Software Risk Management

1. Risk

- as a science was born in the sixteenth-century Renaissance, a time of discovery
- derives from the early Italian *risicare* means “to dare”.
- Games of chance led to the discovery of the theory of probability, the mathematical heart of risk.
- is defined as the possibility of loss
- is obtained by specifying values for the risk attributes of probability (the possibility/likelihood that the consequence will occur) and the consequence (the loss/the effect of an unsatisfactory outcome)
- is measured by multiplying likelihood times loss (Risk Exposure)
- are dynamic, change over time
- overlaps with other risks and is interrelated with other risks, henceforth, jointly affects a number of attributes of the project

2. Risk management

- had begun in the eighteenth century era of Enlightenment, a time of the search of knowledge and exploration of the unknown
- is a general procedure for resolving risks (risk management is said to resolve a risk if, when it is applied to any instance, the possible consequences are all acceptable)
- consists two major activities:
    - Risk assessment: defines the risk (discovery process of identifying sources of risk and evaluating their potential effects)
    - Risk control: resolves the risk (process of developing risk resolution plans, monitoring risk status, implementing risk resolution plans, correcting for deviations from the plan)
- goes beyond modern management theory, such as Total Quality Management (TQM) and Business Process Reengineering (BPR), because it is basic to decision making.
- is based on theories (Bayes theorem, Chaos theory, Creativity theory, Decision theory, Game theory, Portfolio theory, Probability theory, Uncertainty theory, Utility theory) that provide different strategies for decision making under probabilistic conditions.
- Must be performed regularly, iteratively throughout the life cycle of a software system

3. Software Risk

A measure of the likelihood and loss of an unsatisfactory outcome affecting the software project, process, or product

1. Software project risk:
    - defines operational, organizational, and contractual software development parameters
    - primarily a management responsibility
    - includes resource constraints, external interfaces, supplier relationships, contract restrictions, unresponsive vendors, lack of organizational support
    - Supposed lack of control over project external dependencies makes project risk difficult to manage
    - Funding is the most significant project risk reported in risk assessments
2. Software process risk:
    - includes both management and technical work procedures
    - in management procedures like planning, staffing, tracking, quality assurance, and configuration management activities, specially, planning is the most reported risk
    - in technical procedures like requirement analysis, design, code, and test activities, specially, development process is the most reported risk
3. Software product risk:
    - contains intermediate and final work product characteristics
    - primarily, a technical responsibility
    - in requirements stability, design performance, code complexity, test specifications activities
    - specially, requirements are the most reported risk

4. Software Risk Management

- is a practice of measuring and controlling risk that affects the software project, process, or product
- The basic concepts of software risk management are goal, uncertainty, loss, time, choice, make intelligent decisions, resolve risk, and prevent problems
- We begin with defining goals and objectives clearly, and then describing the risk in terms of uncertainty, loss, and time. Further, consideration of risk information helps to sort out their priorities and provides the knowledge to make intelligent decisions to resolve risks
- The risk resolution strategy is not only to minimize risk but to maximize opportunity, the chance of a good outcome also
- A proactive rather than reactive strategy is better to reduce the problem of costly rework

- As we progress towards the project, the probability of risk decreases, and the impact of risk increases over time.

5. Need for software risk management

- The ability to manage uncertainty on projects is a requirement designed to deal with scarce resources, advances in technology, and the increased demand for complex systems in a rapidly changing environment.
- Given the current business climate of shrinking profit margins, the global economy and its uncertain market conditions, and the competitive forces pressured by rapid technology advances, all of these leads to the very reason of software risk management.

6. Consequences of risk ignorance

- lack of skills to grapple/tackle with the risk
- lost opportunity to perceive/recognize risk
- suffer from mistakes and can't control risks
- pain of regret to learn and practice risk management

7. Major Factors in risk management capability

- maintain focus on the four critical success factors of risk management to manage risk successfully - people, process, infrastructure, implementation
- people participate in managing risk by implementing the risk management process according to the risk management plan
- process transforms uncertainty (the input) into acceptable risk (the output) through risk management activities
- infrastructure specifies how the organization requires the use of risk management on the projects by establishing policies and standards
- implementation is the plan and methodology used to perform risk management on a specific project

7.1. People factor and the risk

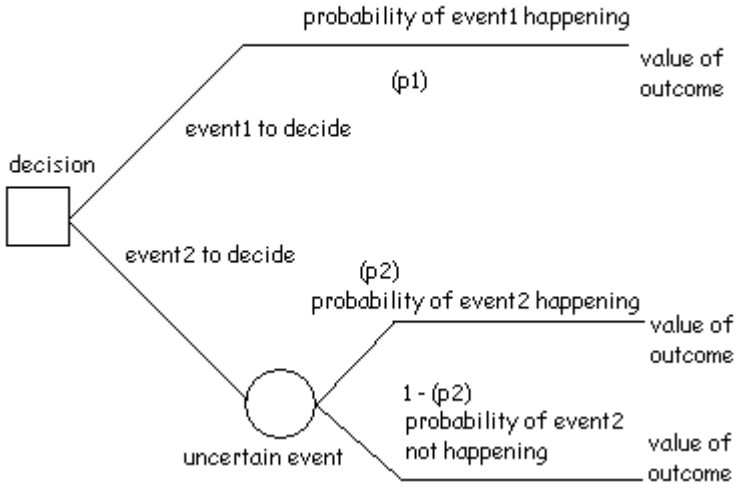
- involve people through participation at all levels in risk management activities
- develop the people's ability to manage risk by education, training and experience
- provide people's motivation for change must be sufficient to overcome the barriers to adopting something new
- individuals have risk preferences that you can use to predict their behavior

7.1.1. Driving forces for risk management adoption

- provides a focus on goals
- satisfies customer requirements
- increases visibility for high-risk areas
- promotes communication of risks
- provides for risk-aware decisions
- helps resolve difficult issues
- contributes to a more realistic plan
- helps avoid surprises
- helps prevent problems
- reduces rework

7.1.2. risk preference and decision tree

- risk preference is an attribute toward risk that varies among people in accordance with his/her nature
- decision tree is a tool to structure difficult decisions to understand the available options. The tree flows from left to right; the immediate decision is represented by the square at the left side. The branches emanating from the square correspond to the two choices available. The circle represents the chance event. The branches emanating from the circle represent the possible outcomes. The values of outcomes are specified at the ends of the branches in terms of risk exposure or expected value
- decisions are made based on risk preference (decision tree models one decision (the square) and one uncertain event (the circle)



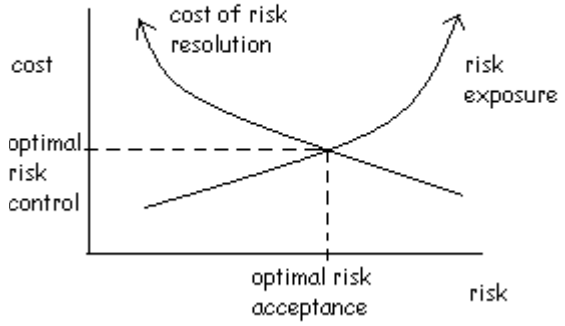
7.1.3. Risk Neutral people remain between Risk Averse and Risk Seeking

- risk averse people have conservative risk attitude with a preference for secure payoffs/benefits. The decisions are based on sensible and realistic grounds.

- risk seeking people have a liberal risk attitude with a preference for approximate payoffs/benefits. The decisions are based on optimistic and fearless attitudes.
- risk neutral people have unbiased/independent risk attitude with a preference for future payoffs. This means risk-neutral types are neither risk seeking nor risk averse, but rather seek strategies and tactics that have high future benefits. The decisions are based on the belief of long-term benefits

7.2. Process: the steps to manage risk

- set of activities and mechanisms that people use to transform inputs to outputs.
- there are five process elements in the risk management process -
    - identify risks and sources of risk,
    - analyze risks based on probability and consequence criteria,
    - plan the next task to resolve risk. Develop alternative strategies for risk resolution, define risk action plan, establish thresholds as standards to take action in case of deviations/variences from thresholds/standards.
    - track/monitor planned thresholds and risk status. Use triggers to provide early warning to implement the risk action plan while there is time to resolve the risk. Report risk estimates to take actions in case of deviation/variance from thresholds/standards.
    - resolve risk by responding to notification of triggering events, executing the risk action plan, and reporting results of risk resolution efforts until the level of risk is acceptable.
- the standard process is not one size fits all (for small and large projects), although it is valuable in terms of serving reusable component for organization (saving project schedule to write procedures again).
- the defined process should be flexible (tailored version of the standard process) to meet their individual needs.
- the process execution must be cost-effective to balance risk resolution and risk acceptance. We must weigh the cost of risk control against the expected loss without risk control. A risk increases, exposure to loss increases. Risk decreases with the cost of risk control. Overall cost and risk are minimized through cost-effective risk resolution by optimized risk management process.



7.3. Infrastructure: the organizational foundation

- is needed to establish a risk-aware culture
- four infrastructure factors describe the enterprise support required to manage risk:
  - organizational environment
  - requirements (minimum standard): like requirement guidelines (e.g., corrective action, contract review, development plan, design reviews)
  - required resources (investment): like budget, schedule, staff to be applied to resolve risk
  - results (return of investment (ROI = ratio of savings to cost that indicates the value provided)): analyze risk management costs and benefits
- affect/influence people's behavior through policy
- set expectations for project behavior

7.4. Implementation: risk management execution in project

- success begins with a high-quality risk management plan (consisting approaches like proactive actions, integrated risk management in project, systematic procedures, disciplined principles and methods) to manage risks
- projects have a unique personality that their methods reflect (choose methods that reflect a project's personality)

8. identify risks

the process definition steps for identifying risks are:

- define the risk identification process
- develop risk checklists
- define the risk assessment method
- develop the risk management form
- establish the risk database schema

8.1. define the risk identification process

- specifies the process controls, inputs, outputs, and mechanisms (external view)
- specifies the process activities that transform inputs to outputs using mechanisms (internal view)

8.1.1. Process Goals

- encourage input of perceived risk from the team
- identify risk while there is time to take action
- uncover risk and sources of risk
- capture risk in a readable format
- communicate risk to those who can resolve it
- prevent project surprise

8.1.2. Process Definition

identification of risk encapsulates the activities of the process that transform inputs to outputs.

- the process-controls regulate the process (project resources, project requirements, risk management plan)
- the process-inputs enter the process (uncertainty, knowledge, concerns, issues)
- the process-outputs exit the process (risk statement, associated risk context)
- the process-mechanisms support the process (risk checklist, risk assessment, risk management form, risk database)

8.1.3. Process Activities

are the tasks necessary to transform uncertainty into a risk statement:

- conduct risk assessment (identifies risk and evaluates risk based on established criteria e.g., likelihood of occurrence, consequence, and time frame for action)
- identify risk systematically (checklist, interview, meeting, review, routine input, survey, working group)
- define the risk attributes (probability, consequence)
- document identified risk (write risk statement, elaborate associated risk context using what, when, why, how, where of the risk issue)
- communicate identified risk (verbal, written)

8.2. develop risk checklists

- provide a systematic way to identify risk.
- you can discover unknown risks that exist on your project by reviewing the project's critical success factors, listing all items on the critical path of your schedule, and itemizing the project interface, internal and external.

8.2.1. software risk taxonomy

- SEI risk taxonomy (structured checklist that organizes known software development risks from general classes to specific element attributes, organized into three major classes - product engineering, development environment, program constraints)

8.2.2. Work Breakdown Structure (WBS)

- provides framework for identifying specific project risks
- more realistic risk identification in relevance to concerned project

8.3. define the risk assessment method

- interview-style method to identify and appraise risks
- the risk assessment objectives include training techniques for risk identification that used throughout the project and providing a baseline of assessed risks for continued risk management

8.3.1. Assessment preparation

- select and train the assessment team
- review the project profile
- select the interview participants
- prepare the risk assessment schedule
- coordinate the meeting logistics
- brief the project participants

8.3.2. interview session

- interview the peer group
- record the risks
- clarify the risk statements
- observe and document the process results

8.3.3. preliminary risk analysis

- evaluate the identified risks
- evaluate the interview session
- categorize the risks
- enter the risks in the risk database

8.3.4. Results and demonstration

- prepare the results briefing/meeting
- debrief/communicate the project manager
- brief/present to the project team
- evaluate the risk assessment
- distribute the risk management form

8.4. develop the risk management form

- used as a risk identification mechanism that anyone may submit at any time to identify risks.
- the originator enters his or her name, the date, and a brief description of the risk

8.5. establish the risk database schema

- risk database contains data fields to describe a risk completely
- the database design should include links to requirements and pointers to related risks

- risk database schema is the design of the fields for the risk database
- the risk database should contain at least these data fields (log number, date, status, originator, risk category, risk title, probability, consequence, time frame, project, phase, function, WBS element, risk statement, risk context, risk analysis, current priority, previous priority, risk resolution strategy, risk action plan, quantitative target, indicator, threshold, trigger, cost, savings)

9. Analyze Risk

9.1. define the risk analysis process

- specifies the process controls, inputs, outputs, and mechanisms (external view)
- specifies the process activities that transform inputs to outputs using the mechanisms (internal view)

9.1.1. process goals

- analyze risk in a cost-efficient manner
- refine the risk context
- determine the source of risk
- determine the risk exposure
- determine the time frame for action
- determine the highest-severity risks

9.1.2. process definition

encapsulates the activities of the process that transform inputs to outputs

- process controls (project resources, project requirements, and risk management plan) regulate the process
- process inputs (risk statement, associated risk context) enter the process
- process outputs (prioritized risk list, refined risk context) exit the process
- process mechanisms (evaluation criteria, analysis techniques, analysis tools, risk database) support the process

9.1.3. process activities

- group similar and related risks
- determine risk drivers (variables that cause the probability and consequence of software risk to fluctuate significantly)
- determine source of risk
- use risk analysis techniques and tools
- estimate the risk exposure
- evaluate risk against criteria
- rank risks relative to other risks

9.2. define risk analysis techniques

9.2.1. causal analysis

- determine the cause of the error
- determine the actions that will prevent the error in the future
- implement these corrective actions

9.2.2. decision analysis

used to structure decisions and to represent real-world problems by models that can be analyzed to gain insight and understanding.

- influence diagram technique (provides graphical representation of the elements of decision model with the common notation: squares represent decisions nodes, circles represent chance events, rectangles with rounded corners represent values, double circles represent outcomes known when the inputs are given)
- decision tree technique (provides graphical representation of the elements of decision model with the common notation: squares represent decisions, circles represent chance events, the ends of the branches specify values of outcomes, branches emanating from a square represent choices, branches emanating from a circle represent possible outcomes)

9.2.3. gap analysis

- determines the difference between two variables
- the large gap illustrates the deficiency in that certain area
- the smaller gap corresponds to low risk

9.2.4. Pareto analysis

- determines the order to address the issues
- based on 80/20 rule or the Pareto principle: 20% of the sources cause 80% of the problems
- used to focus on the risks that have the greatest potential for reducing problems
- the relative importance of the risks in a quickly interpreted visual format is displayed by Pareto chart. Pareto chart can display the number of identified risks (frequency) or the risk exposure (cost).

9.2.5. sensitivity analysis

- helps to determine the sensitivity of the model to variations in input variables by setting each variable to its extreme points (holding all other variables at nominal values)
- Two useful techniques for sensitivity analysis are tornado diagrams (allows to see the most sensitive variables first) and utility functions (incorporate the decision maker's risk attitude to maximize expected utility rather than expected value)

9.3. define risk evaluation criteria

- serve as a first cut at ordering risks according to their importance
- defined to measure each risk against a known standard
- criteria to measure are probability, consequence, and time frame for action to prevent risk occurrence

9.4. establish the risk prioritization scheme

- to provide focus for important risks
- the nominal group technique (allows a team to come to a consensus quickly on the relative importance of risks by combining individual priorities into team priorities) and weighed multi-voting (used to rate risks by team members with a number of tokens) are useful in planning, quality management, and process improvement

10. plan risk

10.1. define risk planning process

10.1.1. process goals

- provide visibility for key events and conditions
- reuse successfully risk resolution strategies
- optimize selection criteria (e.g., risk leverage or risk diversification)
- understand the next action for each high-severity risk
- establish automatic triggering mechanisms

10.1.2. process definition

- process controls (project resources, project requirements, risk management plan)
- process inputs (risk list, refined risk context, measures, metrics, triggers)
- process outputs (risk scenarios, thresholds/standards, risk action plan)
- process mechanisms (quantitative targets, resolution strategies, selection criteria, risk database)

10.1.3. process activities

- develop risk scenarios for high-severity risks
- develop risk resolution alternatives
- select the risk resolution approach
- develop a risk action plan
- establish thresholds for early warning

10.2. define risk resolution strategies

10.2.1. risk acceptance

- strategy for risk resolution of consciously choosing to live with the risk consequence.
- It is a strategy to use when you can live with the loss

10.2.2. risk avoidance

- strategy for risk resolution to eliminate the risk altogether.
- Avoidance is a strategy to use when a lose-lose situation is likely

10.2.3. risk protection

- strategy to employ redundancy to mitigate (reduce the probability and/or consequence of a risk)

10.2.4. risk reduction

- strategy to decrease risk through mitigation, prevention, or anticipation.
- Risk is reduced by decreasing either the probability of the risk occurrence or the consequence when the risk is realized.
- Reduction is a strategy to use when risk leverage exists.

10.2.5. risk research

- strategy to obtain more information through investigation
- research is a strategy to use when more information is needed

10.2.6. risk reserves

- strategy to use contingency funds and built-in schedule slack
- reserve is a strategy to use when uncertainty exists in cost or time

10.2.7. risk transfer

- strategy to shift the risk to another person, group, or organization
- transfer is a strategy to use when another group has control

10.3. define selection criteria

- selection criteria help determines the best alternative to resolve risk
- defined selection criteria provides a common basis to understand the characteristics of a good alternative.
- two policies often used as selection criteria are leverage and diversification

10.3.1. risk leverage

- a measure of the relative cost-benefit of performing various candidate risk resolution activities
- leverage is a rule for risk resolution that reduces risk by decreasing the risk exposure (RE).
- risk resolution cost is the cost of implementing the risk action plan

- the concept of leverage helps determine actions with the highest payback

  risk leverage = [RE $_{(before)}$ - RE $_{(after)}$] / risk resolution cost

10.3.2. risk diversification

- is a rule for risk resolution that reduces risk by distribution
- diversification builds a balanced approach that stresses mastery of software project fundamentals

10.4. Develop the risk action plan template with the fields:

- risk resolution strategy
- objectives
- alternatives
- approach
- approval authority
- responsible person
- resources required
- start date
- activities
- due date
- actions taken
- results achieved

11. track risk

11.1. define the risk tracking process

11.1.1. process goals

- monitor the events and conditions of risk scenarios
- track risk indicators for early warning
- provide notification for triggering mechanisms
- capture results of risk resolution efforts
- report risk measures and metrics regularly
- provide visibility into risk status

11.1.2. process definition

- process controls (project resources, project requirements, risk management plan)
- process inputs (risk scenarios, risk thresholds, risk status)
- process outputs (measures, metrics, triggers)
- process mechanisms (risk tracking techniques, risk tracking tools, risk database)

11.1.3. process activities

- monitor risk scenarios
- compare risk thresholds/standards to risk status
- provide notification for triggers
- report risk measures and metrics

11.2. define risk tracking techniques

- often driven by the availability of tools
- sophisticated scheduling tools can be used to track activities and resources over time
- whatever your level of automation, tracking a minimum set of programmatic and technical performance measures is essential to monitoring risk
- one risk tracking technique uses static measures to indicate dynamic risks. A range of acceptable status is defined; then status is tracked to determine trends. When measures fall below acceptable values, action plans are triggered.
- The three steps to monitor risk using static measures are:
    - define warning levels of unacceptable status as thresholds
    - monitor status indicators in terms of measures and metrics
    - regulate the risk action plan execution using triggers

11.2.1. Project control panel

- a visualization of key project indicators that serves as the status display for management and technical metrics
- is both a communication tool and an operational tool
- can be be automated that can monitor project health by a core set of metrics, group metrics into gauge clusters, convey dissimilar metrics using different formats, highlight safe operating areas and warning levels, update display based on real-time work flow, display lower-level and trend data.
- key indicators of project control panel (progress, size, change, quality, risk, staff)

11.2.2. software measures

- determines how well project, process, and product goals are being met.
- software measures such as earned value are leading risk indicators
- an unreliable software measurement process is a significant risk

11.3. define risk measures and metrics

the following measures can be used to determine risk management metrics:

- number of risks
- number of logged risks - the cumulative total of identified issues logged in the risk database
- risk category - a count of number of risks identified in each risk category
- risk exposure
- risk severity - a level of relative risk that includes the dimension of time

- risk leverage
- risk threshold/standard
- risk indicator
- risk management index - percentage of total risk exposure to project cost
- return on investment (ROI) - a summation of the savings for all risks divided by the cost of risk management

11.4. define triggering devices

- triggers provide three basic control functions:
  - activation by wake-up call for revisiting a risk action plan,
  - deactivation by signaling the closure of the risk resolution activity,
  - suspension by putting the execution of risk action plans on hold
- four types of triggers provide notification of unacceptable risk levels:
  - periodic event - notification for activities on the schedule
  - elapsed time - notification for dates based on a calendar
  - relative variance - notification for values outside an acceptable range
  - threshold value - notification for values that cross a predetermined threshold

12. resolve risk

12.1. define the risk resolution process

- specifies the process controls, inputs, outputs, mechanisms (external view)
- specifies the process activities that transform inputs to outputs using the mechanisms (internal view)

12.1.1. process goals

- assign responsibility and authority to the lowest possible level
- follow a documented risk action plan
- report results of risk resolution efforts
- provide for risk aware decision making
- determine the cost-effectiveness of risk management
- is prepared to adapt to changing circumstances
- take corrective actions when necessary
- improve communication within the team
- systematically control software risk

12.1.2. process definition

- process controls (project resources, project requirements, risk management plan)
- process inputs (risk action plan)
- process outputs (risk status, acceptable risk, reduced rework, corrective action, problem prevention)
- process mechanisms (risk resolution techniques and tools, risk database)

12.1.3. process activities

- respond to notification of triggering event
- execute the risk action plan
- report progress against the plan
- correct for deviation from the plan

12.2. define risk resolution techniques

12.2.1. creativity

- inventiveness in originating ideas
- implementing the risk action plan may require gathering new and innovative ideas
- we can use innovation styles (envisioning, experimenting, exploring, modifying) for innovation to resolve risk creatively

12.2.2. collaboration

two or more individuals with complementary skills, interacting to create a shared understanding that none had previously possessed or could have come to on their own

12.3. define risk management Return On Investment

- the savings for all managed risks divided by the total cost of risk management activities:
- $ROI_{(RM)}$ = (Summation of Savings) / Cost
- cost of risk management is the total investment in resources
- savings is the return for each managed risk (avoidance savings, reduction savings)

12.4. develop a Corrective Action Procedure

- helps to correct for variations in the process or the product
- the corrective action procedure has four steps:
  - identify the problem
  - assess the problem
  - plan action
  - monitor progress

13. develop the policy

- obtain commitment
- allocate resources
  - apportion the budget,
  - apportion the schedule,
  - assign the personnel
- survey existing practice
  - new business practices,
  - proposal practices, project practices,

    - research and development practices
- define draft policy
    - involve the opinion leaders,
    - outline the policy contents like (subject, reference, purpose, policy, scope, objectives, responsibility, authority, procedure)
- review draft policy
    - promote understanding,
    - incorporate the feedback
- document policy in a standard format
- approve policy
- communicate policy

14. define standard process

- establish an action team
    - build a high-performance team (a shard compelling vision, individual accountability, synergy in collaboration)
    - organize the team for success
    - level the playing field
- develop the draft standard process
    - select a process design method,
    - gather the risk practices data,
    - scope the effort and products,
    - define the draft standard process
- review the draft standard process
    - prepare the review package,
    - review the draft standard process,
    - incorporate the recommended changes
- document the standard process
    - elaborate the draft standard process,
    - evaluate the standard process,
    - close the action items
- approve the standard process
- distribute the standard process

15. Train risk technology

- Prepare for training
    - need
    - level
    - size
- Develop training material
    - risk management concepts
    - risk assessment methods
    - risk management process
    - risk management measures

        - proactive risk management
    - Apply training metrics
    - Deliver training
        - have something good to say
        - set it well, read your audience
        - use words with emotion
        - identify with your audience
    - Obtain training feedback
        - value of training content,
        - speaker presentation skills,
        - training facilities,
        - the part of training I like best,
        - the part of training I liked least,
        - I still have a need for .....,
        - other comments

12. Verify compliance/fulfillment

Verify compliance of risk management activities through an independent audit. The steps to verify compliance to a risk management plan are as follows:

- Review the risk management plan
    - completeness,
    - understandability,
    - level of detail,
    - consistency,
    - realistic
- Audit/check agents and artifacts
- Generate an audit report
- Track action items

Three major goals of quality assurance:

- Ensure compliance
    - conduct independent reviews and audits.
    - Check the plans and work against established standards by auditing the evidence
- Report discrepancies
    - Alert management to deviations from standards by reporting audit findings.
    - Expose deviations from standards and procedures as soon as possible
- Monitor quality

- improve quality by making recommendations to prevent problems and tracking action items to closure

13. Improve risk management practice

The steps to improve risk management practice are as follows:

- develop an appraisal method
- Assess risk practices
- Develop an improvement plan
- Implement the improvement plan

- Importance is the key to performance because we prioritize activity based on importance.
- To improve the performance of risk management practices, we must first understand the value of the practice.
- It is necessary to improve quantitatively, because only then can we use metrics and statistical comparisons.
- Over time, quantitative results characterize progress and trends in performing risk management.

14. Establish the Initiative

The following activities are included in a checklist to help you respond to project requirements for risk management:

- review risk management requirements
- plan risk management activities
- budget risk management activities
- schedule risk management activities
- staff risk management activities
- coordinate risk management training

- Risk management is a derived requirement for all projects because of the increasing rate of change in software industry.
- The environment for software development is more complex and costly than ever before.

- Risk is not free.
- It is a potential loss, and the only way to turn that around is risk management.
- Risk management is an investment in future payoff/benefit.
- Later, mitigation costs are incurred when there is reason to believe that risk leverage exits.
- You should add a line item for each risk management activity on the project master schedule.
- A risk management initiative cost is the sum total of the budgeted line items.

15. Develop the plan

The contents of a comprehensive risk management plan:

- goals
- strategy
- process
- verification
- mechanisms

- You can delegate responsibility and authority for risk management by clearly defining project roles.
- People can be held accountable for managing risk only when there is no ambiguity in their responsibilities.
- Risk is a function of project role, not an individual person.
- People inherit risk when they are assigned a project role.
- The most effective approach for risk management plan is proactive, integrated, systematic, and disciplined.

16. Control risk

Control the risk to plan, track, and resolve the risk in the project plan and remaining work

Activities in the checklist to control risk:

- develop risk resolution alternatives
- select the risk resolution strategy
- develop the risk action plan
- monitor risk status
- execute the risk action plan

- take corrective action as required

Factors that cause decisions to be difficult:

- Complexity
- Uncertainty
- multiple objectives
- different perspectives

- The software industry will always need risk management.
- The form of risk management will become specialized, as it has in other industries.
- Perhaps when software development is insurable at a reasonable cost, the instruments of software risk management will be mature.

References

1. Ivar Jacobson, “Object oriented software engineering”, Addition-Wesley, 1993
2. Ian Sommerville, “Software engineering”, fifth edition, addition-Wesley, 2004
3. David Gustafson, “Scheum’s outline of software engineering”, McGraw Hill Publication, second edition, 2002
4. Roger S. Pressman, “Software engineering”, McGraw Hill Publication, sixth edition, 2005
5. Scott E. Donaldson, Stanley G. Siegel, “Successful software development”, Prentice Hall, 2004
6. Barry Boehm, LiGuo Huang, “Value-Based Software Engineering: Reinventing “Earned Value” Monitoring and Control”, ACM SIGSOFT Software Engineering Notes vol 28 no 2 March 2003
7. Jyrki Kontio, Gerhard Getto, Dieter Landes, “Experiences in improving risk management processes using the concepts of the Riskit method”, SIGSOFT '98 11/98 Florida, USA, 1998 ACM
8. Tim Menzies, Erik Sinsel, "Practical Large Scale What-if Queries: Case Studies with Software Risk Assessment", 0-7695-0710-7/00, 2000 IEEE
9. W. Eric Wong, Yu Qi, and Kendra Cooper, "Source Code-Based Software Risk Assessing", SAC’05, March 13-17, 2005, Santa Fe, New Mexico, USA 2005 ACM 1-58113-964-0/05/0003
10. Geir Kjetil Hanssen, Tor Erlend Fægri, "Agile Customer Engagement: a Longitudinal Qualitative Case Study", ISESE'06, September 21–22, 2006, Rio de Janeiro, Brazil 2006 ACM 1-59593-218-6/06/0009
11. Watts S. Humphrey, “PSP: a self-improvement process for software engineers”, Pearson education Asia, 2006

12. Bernd Freimut, Susanne Hartkopf, Jyrki Kontio, Werner Kobitzsch, "An Industrial Case Study of Implementing Software Risk Management", ESEC/FSE 2001, Vienna, Austria ACM 2001 1-58113-390-1/01/09
13. Barry Boehm, "Value-Based Software Engineering", ACM SIGSOFT Software Engineering Notes vol 28 no 2 March 2003
14. Barry Boehm, Rony Ross, "Theory-W Software Project Management: A Case Study", 0270-5257/88/0000/0030 1988 IEEE
15. Barry Boehm, Richard Turner, “Balancing Agility and Discipline: A guide for the perplexed”, Pearson education Asia ltd., 2004
16. Barry W. Boehm, “Software risk management: principles and practices”, 07/40-7459/91/0100/0032/ Jan 1991, IEEE
17. Robert N. Charette, “A risk of too many risk standards?”, sixth annual international symposium of the international council on system engineering (INCOSE), July 2006, IEEE
18. Cynthia C. Calhoun, “Identifying and managing risks for automatic test systems”, NASA software IV & V facility, 304-367-8309, IEEE
19. Eric K. Clemons, Michael C. Row, Matt E. Thatcher, “An integrative framework for identifying and managing risks associated with large scale reengineering efforts”, Proceedings of the 28th annual Hawaii international conference on the system sciences, 1995, IEEE
20. Diana Kirk, Ewan Tempero, “Identifying risks in XP projects through process modeling”, Proceedings of the 2006 Australian software engineering conference (ASWEC’ 06), 2006, IEEE
21. John Coppendale, “Managing risks in product and process development and avoid unpleasant surprises”, Risk Management, Engineering management Journal, February, 1995, IEEE
22. Barry Boehm, Daniel Port, “Educating Software Engineering Students to Manage Risk”, 0-7695- I050-7/01, 2001, IEEE
23. B.W. Boehm, “A Spiral Model of Software Development and Enhancement,” May 1988, pp. 61-72, Computer Journal
24. B.W. Boehm and P. Bose, “A Collaborative Spiral Software Process Model Based on Theory W,” Proceedings, ICSP3, IEEE, Reston, Va. October, 1994.
25. Richard E. Fairley, “Software risk management glossary”, IEEE software, May/June 2005
26. Lawrence P. Chao, Irem Tumer, “Risk Assessment Practices at NASA: Studies of Design and Review Methods”, 2006, IEEE
27. Watts S. Humphrey, “Managing Technical People: Innovation, teamwork, and the software process”, Addison Wesley, 1997
28. Ram Chillarege, Shriram Biyani, “Identifying Risk Using ODC Based Growth Models”, 1994, IEEE

29. Frank T. Anbari, “Quantitative methods for project methods”, International institute of learning, Project Management IQ, 1997
30. Watts S. Humphrey, “Managing the software process”, Addison Wesley, 2002
31. Alan Weatherall, Frank Hailstones, “Risk Identification and Analysis using a Group Support System (GSS)”, Proceedings of the 35th Hawaii International Conference on System Sciences – 2002, IEEE
32. Watts S. Humphrey, “Introduction to the Team software process”, Addison Wesley, 2000
33. Craig Larman, “Agile and iterative development: a manager’s guide”, China Machine press, 2006
34. Elaine M. Hall, “Managing risk: methods for software systems development”, Addison-Wesley, 1998
35. Marvin J. Carr, et el, “Taxonomy based risk identification”, June 1993, technical report, CMU/SEI- 93-TR- 6
36. Janne Ropponen and Kalle Lyytinen, “Components of Software Development Risk: How to Address Them? A Project Manager Survey”, IEEE Transactions on software engineering, Vol. 26, No. 2, Feb 2000
37. Don Shafer, “Software risks: Why must we keep learning from experience?” dynamic positioning conference, September 2004
38. James J. Jiang, Gary Klein, Richard Discenza, “Information System Success as Impacted by Risks and Development Strategies”, IEEE Transactions on engineering management, Vol. 48, No. 1, FEBRUARY 2001
39. June M. Verner, William M. Evanco, “In-house software development: what project management practices lead to success?”, IEEE software, 2005
40. ISO/IEC 16085 IEEE 1540-2001, Information technology-software life cycle process, risk management, International standard, 2004
41. Deepak Surie, “Evaluation and integration of risk management in CMMI and ISO/IEC 15504, IEEE
42. Barry Boehm, Alexander Egyed, Julie Kwan, Dan Port, et el “Using the Win Win spiral model: a case study”, July 1998, IEEE
43. James D. Palmer, Richard P. Evans, “Software risk management: requirement based risk metrics”, 1994, IEEE
44. Ray C. Williams, George J. Pandelio, Sandra G. Behren, “Software risk evaluations (SRE) method description, technical report, December 1999, CMU/SEI 99-TR-029
45. James J. Jiang, Gary Klein, Richard Discenza, “Information system Success as Impacted by risks and development strategies”, IEEE Transactions on Engineering Management, Vol. 48, No. 1, February 2001
46. Ram Chillarege and Shriram Biyani, “Identify risk using ODC based growth models”, IEEE, 1994

47. Barry Boehm, “Anchoring the software Process”, IEEE Software, 1996
48. Barry W. Boehm, “Software Engineering”, IEEE transactions on computers, Vol. c-25, No. 12, Dec 1976
49. Grady Booch, “It is what it is because it was what it was”, IEEE Software, 2007
50. Alistair Cockburn, “Agile software Development”, Agile software development series, 2000
51. Kent Beck, Martin Fowler, “Planning Extreme Programming”, Addison Wesley, 2000
52. Rational software corporation, “Managing Project Risk: best practices and tool integration in software development”, 2002
53. Paul S. Royer, “How healthy is your project?”, Proceedings of project management institute annual seminars and symposium, Sept 2000, USA
54. Tom Gilb, “Risk management : a practical toolkit for identifying, analyzing, and coping with project risks”, 1999
55. Marian Myerson, “Risk management processes for software engineering models”, Artech House Inc., 1996
56. Dale F. Copper, Stephen Grey, Geoffrey, Raymond and Phil Walker, “Project Management Guidelines: managing risks in large projects and complex procurements”, Broadleaf Capital International, John Wiley & Sons Ltd., 2005
57. Software Engineering Standards Committee of the IEEE computer society, “IEEE standard for software life cycle processes – risk management”, IEEE 2001
58. Peter G. Smith, Guy M. Merritt, “Proactive Risk Management”, Sound view Executive Book Summary Vol. 24, No. 11, Nov 2002
59. Thomas J. Linsmeier, Neil D. Pearson, “Risk Management: An introduction to value at risk”, Pearson Education, 1996
60. Alfredo del Cano, Pilar de la Cruz, “Integrated Methodology for Project Risk Management”, Journal of construction engineering and management, 2002
61. E. Wiegers, “Know your enemy: software risk management”, Software Development, Oct 1998
62. James P. Lewis, “Fundamentals of project management”, AMACOM books, 1995
63. Tim Bedford, Roger M. Cooke, “Probabilistic risk analysis: Foundations and Methods”, Cambridge University Press, 2003
64. Anne M. Marchetti, “Beyond Sarbanes – Oxley compliance : effective enterprise risk management”, John Wiley & Sons, Inc., 2005
65. Max Wideman, “Project and program risk management: a guide to managing project risks and opportunities”, The PMBOK handbook series Vol. No. 6, Project Management Institute 1992
66. James Bayne, “An overview of threat and risk assessment”, SANS Institute 2002

67. Robert Kauer, Hubert Sacher, “Asset management and cost saving maintenance strategy based on risk – informed decision making”, TUV Indstrie Service GmbH, Germany
68. Peter H. Feiler, Roger Smeaton, “The project management experiment”, Carnegie Mellon University, May 1998
69. Vlasta Molak, “Fundamentals of risk analysis and risk management”, CRC Press Inc., 1997
70. Ian Tho, “Managing the risks of the IT outsourcing”, Elsevier Butterworth Heinemann, 2005
71. Project management institute, “Project management institute body of knowledge (PMBOK) Guide”, PMI, 1999
72. Bob Norton, “Principles of risk management : risk management paradigm”, Secrets of a serial entrepreneur series, C – Level Enterprises, Inc. 2004
73. Jean – Paul Chavas, “Risk analysis in theory and practice”, Elsevier Inc., 2004
74. Philip Best, “Implementing value at risk”, John Wiley & Sons, Ltd., 1998
75. Alan J. Laubsch, “Risk management : A practical guide”, RiskMetrics Group, 1999
76. Linda H. Rosenberg, et el, “The role of metrics in risk management across the software development lifecycle”, American Institute of aeronautics and astronautics, 2000
77. Thomas L. Barton, et el, “Making enterprise management pay off : how to leading companies implement risk management”, Financial Times, Prentice Hall, 2002