Translated from Croatian to English - www.onlinedoctranslator.com

Protection and security of information systems

Management of (software) risk

prof. Ph.D. Krešimir Fertalj

Protected by licensehttp://creativecommons.org/licenses/by-nc-sa/2.5/hr /

Creative Commons

- **you are free to:**
  - **share**—reproduce, distribute and communicate the work to the public
  - **remix**—rework the work
- **under the following conditions:**
  - **appointment**. You must acknowledge and attribute the authorship of the work in a manner specified by the author or licensor (but not in a manner that suggests that you or your use of their work has their direct endorsement).
  - **non-commercial**. You may not use this work for commercial purposes.
  - **shares under the same conditions**. If you modify, transform, or create using this work, you may distribute the adaptation only under a license that is the same or similar to this one.

In the case of further use or distribution, you must make clear to others the license terms of this work. The best way to do this is to link to this website.

Any of the above conditions may be waived with the permission of the copyright holder.

Nothing in this license infringes or limits the author's moral rights.

The text of the license was taken from http://creativecommons.org/.

Risk and risk management

- Risk
  - a condition that may lead to some losses or may jeopardize the success of the project
- Risk management
  - dealing with a concern before it grows into a problem or crisis
- Risk management consists of
  - risk identification,
  - decisions on how to act in case of a particular risk, and
  - risk removal and risk consequence handling
- Management activities should correspond to the size of the project
  - Small projects - simple risk lists, one team member (not manager)
  - Large projects - formal risk management, *risk officer*, full time

Risk management activities

- risk assessment
  - Risk identification
    - establishing a list of risks, especially those that could affect time delays
  - Risk analysis
    - assessment of the probability and impact of a particular risk, and risk assessment for different alternatives
  - Risk prioritization
    - determination of the priority list of risks according to the impact, eg on time delays
- risk control
  - Risk management planning
    - action plan in the event of certain risky situations
  - Risk resolution
    - execution of the plan to eliminate the risky situation that occurred
  - Supervision, monitoring of risks (risk monitoring)
    - monitoring situations, identifying new ones and including them in the management process

Risk evaluation

Risk identification

- Risk description with cause-and-effect statements
  - A worrisome situation is monitored and a possible consequence is assessed
- For example,
  - risk can be considered as a condition: "users do not agree with the requirements placed on the product"
  - or as a result: «it is possible to satisfy only the most important users».
  - combining the statements into a cause-and-effect formulation: «Since the users do not agree on the requirements placed on the product, it is possible to satisfy only the most important users».
- One condition can lead to several consequences, and several conditions can contribute to the same consequence.

Risk recognition

- Deadline risks
- Planning risks
- Risks of organization and management
- Development environment risks
- End User Risks
- Risks of the client
- Risks of (sub)contractors
- Claim risks
- Application risks
- Risks of external influences
- Development team risks
- Design and installation risks
- Process risks

- Examples of the most common risk groups are listed in the appendix

- In addition to general risks, each project carries its own risks
  - for example, an important team member threatens to fire him if he can't bring his dog to work

Risk analysis

- After determining the list of project risks
  - Analysis of each risk individually
  - Determining the impact on the project

- Application
  - choosing between several development options or
  - determining the risk of the already selected development option

Risk documentation

- Template for documenting an individual risk statement
  - **ID**: Unique identifier
  - **Opening date**: Date when the risk was identified
  - **Closing date**: The date when the risk was closed
  - **Description**: Description of risk in the form of "condition-consequence"
  - **Probability**: Likelihood that the risk will become a problem
  - **Effect**: Potential damage if the problem materializes
  - **Exposure**: Probability * effect
  - **Resolution plan**: avoidance, reduction, transfer, acceptance of risk
  - **Carrier**: Person responsible for risk resolution
  - **Deadline**: The date by which the mitigation plan must be completed
- Instead of a structured document - a table with a list of risks

Risk assessment

- Risk as "unexpected loss"
- **Probability** of loss ranges from 0.01 to 1.0 (up to 100%)
- **Size** loss, effect
  - we are interested in the time schedule - expressed in days/weeks/months
  - alternatively financial loss in monetary units
- **Exposure**, impact (risk exposure, risk impact)
  - When we are interested in the schedule, the delay is calculated (scaled).
  - Exposure = Probability * Effect
  - Example: 25% probability that something will last 4 weeks longer - exposure 1 ie.
- Sometimes it is not necessary to precisely quantify the risk.
  - Probability and effect can be *high, medium* or *low*.

An example of a risk assessment

Risk	Probability loss	Size loss (in weeks)	Exposure risk (in weeks)
Over-optimistic development	50%	5	2.5
plan Additional requirements	5%	20	1.0
for full automatic support software updates			
version			
Additional functionalities	35%	8	2.8
according to marketing requirements (specific functionalities unknown)			
Unstable graphical user interface subsystem	25%	4	1.0
Inappropriate design that requires redesign	15%	15	2.25
Project approval is taking longer than expected	25%	4	1.0
Funds for work are not available on time	10%	2	0.2
Reports by management require more development time than expected	10%	1	0.1
The contractor's delay in the delivery of the graphic subsystem The new programming tool does not bring the promised savings	10-20%	4	0.4-0.8
	30%	5	1.5

Potential risks and their impact on project delays were identified.

Impact, 1 to 20 weeks delay with probability of individual risk 5% to 50%.

Estimation of the size of the loss

- It is usually easier to estimate the magnitude of the loss than the probability of occurrence

- For the example in the previous table,
  - let it be estimated that the project will be approved on February 1 or March 1, depending on when the supervisor will discuss the project proposal
  - The size of the approval risk on March 1 is exactly one month
- When it is not easy to directly assess the size of the loss
  - divide possible losses into smaller ones,
  - and estimate their size, and then
  - aggregate individual estimates of sub-losses.
- For example, if three new software tools are used,
  - for each tool separately estimate the size of the loss, and then
  - sum up the oversights for individual tools.

Estimation of probability of loss

- Probability assessment usually subjective - procedures to increase accuracy
- The most knowledgeable person assesses the probability of each individual loss
- ***Delphi*** or some other consensus-building process
  - Each member of the group assesses each risk separately
  - Estimates, especially extreme ones, are discussed (argued).
  - The estimation procedure is repeated until convergence
- **Betting method**
  - For example "If the accessories are ready on time, I give/you get HRK 125, otherwise I get HRK 100"
  - The bet is redone until both parties are satisfied
  - The risk probability is the result of dividing the profit of the bet maker and the total amount.
  - For the given example, probability = HRK 100 / HRK (100 + 125) = 44%.
- **Procedure of adjective calibration ("adjective calibration")**
  - determine the level of risk descriptively (e.g. very likely, likely, ..., unlikely)
  - then the descriptive estimates are quantified [Boehm 1989]# better qualitatively

Time losses of the entire project and time stocks

- Exposure to risk is *expected value time nski losses*
  - Statistically, the expected loss is the product of the probability and the size of the loss
  - In the example, loss due to inappropriate design = 15%*15t = 2.25 weeks
- Total losses before risk management steps are taken
  - by adding up individual losses, for example in table 12.8 to 13.2 weeks

- The time plan should be adjusted to the expected time losses
  - after creating a risk management plan
  - set the expected time losses as the time reserve of the project
- alternatively, a timeline with +/- tolerances for each risk
  - the time plan is updated every time a risk materializes

Risk prioritization

- Risk prioritization – directing management
  - In projects, usually 80% of the budget is spent on correcting 20% of the problems, so it is necessary to focus on the 20% most important [Boehm 1989]
  - "Considering that it is unsuccessful to try to eliminate the risk, and it is questionable to minimize it, it is crucial that every risk taken is the *real*" [Peter Drucker]
- It is easier to focus only on weather risks than on all types of risks at once!
  - Trivially, by descending order by exposure

Risk assessment arranged according to priorities

Risk	Probability loss	Size loss (in weeks)	Exposure at risk (in weeks)
Additional functionalities according to marketing requirements (specific functionalities unknown)	35%	8	2.8
Over-optimistic development plan	50%	5	2.5
Inappropriate design that requires redesign	15%	15	2.25
The new developer tool does not deliver the promised savings	30%	5	1.5
Additional requirements for full automatic support software updates	5%	20	1.0
version			
Unstable graphical user interface subsystem	25%	4	1.0
Project approval is taking longer than expected	25%	4	1.0
The contractor's delay in the delivery of the graphic subsystem. There are no means for work	10-20%	4	0.4-0.8
available on time	10%	2	0.2
Reports by management require more development time than expected	10%	1	0.1

Comment on priority by exposure

- The ranking of the risks in the table gives a rough estimate of the priority of the risks
  - Successfully solving the first 5 risks brings savings of 9.8 weeks
  - Solving the last 5 saves from 2.1 to 3.7 weeks
- Tabular *sort* is rough estimate priority
  - Risks with large amounts of losses should perhaps be closer to the top
  - For example, "Additional requests ..." has a probability of 5%, but incurs a loss of 20t
    - it is necessary to ensure that this risk does not occur even though it is unlikely
- Sometimes it is more important combination in relation to individual risks
  - Example, **Interface instability...** and **The contractor's delay...**
  - The combination has a higher risk than the individual

Assessment accuracy and disregard for risk

- The ranking of risks according to priority is only an approximation
  - because all the data used is only *assessments*.

- The accuracy of the priorities depends on the accuracy of the estimates of probabilities and sizes
  - Converting estimates into numbers creates the impression that the priority list is accurate, although it cannot be more accurate than the subjective data on which it was derived!

- Ignoring risk
  - There is no point in spending time on risks that carry small losses
  - In order not to spend more on dealing with risk than is worth its loss

Risk control

Risk control

- risk control
  - **Planning** risk management
    - action plan in the event of certain risky situations
  - **Resolution** risk resolution
    - execution of the plan to eliminate the risky situation that occurred
  - **Supervision**, risk monitoring
    - monitoring situations, identifying new ones and including them in the management process
- Risk resolution
  - **Avoiding -** Avoidance (eliminate, withdraw from or not become involved)
  - **Forwarding, sharing -** Sharing (transfer, outsource or insure)
  - **Reduction -** Reduction (optimize – mitigate)
  - **Acceptance -** Retention (acceptance and budget)

Risk management plan and risk resolution

- Risk management plan
  - An action plan is created for each identified high risk
  - A plan can only be a statement "**who, what, where, when, why and how**" act
  - The plan should contain general provisions for monitoring risks, closing risks that have been resolved and identifying new risks.

- Risk resolution - depends on the particularities of each risk
  - For example,
    - Ex. 1: risk of inappropriate design in an unexplored problem area Ex. 2:
    - risk of "losing" work space, by moving to another team
  - What to do ?

General risk resolution procedures

- **Avoid**risk - not to take the risk or remove the cause
  - Example 1.a: assume responsibility only for the known part, leave the unknown to the client?!
  - Example 1.b: change the scope of the project - the problem becomes part of another version or project
  - Example 2.a: persuade the group claiming the space to give up (completely)
  - Example 2.b: induce the competition to move to another space

- **Redirection**of risk - a risk in one part is not a risk in another
  - consequences and/or management are transferred to another part of the project or to a third party
  - Example 1.a: service rental (outsourcing) of the risky part
  - Example 1.b: proposal to the client to include / revise the design - take part of the responsibility
  - Example 2.a: suggestion that another group replace the workspace
  - Example 2.b: agree to the transfer but with a delay until a better time or the end of the project

General risk resolution procedures (continued)

- **Reduction** risks
  - Accept the possibility of risk and develop a backup plan
  - Ex.1: provide enough members to test a poorly designed system, plan additional time to correct errors
  - Example 2: if a move is unavoidable, it should be carried out at a time when it has the least impact on work and help with packing and moving should be organized

- **Acceptance** risks
  - Accept the possibility that the risk may happen and do nothing
  - Appropriate if the consequences are small and the effort to avoid is high

General risk resolution procedures (other)

- Gathering information about risk
  - If it is not known how serious the risk is, it should be investigated.
  - Ex.1: prototype for feasibility test, or external design evaluation
  - Example 2: cooperation with the relocation organizer - replacement space
- Disclosure of risks
  - Familiarize stakeholders with risk and consequences - management, users, ...
  - minimize their surprise should the risk occur
- Risk records
  - a collection of resolution plans, which can be used in future projects

[some] Control mechanisms

Risky situation	Mode of control
Unplanned addition of new program features	Be oriented towards the client Use incremental development processes Control the application's feature set Provide a fallback design
Exaggeration in requirements or development	Do not meet all requirements Set a timeline for requirements Control the application's feature set Use phased delivery Use a system of test prototypes Design according to a time plan
Decrease in quality due to too short a time limit Over-optimistic development plan	Take time for questions and answers, and pay attention to the basics of quality assurance Use timed assessment procedures, multiple assessments, and automated assessment tools Use negotiation tactics Design according to a time plan Use incremental development procedures
Inappropriate design	Set the design as a separate activity for which the plan will provide time Use design inspections
Silver bullet syndrome	Be skeptical of requirements related to productivity Create a program to measure the quality of software support Establish a group to take care of software tools
Research oriented development	Don't try to research and maximize development speed at the same time Use a risk-oriented plan
Bad staff	Hire the most talented staff Recruit and deploy key employees long before the start of the project Train employees Build a team
Errors of the contractor	Check the contractor's references

Risk monitoring

- Risk volatility
  - risks appear, increase/decrease, disappear over time
  - permanent monitoring and measurement

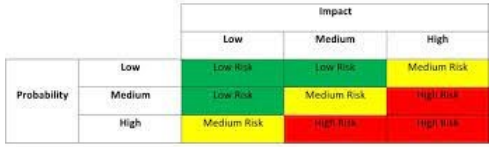
- "list of the biggest 10" (Top 10)
  - one of the best monitoring strategies
  - not necessarily exactly 10 risks
  - content - risk status, number of occurrences, steps since previous update
  - update once a week (or according to the iteration of the project life cycle)
  - the most important aspect - ensuring regular insight, regular thinking about risks and alerting in case of changes in the importance of risks

List of the 10 biggest risks

This one week	Past week	Number weeks on the list	Risk	Steps taken to reduce risk
1	1	5	Unplanned addition new software characteristic	A phased delivery system is adopted; need to be explained to marketing and end users.
2	5	5	Inappropriate design, which requires a redesign	A redesign is in full swing.
3	2	4	Trial Manager there is no project yet took the job	The selection of external reviewers is in progress. The job was offered to the best to the candidate; waiting for the offer to be accepted.
4	7	5	Unstable graphically interface subsystem	The design of the graphic interface is placed in the foreground of the project; the design is not finished yet.
5	8	5	The contractor is late in delivery of graphic subsystem	An experienced person is appointed to liaise with the contractor; still no response from the contractor.
6	4	2	Development tools lag in delivery	5 out of 7 development tools are OK. The group designated for the procurement of development was notified.
7	-	1	Slow review cycle from side manager.	Evaluation in progress.
8	-	1	Review cycle of by the user slow	Evaluation in progress.
9	3	5	An overly optimistic plan	The first stage of the project was completed on time.
10	9	5	Additional request for automatic by updating the version	Investigate the feasibility of manually updating the version.
-	6	5	He is the head of design preoccupied requirements for support the previous project	The previous project got a new leader.

Qualitative risk assessment

- numerically, but with relative values
- Matrix of predefined values



Qualitative risk assessment table

  - risk level as the sum of asset value (AV), vulnerability (V) and threat (T), eg.
    - AV ranging from 0 (small) to 4 (very large)
    - V and T range from 0 (low level) to 2 (high level)
    - R = AV + V + T
  - Values 0-8
    - Low (M): 0 - 2
    - Medium (S): 3 - 5
    - High (V): 6 – 8

	Threat	0			1			2		
	Vulnerability	0	1	2	0	1	2	0	1	2
Value resources	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

  - Characteristics
    - Arbitrary determination of parameters, simplicity
    - neglecting higher risks due to (function) distribution (does not look at probability and consequence)

Addition

Types of risk

Timing risks

- Unplanned addition of features that disrupt the design
- Unnecessary refinement of individual parts of the application
- Reducing quality to meet deadlines
- Too optimistic development timelines
- Inappropriate design of software support
- Silver bullet syndrome
- Research-oriented development
- Weak development team
- Errors for which subcontractors are responsible
- Divergence between users and the development team

- The simplest way of recording risks
  - lists of risks ordered by impact on delay

Risks of planning (time schedule)

- Time plan, resources and product definition are not agreed.
- The time plan is too optimistic (as in *at best*).
- The time plan does not cover all procedures to be carried out.
- The plan is made with a wrong assumption about the composition of the development team.
- The application is larger than intended (eg LOC/FP/OP vs. surrogates).
- The required effort is greater than expected.
- Excessive pressure on team members due to deadlines reduces their productivity.
- The timeline was changed without any necessary changes in process or resources.
- The time delay of one part causes the delay of dependent parts.
- Unknown parts of the application take more time than expected.

Risks of organization and management

- Management or senior management do not support the project.
- Employee departure reduces the capacity of the development team.
- Management and marketing insist on decisions that extend the deadline.
- Development team inefficiency reduces productivity.
- Slow decision making.
- Budget cuts disrupt plans for project development.
- Making decisions that reduce the motivation of team members.
- Non-technical parts of the project take longer than expected (eg approval, procurement).
- Poor project management and poor monitoring of project progress.
- Abandoning the project plan under deadline pressure.

Development environment risks

- The equipment does not arrive on time.
- Equipment is available but inadequate (eg Internet, office equipment).
- The equipment is crowded, noisy or interferes with work.
- The development tools are not suitable for the type of problem being solved.
- Development tools are not available at the required time.
- Development tools are not working as expected.
- Too long a learning curve for new development tools.
- License expiration.

End User Risks

- Risks related to the end user
  - Users insist on new requirements.
  - Users demand a redesign of the application.
  - Users do not provide the necessary information.

- Risks related to user requests
  - Misunderstanding of the request.
  - Unconfirmed requests.
  - Unverified requests.
  - Hidden requests.
  - Request changes.

Client's risks, contractor's risks, external influences

- Risks related to the client
  - Slow response from the client (according to plans and specifications).
  - The client does not want or is not able to participate in decision-making.
  - The client requires technical solutions that extend the duration.
  - The client manages the development process.
  - Low-quality or incompatible components procured by the client independently.
  - The client avoids the handover, even though the software support meets all the specifications.
  - The client demands an unfeasible speed of development.
- Risks related to the contractor or subcontractor
  - The contractor is late with the delivery of components.
  - The supplied components are of poor quality, so they need to be improved.
  - The contractor is unprofessional or insufficiently engaged.
- Risks related to external influences
  - Development depends on legal regulations that change unexpectedly.
  - Development depends on technical standards, which change unpredictably.

Application risks

- The modules that cause the most errors require more effort than expected.
- A poor quality application requires more effort than expected.
- (Unnecessary) training increases development time.
- Developing faulty software functions requires redesign and implementation.
- An unacceptable user interface requires a redesign.
- Responsiveness or data volume issues take longer than expected.
- Strict compatibility requirements...
- Requirements placed on interfaces with other systems ...
- Request for portability to other OS...
- Working in an unknown/untested environment causes unforeseen problems.
- The development of a new atypical component takes too long.
- Relying on immature technology prolongs the development of software support.

Development team risks

- The recruitment of members of the development team is taking longer than expected.
- Prerequisites (e.g. training, completion of other projects, work permits)...
- Bad relationships between team members and/or management slow down decision-making and implementation.
- Team members are not engaged enough, and the result is poor performance.
- Low morale and motivation reduce productivity.
- The lack of necessary specializations causes defects and rework.
- Members need additional time to familiarize themselves with the tool, environment, equipment.
- External collaborators leave the project before the end of the project.
- Permanent employees leave before the end of the project.
- New members join the project late, which reduces the effectiveness of existing members.

Risks of the development team (continued)

- Team members do not work effectively together.
- Conflicts between team members - poor communication, design, rework, ...
- Problematic members – impaired team motivation and relationships.
- The most capable members are not available for political or other reasons.
- It is not possible to recruit members with the required characteristics.
- Key employees are not available full time.
- Not enough employees are available to work on the project.
- Tasks entrusted to team members exceed their strengths.
- Employees work slower than expected.
- Managers "sabotage" the project - ineffective planning.
- Technical staff "sabotage" the project ... useless work or poor quality

Design and installation risks

- Simplified design according to requirements - redesign and re-installation.
- Overcomplicated design causes unnecessary and unproductive implementation.
- Bad design causes re-design and re-implementation.
- Inappropriate procedures - additional teaching, work, correction of errors.
- Implementation in inappropriate / outdated language - productivity ...
- Inappropriate program libraries - replacement or development of your own.
- Low-quality prog. code / libraries - additional testing, corrections and rework.
- Overestimated time savings expected from tools.
- The difficulty of integrating separately developed components – redesign, refinement.

Development process risks

- Too much administrative work.
- Imprecise monitoring of development – too late assessment of the real situation.
- Abbreviated testing in various stages - more significant revisions in later ones.
- Imprecise quality monitoring – finding out about poor quality too late.
- Too little formalism (standards) - poor communication, quality - processing.
- Too much formalism (blind adherence) - unnecessary extra work.
- Upstream development progress reports are taking longer than expected.
- Poor business risk analysis did not reveal the biggest project risks.
- Project risk analysis takes more time than expected.