RiskUse - Guidelines, version 1.0

Lindholm, Christin

2014

RiskUse

Guidelines, version 1.0

Christin Lindholm

RISK MANAGEMENT PROCESS

A software risk management process including user perspective. First version

Email: christin.lindholm@cs.lth.se

RiskUse - risk management process

The purpose of the risk management process, RiskUse is to provide practitioners, mainly risk managers with a software risk management process that has a well-defined user perspective. The aim is to present a risk management process that allows the development organisation to perform adequate risk management activities that can ensure that the developed software is safe from a user perspective.

1. RiskUse - phases and steps

RiskUse consists of five phases; including different steps in each of the phases displayed in Figure 1. The different phases and steps are defined below.

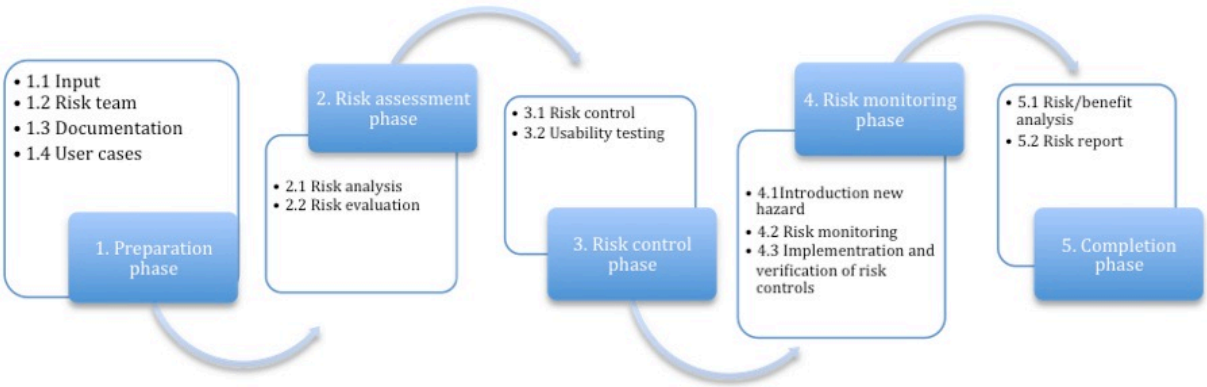

Figure 1 The risk management process, phases and steps.

1. Preparation phase: This is the first phase of the risk management process and it is the phase where the risk manager makes the preparations for the entire process. The phase consists of four steps:

Step 1.1 Input: The requirement specification and descriptions of intended use, intended users and system context for the system is collected. The documentation is used to get a general understanding of the system, to establish a risk team with the right combination of competencies and used as a foundation in the use case development process.

Step 1.2 Risk team: The risk manager establishes the risk team. The team shall consist of:
Developers - with knowledge on how the system or device is designed, are produced, functions and how it shall be used.
Users - who represents different user groups The description of intended users can be used as support in the selection process.
Risk manager - who is responsible for the entire risk management process and chair of the risk meetings. When possible an assistant risk manager shall be selected who will be responsible for the documentation at the risk meetings.

Step 1.3 Documentation: During the preparation phase it is decided which risk documentation that shall be produced. The documentation shall at least consist of:
Risk management plan - including description of traceability and scales of assessment and risk acceptance, see Section 1.1
Risk meeting documentation - each risk meeting shall be documented, see Section 1.4.

Risk management report - including risk/benefit analysis for the residual risks and post product information, see Section 1.7.
All documentation shall be maintained in a risk management file.

Step 1.4 Use cases: Use cases based on the system's functionality shall be designed and used as use case-based identification method of hazards at the risk meetings, see Section 1.3.

2. Risk assessment phase: the phase where the risk meetings are held and the hazards and hazardous situations are identified from the use cases by the risk team. Risk(s) are estimated from each hazardous situation and then analysed and evaluated. The two steps of the phase are:

Step 2.1 Risk analysis: The known and foreseeable hazards and hazardous situations are identified through the use cases and documented in the risk meeting documentation. For more details, see Section 1.4.
For each identified hazardous situation the associated risks are estimated according to the scales presented in Section 1.5
The risk value is calculated for each risk by multiplying the Severity with the Probability value, i.e. **Risk =** Severity x Probability. The highest risk value a risk can receive is **Risk** = 4 x 4 = 16.
The severity, probability and risk values are documented in the risk meeting documentation.

Step 2.2 Risk evaluation: For each identified hazardous situation with associated risk(s), risk evaluation shall be made and documented in the risk meeting documentation. More specifically the risk team decides if risk reduction is necessary.
For each risk that meets one or several criteria for risk reduction or mitigation according to criteria for risk acceptability described in Section 1.5 one or several risk control measures shall be established.

3. Risk control phase: the phase contains the risk control process and the assignment of risk control measures to usability testing

Step 3.1 Risk control: Appropriate risk control measure shall be identified en decided for each hazard that needs to be reduced or mitigated. The decision shall be documented in the risk meeting documentation. It shall be decided if the risk control measure is suitable for usability testing and if so, it shall be documented in the risk meeting documentation.
The risk control measures are during the risk control phase assigned to developers, i.e., which developer becomes responsible for implementing and verifying the assigned measure. Follow-up dates are decided and documented. The assignment can be done during the risk meeting or after the risk meetings. All risk control measures shall result in one or several requirements in the product requirements specification. The risk control measures are traceable by the use of the unique hazard id, specified on the form UC.x.y Hx.
The risk values have to be re-assessed and possible residual risks identified.

Step 3.2 Usability testing: Risk control measures suitable for usability testing is incorporated in the usability process and assigned to usability testing. After the usability

testing is performed a new iteration of the risk evaluation phase is done. The use case descriptions could be used as a foundation for the test cases in the usability test. See further Section 1.6.

4. Risk monitoring phase: the phase where the introduction of new hazards is discussed and identification of residual risks is performed.

Step 4.1 Introduction new hazard:	For each identified risk control measure, the introduction of new hazard and hazardous situations is discussed. If a new hazard and hazardous situation are identified, a new unique hazard id on the form UC.x.y Hx shall be generated and incorporated in the in the risk meeting documentation. The hazard id shall be coloured blue, (see Section 1.4) and a new iteration of the risk assessment phase and risk control phase is done.
Step 4.2 Risk monitoring:	After the discussion and decision about appropriate risk control measures the risks shall be analysed again according to the scales in Section 1.5. The remaining risks, the residual risks that do not meet the acceptance criteria, one of two options shall be chosen, either further risk control, according to step 3.1 or risk benefit/analysis according to step 5.1.
Step 4.3 Implementation and verification of risk controls:	The assigned developers shall perform verification and validation of the implementation of the risk control activities. The results of verification and validation shall be balanced against the documented values for severity, probability and risk documented in the risk meeting documentation, a new analysis of the risk values are made. If the risk values, not are lowered enough new risk control measures has to be decided, implemented and verified.

5. Completion phase: the last phase where the residual risks are handled and the risk management report is written.

Step 5.1 Risk benefit/analysis:	For residual risks not meeting the acceptance criteria and were further risk control is not applicable a risk/benefit analysis shall be made. Review data shall be gathered to support the conclusion that the medical benefits of the medical device (entire medical device or particular features of the medical device) outweigh the residual risk. The review data shall be documented.
Step 5.3 Risk report:	A risk management report shall be written prior to release for commercial distribution. A review of the risk management process shall be done and the result shall be documented in the risk management report. Information important for the production and post-production phase that are gathered and documented during the risk meetings, for example, warnings in the graphical user interface, labelling and special training shall be documented in the risk management report, see Section 1.7.

1.1 Risk management plan

All the planned risk management activities shall be documented in the risk management plan. The plan shall be maintained in the risk management file. The risk management plan shall at least include the following:

- Description of the medical device including a description of intended use and intended users.
- Definition of the risk management scope and how the activities relate to the life-cycle phases.
- Description of the risk management team.
- Definition of the input to the risk management process, for example requirement specification, project plan, verification and validation plan.
- Description of how traceability is handled.
- The procedures for the risk meetings, including risk meeting documentation.
- Detailed description of the procedures of risk analysis, risk evaluation and risk control, including the scales for estimation and the risk acceptance criteria.
- Description of how residual risks and the introduction of new hazard are handled.
- Description of implementation and verification of risk control procedures.
- Description of how production and post-production information are collected and handled.

Recommendation: The description of intended use and intended users could be reused from the product project plan and also reused in the risk management report. Endeavour as hands-on descriptions as possible.

1.2 Traceability

Traceability of the hazards is maintained in the risk management process by the hazard id, specified on the form UC.x.y Hx. The first part, UCx refers to the use case that the hazard was identified in, y to the step in the use case and Hx is a local unique identifier that allows for more than one hazard to be assigned to a particular step in a use case. By colour blue the hazard id generated for a new hazard identified after risk control measures, new hazards are traceable and easy to track in the risk meeting documentation (Section 1.4)

To maintain traceability to the requirements, both to the product and user requirements, each use case description contains the unique identifiers for the requirements relevant for the specific use case. There is a chain of traceability through the process and also backwards see Figure 2.

Figure 2 Traceability chain.

In the usability test cases are documented, which hazards they test and the results of the usability testing are mapped back to the hazards. The same approach can be used according to other verification and validation activities.

1.3 Use cases

The use cases shall be written before the risk meetings and the risk manager or other members of the development organisation do it. The use cases are then used as input during the risk meetings. At the meeting the risk manager first makes a walk-though of the use case(s) and alteration are made if need. The risk manager then guides the discussion throughout the meeting and each step in a use case is discussed according to hazard.

Each use case description shall contain:

Unique id: on the form UC.x.y were UC.x refers to the use case and y to the step in the scenario.

Requirement specification: Specification of the relevant requirement specification, for example the document number.

Requirements: Specification of the user requirements (UR) and the product requirements (PR) relevant to the use case, for example: UR1 [PR6]

Preconditions: Preconditions for the use case, for example: The patient is already registered in the system.

Use case: Each step in the use case is defined, for example: UC 5.1 Chose new evaluation scale.

Comments: Important issues from the risk meeting concerning the use case, for example: the value shall not be displayed for the user.

1.4 Risk meeting

In this Section some guidelines and recommendations are given according to risk meetings in the risk management process.

General guidelines regarding preparation for the meeting:

Participants: there should be at least one participant from each group of participants; the intended users, the developers and risk managers.

Organisation: the risk managers organise and document the risk meetings. A risk manager is also the chair of the risk meetings.

Time schedule: the recommended time for a risk meeting is 2 hours. Longer meeting time makes it difficult for the participant to stay focused.

Input to the meeting: Predefined use cases and description of intended use, scales for estimation and criteria for risk acceptance.

Guidelines for the setup of the meeting:

Introduction: The procedures for the meeting, the scales the system context and intended used are presented by the risk manager and discussed among the participants at the beginning of the meeting. All participants should be familiar with the procedures, scales and intended use. The risk manager also performs a walk-though of the use case(s) and alterations are made if needed.

The meeting: The hazards are identified through brainstorming, with the risk manager as facilitator. For each step of the use case, all participants suggest possible hazards and hazardous situations connected to the specific use case step discussed. Characteristics that could affect safety of the device, stressful situations, environmental factors and transportation of the medical device should also be taken into consideration.

All the identified hazards and hazardous situations are documented in the risk meeting documentation. In the next step, the risk analysis is the associated risk(s) for each identified hazardous situation estimated according to the scales for estimating severity and probability described in detail in Section 3.1.5. The

risk value (R) is calculated for each hazard by multiplying the severity (S) with the probability (P) value, i.e. **Risk =** S x P.

In the risk evaluation step is a decision made for each risk if risk reduction is necessary. The decision is based on the criteria for risk reduction (Section 3.1.5). For all the decided to proceed on, risk control measures shall be discussed and decided on and assigned to usability testing if suitable. The effects of the decided risk control measures are discussed and analysed according to the same scales. New hazards generated from the risk control measures shall be documented and analysed. The remaining risks are accepted, assigned new further measures, or left as residual risks. The implementation of risk control measures is, if possible assigned to a named developer.

Recommendations:

It is recommended that the facilitator of the risk meeting have a strict control of the meeting with the ambition to get opinions from all the participants and thereby avoid dominance factors. Explicitly addressing each participant or giving each participant a specific timeslot can for example accomplish it. Another important factor is to define and separate the estimation of severity and probability and to strictly apply the predefine scales, so that the estimation of the different values do not affect each other during the discussions.

Technical risks identified during the meeting are often of a more general nature and not use case-specific, there is a need for handling them separately, recorded them at the meeting and then transfer them to technical risk analysis.

During the discussions about risk control measures it is common that possible alternative solutions and improvement measures that are not true risk control measures are focused on. This solutions and measures should be documented separately and be discussed on another kind of meeting.

Risk meeting documentation:

The documentation can be documented in a spreadsheet or other preferred format, which are continuously updated during the risk management process. During the meeting it is preferable if the on going documentation can be displayed for all the participants, so it can be seen and agreed on during the discussion.

Since hazards and hazardous situations shall be revaluated over time, must the documented descriptions be detailed and unambiguous, so that the interpretation of the hazards and hazardous situations will be the same from time to time.

Recommendations:

The risk meeting documentation is recommended to record the following:

- Use case id
- Hazard id
- Description of harm
- Description of hazard and hazardous situation
- Estimation of severity and probability
- Risk value (severity x probability)
- Risk reduction, yes or no?
- Description of cause
- Description of measure/s
- Suitable for usability testing, yes or no?
- Responsible for measure (name)
- Follow-up date
- Reassessment severity and probability
- New risk value
- New hazard, yes or no?

Colour coding in the risk meeting documentation facilitates to identify the level of risk acceptance for a hazard and also to identify new hazards. The calculated risk value can be colour codes according to Table 1.

Table 1 Colour coding in the risk documentation

Risk value = red	Risks ≥ 8 shall be reduced or mitigated.
Risk value = yellow	Risks ≤ 7 and 0 shall be reduced or mitigated if the risk analysis team decides so.
Risk value = organge	Risks where the probability of occurrence depends on software, where the severity is greater than 1, shall be reduced or mitigated.
Hazard id [UCx.yHx] = blue	New hazard identified after risk control measures or revaluation of residual risks.

1.5 Scales for estimation and risk acceptance

The risk management process mandates that the risks are assessed independently from other risks and that each variable are estimated in sequence, starting with severity and then followed by probability. The scale for estimation of severity of harm is presented in Table 2 and the scale for estimation of probability of occurrence in Table 3.

Table 2 Severity scale

Severity [Numeric]	Denomination	Example
4	Catastrophic	Death, suicide, persistence of severe disability
3	Major	Sustained moderate disability, significant prolongation of treatment episode
2	Moderate	Temporary disability, prolonged treatment episode
1	Very unlikely	Discomfort or minor injury
0	Insignificant	No consequence

Table 3 Probability scale

Probability [Numeric]	Denomination	Occurrence
4	Very likely	Daily
3	Likely	Weekly
2	Unlikely	Monthly
1	Very unlikely	Ones in 1-2 years
0	Insignificant	Never

When estimating probability it shall be noticed that the probability value documented, the probability of occurrence is a contexture of P1 and P2, where:
P1 is the probability of the hazardous situation occurring.
P2 is the probability of the hazardous situation leading to harm.

The criteria of risk acceptance used in the risk management process mandates that risks ≥ 8 shall be reduced or mitigated and risks ≤ 7 and 0 shall be reduced or mitigated if the risk analysis team decides so, see Fig. 3. Risks where the probability of occurrence depends on software, where the severity is greater than 1, shall also be reduced or mitigated.

Probability	Severity of harm Catastrophic (4)	Major (3)	Moderate (2)	Minor (1)	Insignificant (0)
Very likely (4)	16	12	8	4	0
Likely (3)	12	9	6	3	0
Unlikely (2)	8	6	4	2	0
Very unlikely (1)	4	3	2	1	0
Insignificant (0)	0	0	0	0	0

Figure 3 Criteria of risk acceptance

1.6 Usability testing

Usability testing can indicate hazards that are not identified in the risk management process and render the possibility to verify if risks with high risk value actually cause the presumed problems. The usability test shall be made according to well-recognised methods. The results are then analysed and mapped against the risk values documented in the risk meeting documentation. Reassessments of the concerned risks are made at a risk meeting, risk control actions are decided and the risk meeting documentation is updated.

1.7 Risk management report

The risk management report shall show that the risk management activities have been performed according to the risk management plan and that the overall residual risks are acceptable.

Information important for the production and post-production phase that are gathered and documented during the risk meetings, for example, warnings in the graphical user interface, labelling and special training shall be documented in the report.

Material from the risk management plan can be reused such as a description of the product, intended use, intended users and the risk management process.

1.8 Iterative development

The risk management process can be used in linear development processes but also in iterative development processes. The overall risk management process is the same, but with a smaller scope and new use cases for each iteration. The scope of each iteration is defined in the risk management plan and new risk teams may be added over time due to member changes. The activity in the risk assessment phase and risk control phase stay the same and the usability testing is made for suitable functionality within the on going iteration.

Either small risk management reports are written at the end of each iteration were repeated unchanged parts of the report creates a framework to which the small reports are added or a new complete report for each iteration. However, parts such as description of traceability, risk analysis method and risk estimation scales can be reused.

The different phases in the risk management process can run in parallel for the different iterations. For example, when risk monitoring in on going in one iteration, the preparation and risk assessment can start for another iteration.

1.9 Risk monitoring after release

When the product is released post-production problems shall be reported back to the development organisation. The post-production problems can be reported by, for example, users, customers, service personal, personal who installs the medical device and from incident management systems. Maintenance of the medical devise could be a source to consider according to post-production problems.

The development organisation shall also keep up to date with public available information about similar medical devices on the market.

The post-production problems shall be discussed at a risk meeting and a decision shall be made according to if problems shall be in cooperating in the risk management process or not.