For want of a nail…
The benefit of implementing a robust Risk Management program and pitfalls to avoid

Part 1: General Overview

ISO 14971:2007 defines risk as *the combination of the probability of occurrence of harm and the severity of that harm*. **ISO 31000:2009** defines risk as *the effect of uncertainty on objectives*.

As medical device manufacturers we also recognize both **consumer risk** – *the risk of accepting a bad part as good* (beta error) and **producer risk** – *the risk of rejecting a good part as bad* (alpha error). Anecdotally, I tend to think of risk as *opportunity for disaster* (OFD).

A risk management program is a series of interrelated processes and tools, designed to identify, describe, assess, mitigate and track risk, thereby managing organizational risk. Industry has various types of tools to both identify and assess risk, such as Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA). We also have the means for ranking risk which then allows us to prioritize how we allocate resources to deal with that risk. The most commonly used metric is the risk priority number (RPN). Another commonly used tool is Strength-Weakness-Opportunity-Threat (SWOT) analysis.

The attempts to prevent risky events from occurring are called risk mitigation. The preferred hierarchy for risk mitigation is:

1. Design it out
2. Alarm when it occurs
3. Warnings (labeling) that risk laden event could occur

After all efforts at risk mitigation have been implemented, a new risk assessment is performed and this new assessment value is considered the residual risk. A risk management plan is a living document that must be continually updated, and those updates responded to when necessary. Once risks have been assessed, potential causes identified, potential impacts contemplated and mitigation strategies developed, a model is developed which includes residual risk. Every effort should be made to continually update the risk model to take into account data from the field as well as, ongoing production information.

Instilling Robustness

For a truly robust risk management program, the program should encompass all aspects of a product life cycle from design to end-of-life disposal. This means that executive level management must be involved from the start, in order to allocate the appropriate resources to develop and implement a robust risk management program. Teams when formed should be cross functional in nature, in order to model the broadest possible range of risks. Also, often in the medical device field our risk classifications are tied to the FDA classifications of mandatory reportable events, for example:

Critical - Likely to cause death or serious harm

Major - Not likely to cause death or serious harm, but may possibly cause injury

Moderate -Remote possibility that malfunction could cause injury

Minor - highly unlikely to cause injury or harm

So what happens if as a medical device component manufacturer, you don't have access to the data that would allow you to make the above determinations? Then you need to expand your risk classifications. After risk to pubic safety as discussed above, there are opportunities to categorize, plan for and react to, other types of risk. For example:

a. Product risk – nonfunctional, functional but out of dimensional tolerance, visual defect, documentation error etc.
b. QMS risk – missing or faulty element that could lead to other issues, chronic problems, isolated incidents etc. – (addressed by incorporating risk management into your internal audit program)
c. Business risk – cost of failed DOE or other optimization initiatives. Cost of rejecting good part as bad.

By expanding the risk model to incorporate multiple categories of risk, a wider variety of potential failure modes can be identified and accounted for. Accounting for multiple types of risk also allow the risk management process to be more easily integrated with improvement efforts.

Pitfalls to Avoid:

Now that we've covered the basics, let's look at some common pitfalls things that might not be so obvious at first blush.

1. Risk management not fully integrated with other systems (i.e. NCMR, CAPA internal audit etc.). By identifying and classifying various types of risk, the organization knows how respond to internal issues when they arise. One example might be when either a nonconforming material report or audit finding might initiate the generation of a CAPA.
2. Risk management thought of as a set of tools and records rather than a comprehensive program. How often as an auditor have you asked about an auditee's risk management program and were given an FMEA log and records?
3. Use of either quantitative (1 occurrence per 100 opportunities, 1 occurrence per 1000 opportunities etc.) or qualitative (rarely, occasionally, often) assessments solely for frequency of occurrence when there are times that a program may require one or the other, depending on the situation.
4. Risk management is an organic program that must reflect current conditions. There should be a continual feedback and adjustment loop in place. Risk assessments must be updated and controls adjusted, based on both internal and external data. Often there is no process in place to make this determination and implement changes when necessary.
5. Failure to assess any risks that might be associated with efforts to improve.

In conclusion, risk management is a program that is not only required but has value well beyond that of meeting regulatory requirements. When implemented properly, the benefits of having a robust risk management program, go beyond the realm of securing public safety and into the arena of protecting corporate health as well. The next article in this three part series will focus on Assessing Risk.