Risk Management Series – Article 9: Risk Management Report

Foreword
MEDlcept presents this ongoing series of articles focused on the implementation and practical conduct of risk management in the medical device industry to provide practitioners with insight into how to apply risk management principles and tools to improve the performance and safety of their devices; and, as an added benefit, to maintain compliance with risk management standards.

Our team at MEDlcept publishes these articles to capture best practices, to explore the more challenging aspects of maintaining risk management systems over the long term, and to elicit discussions among practitioners.

To this last point, if you have questions or comments on the issues discussed, or if you have recommendations for topics to consider in the future, please let us know: 508-231-8842.

Introduction
Our last article, Risk Control and Verification (RM8), described the standard approach (i.e., ISO 14971) for identifying appropriate risk controls – following the priorities: inherent safety by design, protective measures, and information for safety. It also, addressed the importance of verification and provided some guidance for determining the most appropriate approach for conducting your verifications. This article describes the Risk Management Report – i.e., summarizing the work that has been done, assessing the overall residual risks, and describing how risks will be managed going forward.

Risk Management Report – Bringing it All Together
Working with a wide range of medical device companies (by both product type and company size) we spend a lot of time reviewing risk management documentation. Whether it’s during an audit, as part of a regulatory submission, preparing a Clinical Evaluation Report, or a focused risk management project; far too often we see that Risk Management Reports are missing or seriously
incomplete. In the worst cases, risk assessment documentation ends with an FMEA and we’re left to read through pages of spreadsheets to come up with our own assessment of the risks.

Companies will often be able to provide a Risk Management Plan, but a complete and comprehensive Risk Management Report is less common. Even when there is a report, if the content of the report is limited to “risk analyses were conducted in accordance with the risk management plan and the overall residual risks were found to be acceptable” (or something similar) it doesn’t provide the reader with much of an understanding of why the organization considers the risk to be acceptable and how the residual risks will be managed.

A weak Risk Management Report is an indication that the organization is not taking risk management seriously. A report that is limited to the “all risks were found to be acceptable” statement often seems to imply that the organization is say: “Yes, we’ve gone through the risk analysis exercise, this proves it, and now we don’t have to think about it anymore.”

Risk Management is not that different from design verification or validation. In those activities, engineers write a protocol (the plan), conduct the study (the analysis), and write a report to summarize the results. That report identifies what studies were completed, whether there were any deviations from the protocol, what next steps need to be performed, and (most importantly) whether the results demonstrate that the device met the protocol objectives. The Risk Management Report serves the same purpose – it summarizes the results of all the risk management activities to document that:

- The risk management plan has been appropriately implemented;
- The overall residual risk is acceptable (or not); and
- Appropriate methods are in place to obtain relevant production and post-production information
After a brief discussion of Risk Management Plans (missing from previous White Papers), this article will describe what should be included in a Risk Management Report, how to think about the acceptability of overall risk, and how consideration of the benefits of the device fit into the overall assessment of risk acceptability. Most importantly we emphasize the importance of not just stating that the risks are acceptable, but documenting why they are acceptable.

**Risk Management Plans**
Looking back over past articles, we see that we haven’t focused much attention on the Risk Management Plan (although we do address establishing the risk management scope in RM2: Prioritizing Risk Management Activities). This is an oversight, because the plan is a critical element of the overall process. So here’s a quick overview of the Risk Management Plan to make sure that we’re on the same page.

The Risk Management Plan establishes the scope of the risk management activities for a particular medical device or family of medical devices. It also establishes the responsibilities and authorities for key activities, particularly the review of risk management outputs. The plan can be a standalone document (for big projects), or incorporated into the overall development plan.

To provide broad guidance on risk management, most companies maintain an SOP. Typically this SOP will mirror the ISO 14971 requirements and include a few elements that are specific to the company – e.g., how the risk management activities fit with design control activities, what groups have responsibility for specific risk management activities, etc. Often, the SOP also includes criteria for estimating the probability of occurrence of harm, assessing the severity of those harms, and determining which risks are acceptable and which are not.

These standard criteria and approaches may not be appropriate for all devices and risk assessment projects. That’s where the Risk Management Plan comes in - it provides you with the opportunity to customize your standard approach and
evaluation criteria to the needs of a particular device. For example, if your company manufactures both defibrillators and heating pads, you would probably be willing accept the risk that a patient may suffer a serious burn from the defibrillator, but not from the heating pad. In the first case, you’re saving a life. In the second case, you’re only providing temporary relief from aches and pains. Your criteria for risk assessment need to be aligned with the benefits of your device.

Risk Management Plans give you the opportunity to supersede (with proper justification) elements of your Risk Management SOP. If the risk acceptance criteria in the SOP is not appropriate to the risk-benefit profile of the device being considered, more appropriate criteria can be established in the Risk Management Plan. If your SOP requires that a process FMEA be conducted, but in this case the product is going to be manufactured by a third-party, you can justify that change in the plan. Similarly, if your SOP does not address the use of Fault Tree Analysis (FTA), but you determine that one would be valuable for a particular product line, the scope of the FTA activity can be clearly stated in the plan.

Since the Risk Management Plan is a controlled document, it must be reviewed and approved by management (typically as part of a Design Review) and changes to the plan must be recorded and maintained in the Risk Management File. Therefore, the plan becomes the vehicle communicating any deviation from the SOP and gaining management approval for moving forward with a customized – and hopefully more appropriate – plan.

**Risk Management Report - Contents**
The major elements of the Risk Management Report are:

- Reference to the Risk Management Plan
- Risk management activities completed (including deviations from the plan and references to relevant documentation, e.g., FMEAs)
• Identification of significant residual risks and, if appropriate, plans to monitor and manage those risks
• A statement describing the acceptability of the overall residual risks

Just as a design validation report identifies any excursions from the established protocol, the Risk Management Report identifies any gaps between the planned risk management activities and what was ultimately completed. Since the plan is a living document (the plan can be updated and re-approved multiple times over the course of development effort) there typically shouldn’t be too many gaps between the final, approved plan and the final report. That said - if there are any deviations, this is the place that they should be documented and the justification for the gap should be presented.

The following sections address how overall residual risk can be assessed and provide guidance on the “risk acceptability” statement. In general, the keys are to highlight those elements of risk that deserve special attention during the post-product phase of the product lifecycle and to place the overall residual risks in the proper context so that the reader understands why the residual risks are acceptable.

Acceptability of Overall Residual Risk
In our article, Determining Risk Acceptability (RM7), we talk a lot about how to make judgments about which risks are acceptable and which are not. We also discuss the differences between Residual Risk (which is the risk associated with an independent hazard and a specific cause) and Overall Residual Risk (which is the risk associated with all hazards and causes). The Risk Management Report is the place where the Overall Residual Risk should be presented in a clear, concise manner so that management can make a judgment as to whether the device is safe enough to be placed on the market.
As described above, you will often see a statement in the Risk Management Report that says something along the lines of “risk analyses were conducted in accordance with the risk management plan and the overall residual risks were found to be acceptable.” Typically, what this statement means is that each individual risk has been assessed with regard to the risk acceptability criteria and each falls into either the “BA” (Broadly Acceptable) range or the “ALARP” (As Low as Reasonably Practicable) range.

But are all combinations of BA / ALARP risks the same? Maybe . . . maybe not.

Take a look at Products 1 through 5 that are described below. The “Management has reviewed . . .” statement is certainly appropriate to the risk profile of Product 1 - our baseline example with ten risks spread across the BA and ALARP regions. But it also applies to the risk profiles of Products 2, 3, and 4. All four of these products have risks are all either Broadly Acceptable or ALARP.

Is the overall residual risk of each of these the same? Not at all. If forced to rank Products 1 through 4 from lowest to highest risk, we would argue that it’s pretty clear that the order should be Product 3, 1, 2, and then 4. However, based on the established risk acceptability criteria (as illustrated by the matrix), they are all acceptable. The only risk profile that is not acceptable is Product 5, due to a single risk in the Unacceptable region.

<table>
<thead>
<tr>
<th>Severity of Harm</th>
<th>Probability of the Occurrence of Harm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 Low</td>
</tr>
<tr>
<td>5 High</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1 Low</td>
<td></td>
</tr>
</tbody>
</table>
If you were the manager with responsibility for product safety for the five products represented by these five figures, which would keep you awake at night?

While the Risk Management Reports for Products 1-4 could all include the statement that “all individual residual risks are acceptable”, there’s still a question as to whether the “overall residual risk” is acceptable. Both Products 2 and 4 have a good number of risks in the ALARP region. That information should be clearly expressed in the Risk Management Report along with detailed plans for how post-
production information is going to be captured and evaluated to ensure that risk estimates are not understated.

Management needs to be made aware that while all risks for Products 1-4 are considered to be Acceptable, there are a lot of risks right on the Unacceptable border. With this understanding, they may determine that overall risk is not acceptable even though all individual risks fall below the Unacceptable line.

One could argue that the overall risk of Product 5 is lower than either Products 1, 2 or 4. While there is a single “unacceptable” risk, all other risks are quite low. If a risk-benefit analysis indicates that the benefits of the device outweigh this one risk, appropriate information can be provided to users about the risk and appropriate risk monitoring systems can be put in place. What’s nice is that it’s just one high-level risk to be monitored and managed. The other products may actually present a greater risk management challenge; since more comprehensive monitoring and management is needed to ensure that none of the multiple ALARP risks are, in fact, Unacceptable.

**What about Benefits?**

One important element that is almost always missing from a Risk Management Report is any mention of the benefits of the device. While a “risk benefit” analysis is not required (unless any one risk, or the overall residual risks, are considered Unacceptable), stating that the identified risks are acceptable without any mention of benefits results in a hollow statement about risk without the context needed to provide the reader with a full understanding of why those risks are acceptable.

In most cases, a brief description of the intended use of the device, indications for use, and/or patient benefits will be sufficient to place the overall residual risk in its proper context. This addition to the report will help to bring all the pieces of the risk management effort together in one place so that management and other reviews can gain a complete understanding of the risk profile of the device.
Conclusion

The bottom line is that it is not sufficient for the output of your risk assessment activities to be a stack of FMEAs that a reviewer would need check line-by-line to understand the risk profile. It is also not sufficient to prepare a report that is limited to the statement that “all overall residual risks are acceptable”. The Risk Management Report needs to confirm that the risk management activities were completed in accordance with the plan (and if there were any deviations); summarize the results of the activities; and identify what steps need to be taken to ensure the ongoing safety and performance of the device.

The summary of the results of risk management activities should identify any risks that are of particular significance and what monitoring activities will be implemented to ensure that the risk estimate is accurate — or, if it’s not accurate, what changes to risk controls would be appropriate. In many cases, your established complaints monitoring system may be appropriate. In other cases, more frequent monitoring to identify trends or additional/focused questions in the complaint intake form may be warranted.

Finally, the Risk Management Report should be explicit about why the overall residual risk is acceptable. By adding “because . . .” to the end of the “all residual risks are consider acceptable” statement, you will be able to provide the context for why your organization is comfortable in accepting certain risks given the benefits of the product based on the intended use. Going back to the defibrillator example, by stating that the overall residual risks (including patient burns) are acceptable because the device provides life saving treatment for cardiac arrest, the risks are put in the proper context relative to the benefits of the device. The organization is likely to accept the overall residual risk. It is less likely that an organization would be willing to make a statement that similar risks are acceptable for a heating pad because it provides temporary relief from aches and pains.
Next Steps

This article concludes our first pass through the risk management process. Up to this point our focus has solely been on planning and conducting risk assessments, implementing and verifying controls, and the process and approvals. That’s not the whole story . . . in fact, it’s just the start. If you compare risk management to a house, at this point the house has been built, but no one is living in it yet. Future articles will address the use of risk management over the lifecycle of your device (e.g., risk management’s role in change management, post-production vigilance, etc.). We’ll also dig into more details about estimating the probability of the occurrence of harm, assessing severities, and determining risk acceptability (these can be complex topics, so there’s always more to say).