Risk Management Plan

The Risk Management Plan contains the risk policy and defines the criteria for risk acceptance. It also references relevant processes and activities which will be conducted for product-specific risk management as part of the integrated software development process (SOP Integrated Software Development).

Mapping of Standard Requirements to Document Sections

ISO 14971:2019 Section	Document Section
4.1	1
4.2	1.2, 3
4.3	(Records of competence are kept as Part of QMS)
4.4	(all)
4.5	(all)
5.1	1.1
7.2	1.3
10.1	1.4

1. Relevant Processes

1.1 Risk Management Process and Activities

Risk Management Activities are integrated in the software development lifecycle as described in SOP Integrated Software Development. The scope of this risk management plan therefore covers the entire software device lifecycle.

When creating a first-time risk analysis for a product, Annex C of ISO 14971 should be reviewed for applicable examples.

1.2 Risk Policy and Risk Acceptability

The following policy establishes criteria for risk acceptability following ISO 14971:2019 and ISO/TR 24971:2020. It applies to all people and activities involved in the design, development and distribution process of the medical device, and intends to ensure highest levels of medical device safety consistent with stakeholder expectations.

The manufacturer defines framework criteria for risk acceptability in the form of estimated usage, severity of harm and probability of occurrence. The criteria are initially defined as part of the early software development process and reviewed during each post-market surveillance cycle.

Estimated usage, categories of severity / probability and risk matrix acceptance are defined based on applicable regulatory requirements, relevant international norms and standards, as well as the generally acknowledged state of the art

(e.g. accepted results of scientific research, reports published by authorities, established industry best practices).

Acceptability for individual risks always must be established based on both, the estimated severity and the estimated probability of a risk. The risk is deemed acceptable based on a combination of both, following the risk matrix defined in para. 1.2.4.

All identified risks must be reduced as far as possible (AFAP) without adversely affecting the benefit-risk-ratio. Risk control measures implemented to reduce the risks must be chosen in the following order:

1. Inherent safety by design
2. Protective measures
3. Information for safety

Users of the device must be informed about any remaining residual risks.

Acceptability of the overall residual risk is established as part of the clinical evaluation process by weighing benefits from intended use against the overall residual risk. Benefits may be described by their magnitude or extent, the probability of experience within the intended patient population, the duration and frequency of the benefit. For example, the manufacturer may compare the device to similar medical devices available on the market: residual risks can be compared individually to corresponding risks of the similar device, considering differences in intended use. The overall evaluation of the benefit-risk-ratio should take into account knowledge of the intended medical indication, the generally acknowledged state of the art in technology and medicine, and the availability of alternative medical devices or treatments.

1.2.1 Estimates for Usage

> Define estimates for how much you think your device is going to be used in the market.

Usage	Values
Product life span	Enter number of years you expect the device to be in the market (from design conceptualization to decommissioning)
Users	Enter number of estimated users here
Usages / user	Enter number of estimated times the device is used per user
Total usages	Do the math!

The software's lifetime is established to be [for example: three years]. This is what is expected to be the maximum time until the implementation of a significant change, by which the manufacturer is able to react to the relevant

changes to the software device environment, such as SOUP changes, cybersecurity innovations, or the evolving technological or medical state of the art.

Estimated product lifetime may not align with the planned PMS / PMCF surveillance periods, as continuous risk management involves continuous updates of the risk management file in order to account for new information in a timely manner.

1.2.2 Severity of Harm

> Define what can go wrong with your product here. Make the examples specific - chances are, your product can't cause skin lacerations. In all likelihood it also doesn't cause death. So, feel free to remove severity rows here. But most importantly, customize the definitions and examples so that they resemble the harms in your product.

Severity	Definition and Examples
S1: Negligible	Minor, reversible damage, e.g. superficial skin irritation, delay of non-critical treatment
S2: Marginal	Minor, reversible damage with required medical intervention, e.g. skin laceration requiring stitches
S3: Critical	Major, irreversible damage with required medical intervention, e.g. irreversible deterioration of disease
S4: Catastrophic	Death

1.2.3 Probability of Occurrence

> Define your probabilities. You can probably just use these definitions. The idea is that each probability row is 10^2 apart from adjacent ones.
>
> Also, change the "Estimated Maximum Event Count". That's the usage number you estimate for your (not yet released product) during its entire lifecycle (which you need to define). So, if you assume that your product will be on the market for 4 years and that it'll be used 100 times per day, that results in 146.100 usages (100 usages/day * 365.25 days/year * 4 years). The numbers in the lower columns of "Estimated Maximum Event Count" are simply the total usage number multiplied by the upper limit probability of the same row, e.g. you want to know "how often can probability P3 occur if the product is being used 100 times per day?"

Probability	Upper Limit	Lower Limit	Estimated Maximum Event Count
P5: Certain	1	10^-2	1000000 *(change this)*
P4: Likely	10^-2	10^-4	10000
P3: Unlikely	10^-4	10^-6	100
P2: Rare	10^-6	10^-8	1
P1: Unthinkable	10^-8	0	0

1.2.4 Risk Acceptance Matrix

The most important part. You assess each severity-probability combination whether it's acceptable for you as a company. There are no definitive rules on what's deemed acceptable. It depends on your company's risk policy and, more importantly, the benefits of your product which you show in your clinical evaluation. So, for example, if your product saves 10 lives per day, it might be acceptable to cause one death per day. If your product doesn't save any lives, it might not be acceptable to cause any deaths. You get the idea, I hope.

Probability	S1: Negligible	S2: Marginal	S3: Critical	S4: Catastrophic	Estimated Maximum Event Count
P5: Certain	acceptable	**unacceptable**	**unacceptable**	**unacceptable**	1000000
P4: Likely	acceptable	**unacceptable**	**unacceptable**	**unacceptable**	10000
P3: Unlikely	acceptable	acceptable	**unacceptable**	**unacceptable**	100
P2: Rare	acceptable	acceptable	acceptable	**unacceptable**	1
P1: Unthinkable	acceptable	acceptable	acceptable	acceptable	0

1.3 Verification of Risk Control Measures

Risk Control Measures are verified as described in the software development lifecycle as described in SOP Integrated Software Development.

1.4 Assessment of the overall residual risk

After determination of the Risk Control Measures any risk that could arise from the combination of the individual risks or mitigating measures is assessed. For this purpose, the probability and severity of the possible residual risk are estimated and evaluated using the existing risk matrix.

1.5 Collection and Review of Post-Production Information

Review and collection of Post-Production information is described in SOP Post-Market Surveillance.

2. Related Documents

- SOP Integrated Software Development
- Risk Acceptance Matrix
- Risk Table
- Risk Management Report

3. Roles

Title	Name(s)
Risk Manager	
Context / Subject Matter Expert, e.g. physician	
