

Effective Risk Assessment

Risk assessment is a fundamental part of quality assurance. When used proactively, it can detect errors before they occur both in products and processes. At its core, risk assessment is a formal method for identifying risks and making business decisions on whether to address them. In practice, risk assessment is a boring chore that often is neglected in many organizations. The focus of this article is to assist the regulatory affairs professional in identifying when risk assessment should be done, how it can be completed and what role the regulatory affairs professional has in risk assessment.

When to Perform Assessments

Risk assessments should be done during new product development or after significant process changes. In both situations, the product or its method of manufacture is no longer clearly understood, and a systematic method for reviewing and assessing its risks is appropriate.

In new product development, risk assessment should be completed before the first product specification has been completed. Typically, when the first product specification is approved, development quickly proceeds to verify and validate the design and design changes become more difficult to implement. As an example, silicone liquid injection molded medical devices often have an upper specification limit on nitrosamines. If this is known prior to completing the product specification, then heating processes to eliminate the contaminants can be developed and implemented before the complete manufacturing process is finalized.

Risk assessments also should be done or re-examined prior to the initiation of a clinical trial. These often are significant project milestones, and the severity of the application justifies revisiting risk assessments. Particularly for complicated designs, it is important to continually apply lessons learned from bench testing, preclinical trials or early human feasibility studies into the risk assessment process. If it is discovered during a feasibility study that the device is incorrectly used by physicians, the labeling may be inadequate and should be revised, because labeling is used as a control during risk assessment.

Risk assessments also are appropriate prior to the initiation of substantial changes to manufacturing processes. Examples of major process changes would be relocating the process to a new facility or a different area of the same facility, technology upgrades, or new software installation. Moving a process usually includes a validation master plan, equipment qualification, and training new supervisors and operators. The probability for tribal knowledge to be lost is larger, so a risk assessment at this

point would be prudent to ensure that all of the quality and process controls are still in place and effective after the relocation. For example, in a chemical compounding operation, an operator may know that components need to be added in a specific order and rate to ensure thorough mixing. If this is not a standard operating procedure, then risk assessment can highlight the risks associated with mixing and ensure that these user techniques are successfully transferred. An example of a technology upgrade would be changing to a new sealing technology such as radiofrequency sealing from heat sealing. While both processes lead to a sealed package, the process parameters and number of defects would be different. These are essentially new processes to the business, and the old controls and inspections may no longer be appropriate. Finally, new software should almost always have a risk assessment. The software industry is still in the Stone Age from a quality perspective. Indeed, many software vendors routinely release error-ridden codes, figuring they will fix them in the next release. For the software managing or verifying product quality, this is unacceptable, and a risk assessment is fundamental to assuring the quality of the software.

Types of Risk Assessment

Three types of risk assessment commonly are used to manage risk: informal assessment, failure modes and effects analysis, and fault tree analysis. Informal assessments are the catch-all category most risk assessment falls into. It itemizes risks and compares them to industry standards or generic categories of cost, safety, quality and customer satisfaction. For example, the risk assessment of a heat sealing technology for a sterile product may be informally addressed by:

Risk	Safety	Quality	Cost	Customer Service
Product Unsealed	Major	Major	Minor	Minor
Heat Sealer Breaks	None	None	Moderate	Major

The informal process is typically performed by a few people or even one person. Since it does not systematically address every possible failure, some judgment is used as to which risks to include or exclude. Useful for very simple changes, the informal method is not really appropriate for more complicated risk assessments.

The failure mode and effects analysis (FMEA) is probably the most common formal risk assessment used today. Pioneered by the automotive industry, FMEA has spread to many FDA-regulated industries and is recognized by most auditors. FMEA is a bottom-up approach, in which every step in a process or feature of a product is listed and its possible failure modes identified.

Each failure mode is assigned a severity on a scale from 1 to 10 with 10 being the most severe. The methodology then proceeds to identify possible causes for each failure mode and to assign a probability from 1 to 10 with 10 being highly likely. After this, the team usually looks at the current process controls to determine how easy it is to detect each failure mode. The detectability for each failure mode is also estimated from 1 to 10 with 10 as perfectly detectable with the current inspection systems or controls. An overall risk priority number (RPN) is calculated by multiplying the severity, probability and detectability. With risks then running from 1 to 1,000, a cutoff is established and risks above the threshold are addressed with a combination of design changes to reduce frequency or controls to improve detectability to bring down the overall RPN. An example of a FMEA for the previous heat sealer would be:

The RA Professional's Contribution

With risk assessment typically executed by the engineering or quality assurance functions, it is imperative for the regulatory affairs function to be involved in the assessments. Engineers typically focus on the safety and functionality of the design, while quality often targets controls and inspections. The RA professional can incorporate regulatory risks by accurately assessing the compliance severities and ensuring that controls do not affect any regulatory submissions.

Different regulatory risks are routinely underestimated by manufacturing such as product mislabeling or mix-up. Often seen as a minor violation of the Good Manufacturing Practices since no actual product was lost, the RA professional can train the team performing the risk assessment to understand the implications associated with the distribution of adulterated products.

Feature	Failure Mode	Severity	Possible Causes	Frequency	Controls	Detectability	RPN
Heat sealer platen	Platen too cool to seal bags	10	Platen damaged	9	Preventive maintenance schedule	5	450
			Defective	2	Temperature verified prior to use		100
			Dirty	7			350

Therefore, if the cutoff was established at 400, then actions would be taken to reduce the probability of the platen being damaged with sealing or improve the detectability. This could include a visual inspection of the platen prior to sealing or designing a fixture to hold the bag so as to protect the delicate part.

The disadvantage of FMEA is that it can be extremely time consuming. While very thorough, the multidisciplinary nature of the assessment can absorb a tremendous amount of resources to complete a relatively routine product assessment. Despite its shortcomings, its popularity for risk assessment is justified as it is a reliable methodology for managing risks.

Another type of risk assessment not applied as frequently is fault-tree analysis (FTA). More common in reliability engineering, FTA is a top-down approach that first looks at system failures and tries to categorize the failures into individual subsystem failures assigning each a probability. At the end of this assessment, probabilities are calculated for each branch to determine the possibility of a system failure. Using the heat sealer example, FTA might look like this:

Sterility failure = (heat sealer failure OR raw material failure OR package breach).

Heat Sealer failure = (platen damaged AND NOT detected during preventive maintenance) OR (defective platen AND NOT detected during installation).

It can be fairly complicated, but it is still sometimes used.

Proposed controls also may compromise the quality or integrity of a submission. If the manufacturing section of a submission indicates that a process is under statistical control and no inspection will be performed, and the quality department is recommending 100% inspection to mitigate a risk, then there is a discrepancy between what is said and what is done. The process is not truly under control with respect to all parameters, and the submission is inaccurate. Likewise, controls often include additional labeling for internal use only; therefore, additional controls or procedures must be implemented to ensure that this unapproved labeling is not left on the packaging and sent to customers.

Conclusion

Risk assessments should be done during new product development and before major process changes. Using informal assessments or the formal failure mode and effects analysis and fault tree analysis can provide systematic and repeatable determinations of risk and their effect on the product and consumers. Regulatory affairs professionals should be involved in this process to ensure that compliance risks are accurately determined and that controls do not undermine current submissions standards.

Jeffrey C. Stephens is the president of Ixian Consulting Inc., a management consulting organization specializing in improving the quality of a firm's products or services.