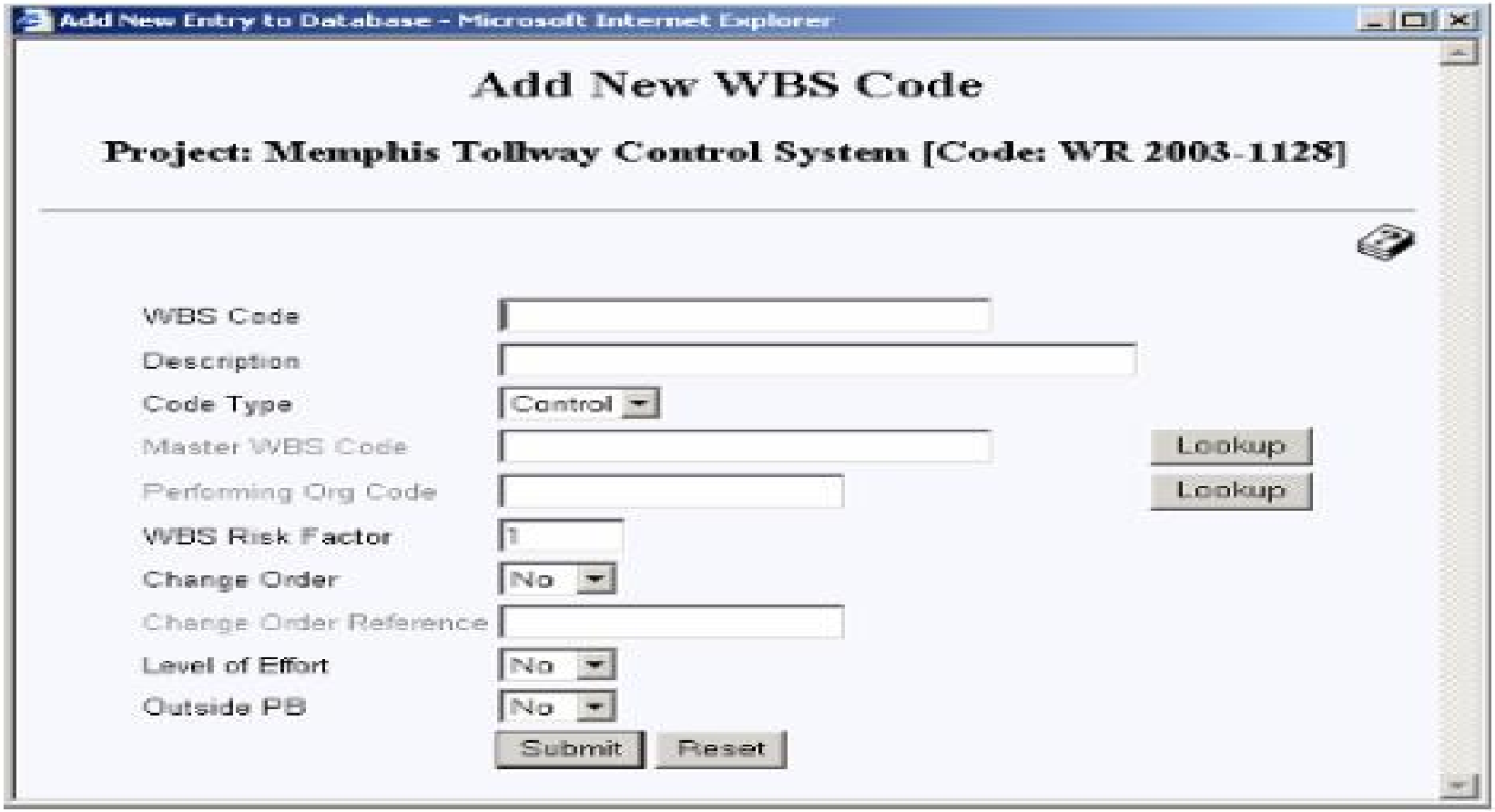
FiveAndDime

- Figure shows a screen from the FiveAndDime system that provides for project level risk factors for internal and technical risks (the project risk factor—how risky is this work) and for external risk (the customer—how risky [difficult] is this customer to work with).

Project form (showing project risk factors)



WBS form (showing WBS risk factor)



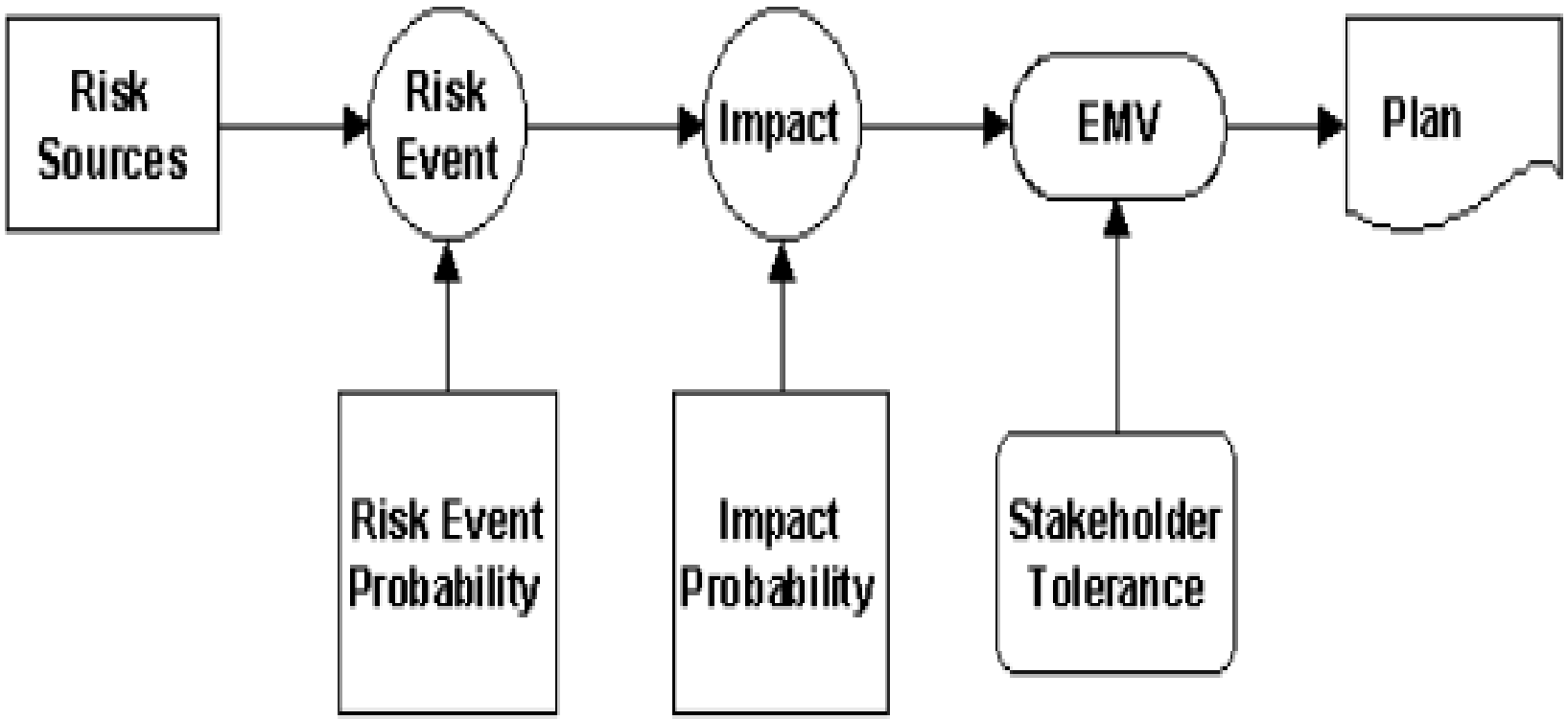
Risk Response Development

- Once the threats and opportunities have been categorized (opportunities to pursue, threats to respond to, opportunities to ignore, and threats to accept), the risk responses are formulated and the risk management plan is completed.
- The risk management plan usually specifies the overall management reserve. This is illustrated in Figure

Risk plan development

Risk/Opportunity	EMV	Priority	Respond ?
Threat 1			
…			
Threat N			
Opportunity 1			
…			
Opportunity N			
Total	**xxx**	-----	-----

Risk plan development



types of risk response

- There are several types of risk response plans (often called “mitigation strategies”):
  - *Avoidance: Eliminate the cause of the event(s) or reduce the EMV via reducing* probability
  - *Mitigation: Reduce the EMV via reducing the impact of the risk event*
  - *Acceptance: Accept the risk (take no preventive action)*
  - *Deflection: Assign (transfer) the risk to another party*

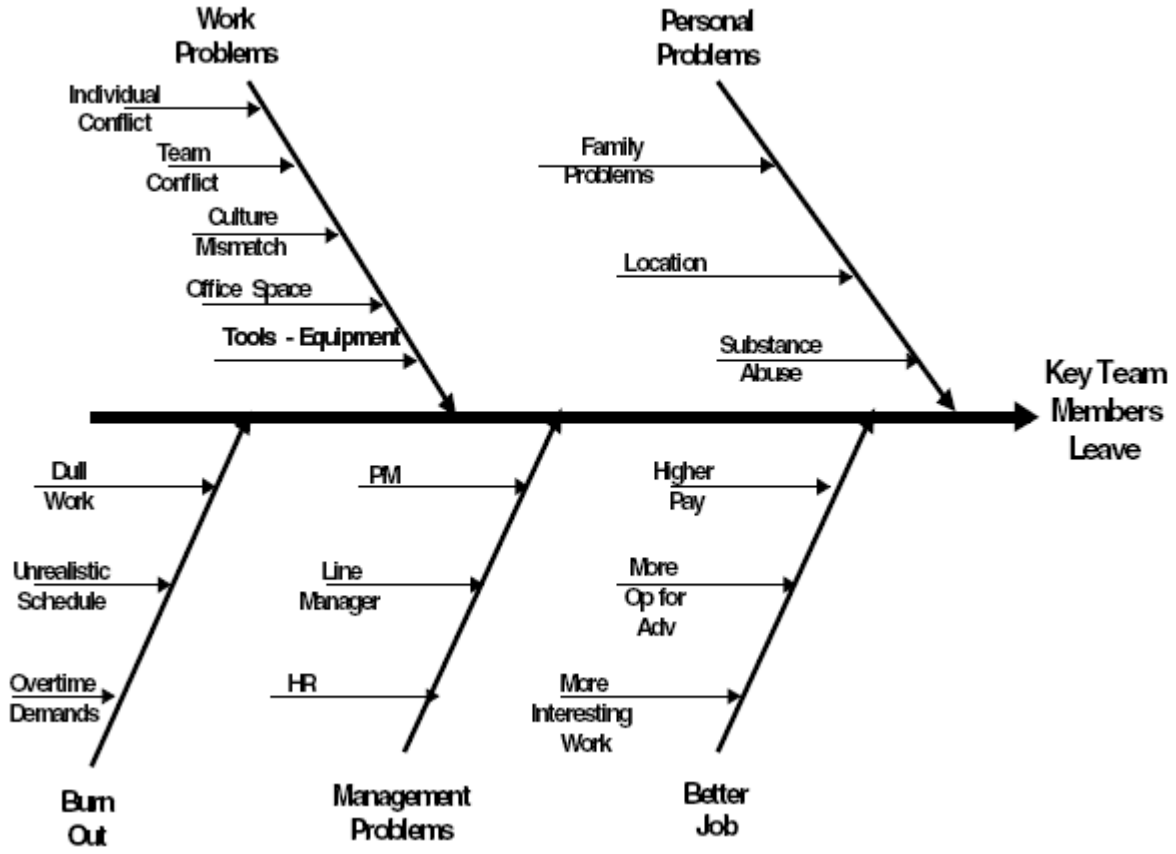
Avoidance

Avoidance reduces the EMV by reducing (or setting to zero) the probability. The main methods used here are safety- and prevention-related techniques, which are employed in the early stages of a project. Prevention measures are available for almost all IT risks and include such methods as employee retention and motivation incentives, buying parts of a system instead of building all of it, use of contract labor for no confidential parts of the system, parallel design and construction of alternative algorithms, platform, independent implementation techniques, use of open source software, using reusable components, and using object-oriented techniques.

Avoidance

For avoidance to be effective, one must identify the root cause of potential risk problems. One method is the Ishikawa Diagram (commonly called the *fish bone or cause-and-effect diagram), which is illustrated in Figure*

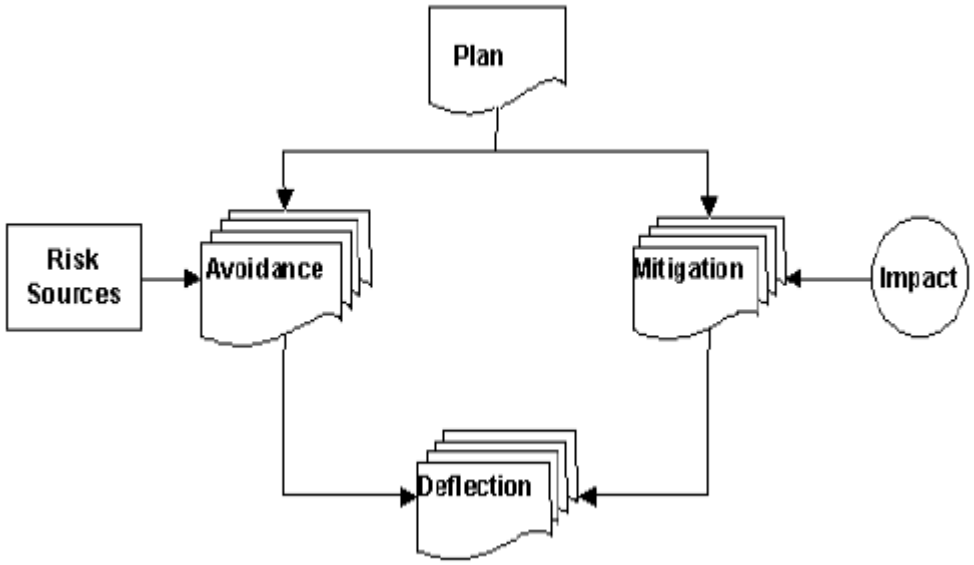
Cause and effect diagram



Mitigation

- Mitigation reduces the EMV by reducing the impact; these methods are:
- Contingency Plans: “Planned mitigation”; alternative means to do something
  - should a certain risk event occur;“contingency reserves”
- • Workarounds: A method devised to handle risk when the risk event happens
  - (“unplanned mitigation”)

Risk plan components



Deflection

- Deflection attempts to transfer the risk (part or all) to another party via:
  - *Insurance: Exchanges most of a risk of a probabilistic event(s) for a certain fixed* cost
  - *Outsourcing: Let someone more capable or experienced do the work*
  - *Procurement/Contracts: Buy/rent the needed expertise, equipment, material, software,* and so forth
- Deflection transfers and reduces the risk, but does not eliminate it.

outsourcing risks

there are considerable risks in outsourcing. Hallows (1998) lists such subcontractor risks as:

- Technical
- Competent resources not assigned
- Lack of familiarity with project or product
- Methodology not proven
- Poor project management techniques
- Technical disconnects due to distance of relationship
- Operational
- Subcontractor staff goes out on strike
- Subcontractor lands a higher priority project
- Distance leads to business and operational disconnects
- Transportation causes problems
- Customs causes problems
- Financial
- Subcontractor goes bankrupt
- Subcontract holds up deliverables due to contract or payment
- disagreements
- Subcontractor uses your schedule to extract extras
- Subcontractor reduces quality

- Jones (1994) lists the major risk factors (and a percentage of projects at risk) in contracting and outsourcing arrangements as:
  - High maintenance costs (60%)
  - Friction between contractor and client personnel (50%)
  - Creeping user requirements (45%)
  - Unanticipated acceptance criteria (30%)
  - Legal ownership of software and deliverables (20%)

Respond to outsourcing risks

These risks can be minimized by thoroughly qualifying the vendor, requiring the vendor to have the proper certifications, having the proper contract (with regard to terms, legal language, length, etc.), handling security issues, and requiring the vendor to report costs and progress using earned value methods

Risk	Avoidance	Mitigation
Incomplete requirements; Insufficient user involvement	Document clearly all requirements and get customer approval; utilize prototypes; make sure your analysts are talking to the right customer personnel; establish formal change control system	Involve users in documenting and approving requirements; use prototypes to flush out requirements; involve users with testing and documentation
Customer is difficult to work with	Assign higher risks and increase reserve; request customer management contact for conflict resolution; determine if the problem is with your personnel or customer personnel; have very good legal contracts	Document all customer interaction; frequently involve customer with requirement analysis, prototype review, design review, and test review
Lack of standard architecture	Obtain software engineering expertise; adopt standard architecture; adopt relevant IT standards; consider open source software	Depending upon depth into project, adopt and enforce relevant standards; use more prototypes
Inaccurate task estimating; Unrealistic task estimates	Use parametric estimation technique and compare with historical data and estimates by those who will do the work	Re-estimate remaining work if original estimate were not done in a quantitative manner and/or if multiple estimation techniques were not used; see cost overruns below
Inexperienced or poor PM	Set up apprentice PM program in organization; require PMI (or equivalent) certification for all PM's (for projects over a certain size); set up a PMO in organization	Project plans, controls, and issues reviewed by internal or external certified PM consultants; upper management review of PM choice
Insufficient staff; recruiting problems, staff illness	Prioritize requirements and phase project; use contract labor; outsource part of work; buy components	Use contract labor; outsource part of work; request extension from customer
Dependency on key team member(s)	Special recognition, position, incentives for these key persons; identify backup employees or contractors	Additional incentives to motivate the key members to stay thru project completion

Risk	Avoidance	Mitigation
Scope creep, requirements changes	Have user sign off on requirements and change order plan; contingency funds for unforeseen changes; more use of prototypes	Document all change requests; Prioritize requirements and phase project; Charge customer for changes and develop new baseline schedule and cost plan
Vendor problems (lateness, quality issues, etc.)	Have a formal procurement process that results in qualified vendors, good legal contracts, and a "win-win" situation for both buyer and seller	Negotiate issues with vendor and use whatever measures are available within your contract (see book chapter on procurement)
Cost overruns (not due to scope creep)	Use earned value metrics (see book chapter on performance measurement); employ multiple estimation techniques, employ PERT estimation	Voluntary uncompensated overtime, scope reduction, project phasing, buy components
Lateness (not due to scope creep)	Use earned value metrics	Crashing, fast tracking, contract resources, scope reduction, project phasing
Quality problems	Carefully set and enforce standards, utilize modern object oriented architectures, use proven technology, plan for thorough testing; use Quality Function Deployment (QFD) to involve customer; use extensive prototyping	Increase prototyping and testing, verify standards adherence, use QFD
Team problems: low productivity, burn out, low morale	HR to interview backups, identify contractors; "team building" measures	"Team building" measures; re-assign people to different tasks or projects; utilize backup personnel or contractors
Weak upper management support	Strong quantified business justification for project; thorough project charter signed off at high level in organization	Revisit business justification with upper management; seek other support in organization; regular reporting of project progress and cost

Risk	Prob.	Budget Impact	Relative EMV	Symptoms
Employee "burnout"	2	1	.02	Low Morale, lateness
Poor project management	1	5	.05	Lateness, cost overrun, earned value issues
Insufficient resources available	3	1	.03	Lateness, staffing problems
Employee turnover	2	1	.02	People leaving
Key programmers leave	2	4	.04	Key people leave
Scope "creep"	3	1	.03	Lateness (project level); additional scope
Task estimates are too low	2	3	.06	Lateness (task level), earned value issues (task levels)
Poor IT architecture choice	1	2	.02	Prototype time lengthens

Example risk plan

Risk	Response
Task estimates are too low	Closely monitor against actual costs to see if project needs to be phased or scope reduced
Poor project management	PM and team address specific issues, Upper Mgmt. involvement
Key programmers leave	Provide added incentives to key people to at least stay until project completion
Insufficient resources available	Phase project or request more $
Scope "creep"	PM steps in to "phase" project and deal with customer
Employee turnover	HR to interview backups, identify potential contractors
Employee burnout	Re-assign people to different tasks or projects
Poor IT architecture choice	Re-evaluate architecture choice, use more prototyping

Risk Response Control

- Risks need to be monitored continuously during the execution of a project by looking at the risk symptoms and seeing if any risk events have occurred or are about to occur.

stumbling blocks in risk management

- Rita Mulcahy (2003) listed the most common stumbling blocks in risk management:

- *Risk identification is completed without knowing enough about the project.*
- *Project risk is evaluated using only questionnaire, interview, or Monte Carlo techniques and thus does not provide a detailed, per task analysis of risk.*
- *Risk identification ends too soon resulting in a brief list (about 20) rather than an extensive list (hundreds) of risks.*
- *Risk identification and risk quantification are blended resulting in risks that are evaluated or judged when they come to light. This decreases the number of total risks identified and causes people to stop participating in risk identification.*
- *The risks identified are general rather than specific (e.g. communication rather than poor communication of customers needs regarding installation of system xxx caused two weeks of rework).*
- *Whole categories of risks are missed such as technology, cultural, or marketplace.*
- *Only one method is used to identify risk rather than a combination of methods. A combination helps ensure that more risks are identified.*
- *The first risk response strategy identified is selected without looking at other options and finding the best option or combination of options.*
- *Risks are not given enough attention during the project execution stage.*