Basics of ISO 9001:2015 Risk Management

Advisera
Making certification simple.

Table of Contents

Introduction

Risk-based thinking is a new concept in the ISO 9001:2015 standard, and this has caused many companies to search for an easy way to manage the risk in their companies. By focusing on understanding your risks through a simple risk management process, you can focus your attention more on addressing the risks that are present for your organization rather than struggling with a complex process that will take excessive amounts of time and resources for little return on investment.

1. Purpose

This white paper is intended for companies that are looking for a simple risk management process to support their implementation of an ISO 9001:2015 Quality Management System (QMS). A basic risk management process can be beneficial for a company by allowing them to focus their QMS on preventing problems from occurring, rather than being strictly reactionary. This paper describes the suggested steps in a basic risk management process, and is supported by this downloadable Diagram of 4 steps in ISO 9001 risk management.

2. What is risk management?

What is risk management, and what is required by ISO 9001:2015? Strictly speaking, ISO 9001:2015 requires a risk assessment process, whereby you identify what risks are present and decide what you will do about them. Risk management takes this one step further by tracking and managing the risks until they are eliminated, or until the time when they could have happened has passed. This basic risk management is a cyclical process in which a company will identify what risks exist, determine what actions to take (if any) to control or prevent the risks from happening, and then continue to track the risks to see if they occur.

Risks are defined as the effect of uncertainty or, in other words, the potential for something happening that you cannot be certain about. This is more often thought of as the potential for bad effects to happen, rather than the risk that good effects could happen. Because we think about risk as predominantly bad effects, risk management is the activity that we do to prevent these bad things from happening.

This cyclical process will allow you to keep track of the risks that you foresee as possibly happening, as well as the actions and controls you have in place to treat these risks. Risk treatment can take the form of eliminating a risk, reducing the possibility that a risk will happen, mitigating the impact of a risk, having plans in place to respond to a risk when it happens, or even accepting a risk as it is and taking no action.

For more information on risk assessment in the ISO 9001:2015 QMS, see this article: The role of risk assessment in the QMS.

3. The importance of risk management

Why should you use risk management in your organization? This is a common question that many quality professionals are asked. For busy managers who are focused on short-term objectives and trying to fix problems that are already happening, risk management can seem like a time-consuming process that doesn't help them right now, and they are not wrong. Risk management is about preventing problems in the long term so that in the future, you are not constantly dealing with problems, but rather preventing problems from happening. This is why the ISO 9001:2015 standard has included assessment of risks and opportunities in the requirements for a Quality Management System.

For more on risks and opportunities in the ISO 9001:2015 standard, see this article: How to address risks and opportunities in ISO 9001.

So, why has this been included in ISO 9001:2015? Many of the changes in the ISO standard for Quality Management Systems have been put into place after reviewing the problems that caused many companies to go out of business during the global economic downturn of 2007-2008. When looking at companies that survived these financially troubling times, it was found that one of the things done by these companies, as compared to their counterparts who did not do as well, was that they proactively reviewed and addressed risks in their processes and found ways to prevent or deal with these problems before they occurred. The need for this process is the driving force behind the inclusion of requirements for addressing risks and opportunities in ISO 9001:2015.

For companies that want to improve their ability to weather the storms of problems that are likely to occur in their processes, risk management is an important part of the Quality Management System. Therefore, ensuring that you know how to assess your risks and put in place controls when necessary is critical to the overall success of your QMS processes. By managing the risks that could cause you problems, you will find that you can more easily deal with the negative consequences of these problems should they occur.

For a better understanding of the risk management process, see this webinar: How to implement risk management in ISO 9001:2015.

4. Four-step risk management process

Now that you know what risk management is, and how it differs from risk assessment, you can determine how you will choose to perform it in your organization. There are many different ways to address risk within your organization, and many tools that are available to help with this process, but unless you have a customer or industry requirement for extensive risk management activities these processes and tools can be excessive and overwhelming. If you are using risk management as a way to improve the processes within your QMS, then a simpler process is sufficient.

So, what are the basics of risk management? For a simple four-step risk management process, consider following these steps:

Step 1: Define how the risks will be addressed and treated

While a procedure is not required for risk management, having a process defined to determine the who, what, where, when, why, and how of risk assessment will make sure that this process happens correctly in your company. Who is responsible for risk assessment in the process? What needs to happen when a risk is identified? Where in the process will risk assessment happen? When does risk assessment need to occur, and when does it not? Why are you performing risk assessment (this can greatly affect the detail required)? How is risk assessment done, and how are risk treatments recorded, controlled, and communicated?

Like all procedures in your company, a procedure for risk assessment and management should include some important information such as the identification and description of the procedure (e.g., a title, date, author, or reference number) so that employees know what the procedure is about and who to talk to if they need clarification. Likewise, having a format that ensures that it is easy to find the who, what, where, when, why, and how of the procedure can make it easy for employees to know what exactly they need to do for risk management in the organization.

For a sample look at a procedure for this process, see: Procedure for addressing risks and opportunities.

Step 2: Identify the risks

Now that the procedure is defined, the next step is to identify what risks exist that could affect your QMS. There are some questions that can be asked to help you to identify what risks exist, such as the following: Can you meet all the requirements for delivering your products and services? Do your suppliers pose any risks to meeting your end goals? What controls need to be put in place for your company processes to ensure that they operate correctly to give you the outputs you desire?

For example, you may identify a risk that one of your suppliers has issued a notice that they will stop making a critical component of your product, without which your product will not work. A second risk that could be identified is that one of your processes has the ability to create bad parts if a certain piece of equipment wears down.

For a better understanding of how to analyze risks, see this article: Methodology for ISO 9001 risk analysis.

Step 3: Evaluate how significant the risks are

It should come as no surprise that not all risks are equally important. Some risks have a much lower chance of occurring, while others will definitely happen if you do not stop them. Likewise, some risks will cause a lot of problems if they do occur, while others will be hardly problematic or be very easy to fix when they happen. It is even important to consider how likely it is to notice the event when a risk happens—if it is likely to go unnoticed, but would cause a large amount of trouble, then working to ensure it does not happen could be critical. For those who are familiar with using a Failure Modes and Effects Analysis (FMEA) process, you will remember that each identified risk is assessed based on the severity of the effect, the likelihood of occurrence, and the chance of detection due to the controls in place.

For the example above, where a supplier has notified you that he will stop making a component, you would likely evaluate the risk as very significant, as it would hamper your ability to deliver your product to your customers. The second example, where equipment wear would create bad parts in a process, may not be a significant risk if the cost of the scrap is low and the chance of detection is high (e.g., you notice and simply fix the process with only $3 worth of scrap each time). In your assessment, you will want to look at three things: severity, occurrence, and detection. How severe is the problem that would be created by the risk if it occurred? How likely is the risk to occur? How likely are you to detect the problem if it occurs? Even if you do not use a formal FMEA template, using these assessment criteria will help you to determine if the risk is significant enough to do something about.

For more information on identifying risk significance, see: How to identify risk significance in ISO 9001:2015.

Step 4: Identify controls and other options to decrease risks

What do you do next? You will then need to expand your thinking about each risk. If a risk can cause a problem that will create difficulty for you, and has a 50-50 chance of happening, then you will need to assess what you will do about it—in other words, what controls you will put in place. Remember that you can also choose to do nothing if the significance of the risk does not warrant action. Knowing how significant the risk is—or, in other words, how it will affect you—is the first thing you need to do before deciding how you are going to react. What controls will you put in place?

To make risk-based thinking work for your organization, you will want to make your risk controls match your risk significance. So, after determining which risks are significant, what do you do? You will want to determine what controls to put in place for each risk, but how do you do this? The secret is to use the risk significance to decide what level of control is needed.

So, once you know how significant a risk is, it becomes easier to know what you need to do about it. Very significant risks need more attention and bigger plans than those that do not present a significant risk. You may put in an engineering control to stop a significant potential risk from occurring, while a slight risk that can be noticed and fixed easily with little cost or time impact may just be monitored with a plan of action when it happens. The controls or other options need to be assessed against the significance of each risk it is designed to address.

With the example of the supplier discontinuing a part, you could either take action to find a new supplier, or you could find a replacement part—which would mean a re-design and potential re-validation of your product to accommodate this change. This risk treatment plan could be long and multifaceted, including

a plan that addresses both the supplier search and the product re-design activities in parallel. Addressing such a complex risk could take significant resources in time and effort to mitigate.

For the example of a process creating scrap parts due to wear of a machine, there are likely several risk treatments that could be considered. Replacement of the machine could be expensive and not cost-effective for the value of the scrap it would save; likewise, a preventive maintenance process would need to be assessed for cost-effectiveness due to the complexity of the preventive maintenance or the downtime encountered. It is even possible that you could simply accept the risk of creating bad parts and simply monitor the process so that you notice when bad parts are created, at which point a simple adjustment can be implemented.

The important thing to do is to ensure that any controls that you decide are necessary become an embedded part of your QMS processes, so that they are not overlooked. Monitoring and measurement activities need to become part of the regular process, and any controls that are in place need to be understood by those operating the process in question, so that they know not only what is to be done, but why controlling this risk is important. Awareness training of the risks in the process is critical, as this knowledge could mean the difference between employees reacting appropriately when problems occur, and losing valuable time and money from having delays in stopping an issue.

For more information on awareness training, which would include risk awareness, see: ISO 9001 awareness training material: How to create it, what it should contain.

For more information on identifying risk controls, see: How to identify risk controls in ISO 9001:2015.

This concludes the four-step process for risk management, but one additional stage to add is the periodic risk review. While not one of the four steps, having a periodic risk review is an important link that makes this four-step process into a cycle. Within your QMS, there are several processes in which a risk review is helpful, and assessing risk at these times by using the four-step process will help you to ensure that you do not overlook any risks. These processes include QMS planning, planning and control for product and service processes, design, purchasing, internal audits, and corrective actions. Including risk assessment in these processes gives you a periodic review of your risks, and is one way to ensure that you have an ongoing assessment of what risks need to be addressed within your company. This risk review should also include a review and update of the risk management process to ensure that it improves and remains useful for your organization.

5. Check out sample documentation

Along with the individual document samples referenced in this white paper, you can see more documents available to help you implement ISO 9001:2015 more easily. One option is the ISO 9001:2015 Risk Management Toolkit; however, for full ISO 9001:2015 implementation resources, you can see the ISO 9001:2015 Toolkit Product Tour to allow you to see sample policies and procedures required by the ISO 9001:2015 standard.

6. Sources

9001Academy

International Organization for Standardization

9001 Academy
ISO 9001 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORE **ADVISERA**

9001 Academy
9100 Academy
13485 Academy
14001 Academy
16949 Academy
45001 Academy
20000 Academy
27001 Academy
EUGDPR Academy
Conformio
eTraining
AdviseraBooks

Advisera
Making certification simple.