Risk Oversight

The Risk Oversight chapter is meant to lay the foundation for the entire risk management section.

We will start by answering the question- **what is Risk**?

Then what are the **different types of Quality Risks** to be aware of.

We will follow that up with a review of the Risk Management process and how risk management should be integrated into the Quality System(QS).

We will then dive into the relationship between Risk Management & Quality Management; and how risk management can be integrated into each of the various topics within the CQE Body of Knowledge.

What is Risk (Severity & Likelihood)

From a very generic perspective, Risk can be thought of as the *effect of uncertainty* on our desired *goal*. Within the world of Quality, our desired goal is generally described as "***high quality"*** or "***customer delight"*** or "***conforming product***".

It's important to remember though that uncertainty can work both ways. It can have a either negative or positive impact on our goals. You can have good luck or bad luck.

For example, if you were to look at the integration of risk management into Project Management, you may experience uncertainty that works in your favor. Most often however, especially in the world of quality, **we generally think of the consequences being a negative event .**

This is essentially because our product should work correctly every time, and there generally isn't any room for any additional positive events when it comes to our products.

So in Quality Risk Management we tend to focus on how uncertainty can result in a negative impact on our product.

Therefore, the definition of risk as it relates to Quality Management has been more narrowly defined as the combination of the probability of occurrence (likelihood) of a negative event and the severity of that event.

$$\boldsymbol{Risk = Severity \times Occurrence}$$

That negative event can be as small as a non-obvious cosmetic issue or as severe as death or serious injury to your customer.

Below is a Risk Ranking Matrix that shows the relationship between the calculated Risk value (Numbers in the matrix) and the Severity of Occurrence (Y Axis) and the likelihood of Occurrence (X-Axis). As either increases, Risk increases.

This matrix assumes that the scales of your Risk Analysis for both Severity & Occurrence are a 10x Scale from 1 - 10; with 1 being the least severe or least likely value and 10 being the highest; however this scale is arbitrary.

Severity of the Event										
	10	10	20	30	40	50	60	70	80	90	100
	9	9	18	27	36	45	54	63	72	81	90
	8	8	16	24	32	40	48	56	64	72	80
	7	7	14	21	28	35	42	49	56	63	70
	6	6	12	18	24	30	36	42	48	54	60
	5	5	10	15	20	25	30	35	40	45	50
	4	4	8	12	16	20	24	28	32	36	40
	3	3	6	9	12	15	18	21	24	27	30
	2	2	4	6	8	10	12	14	16	18	20
	1	1	2	3	4	5	6	7	8	9	10
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
		Probability of Occurrence of the Event									

Types of Quality Risks to Manage

As we talk about integrating risk management into the quality system, it's important for you to know the different types of risks that you'll need to consider.

Essentially, for every area of business or life, there is risk. That is to say, there is some uncertainty that we won't achieve our goals.

From a quality perspective, we have to manage the risks that might prevent us from achieving our goal of a high quality product or customer delight. Hence the name Quality Risk.

The risks to Quality comes in a few different forms and are categorized based on the impacted stakeholder:

- **User Safety Risk** - This area of risk is generally the most severe and can include things like personal injury or death to your customers.
- **Product/Reliability Risk** - This area of risk captures any event that has an impact your product and it's quality, functionality or reliability, which implies a reduction in performance or quality over time.
- **Compliance/Regulatory Risk** - This area of risk captures any event (decision or action) that could be associated with a perception that your organization is out of compliance with an external regulatory requirement.

As you can see the stakeholders associated with these areas of risk are your customers, and maybe even your customers customer, and for those who work in regulated industries; the regulatory bodies themselves.

The other type of risk here that's worth mentioning is the idea of **Business Risk**.

I think it's important to acknowledge that our decisions as Quality professionals can impact the financial results of the organization. This is where the concept of the Cost of Quality comes into play.

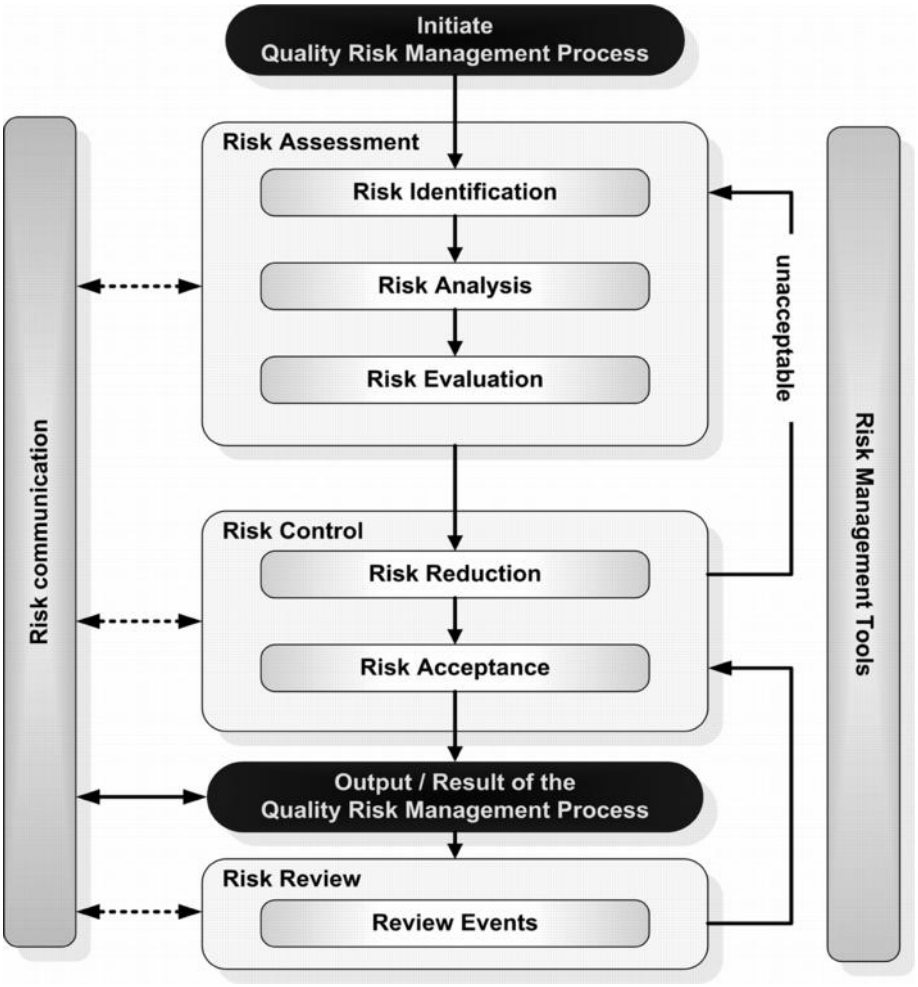
Essentially, **business risk** exists where there is a event that has a negative impact on your business and its financial or competitive performance.

A Review of the Quality Risk Management Process

So now that we understand risk, it's time to talk about **Risk Management**.

Risk Management *is defined as the systematic application of management policies, procedures & practices to the tasks of assessing, controlling, monitoring, communicating & reviewing risk throughout the lifecycle of a product or service.*

These activities are the key - **identifying, assessing, controlling, monitoring, communication and reviewing risk**, and they are they are reflected in the risk management flow diagram below.



Keep these activities (**identifying, assessing, controlling, mitigation, communicating & reviewing risk**) in mind as we discuss the integration of risk management into the Quality System.

What you should begin to see is how many of the various quality processes & systems significantly contribute to these activities within risk management.

So when we're managing risk, we're inherently improving quality; and vice-a-versa.

Integration of Risk Management into the Quality Management System

OK, now we're ready to talk about how Risk Management can been integrated into the various elements of the Quality System.

Before we start, I want to quote ISO 31000:2009 (Risk Management) - "*Risk Management should be embedded in all the organization's practices and processes in a way that it is relevant, effective & efficient.*"

The standard goes on to further say that "*The success of risk management will depend on the effectiveness of the management framework providing the foundation and arrangements that will **embed** it throughout the organization at all levels*".

The reason that we want Risk Management embedded into our quality system is because Risk can be occur or be introduced at any point throughout the lifecycle of your product or service.

Therefore we must ensure that Risk Management is embedded into each element of the Quality System and cover your products entire lifecycle.

Below are the 6 other pillars of the CQE Body of Knowledge that represent the entire product or service lifecycle.

Risk Management and Management & Leadership

Within the Management & Leadership pillar of the CQE Body of Knowledge, there are three key topics that are interrelated with risk management.

These include **supplier management**, **communication** **& top managements responsibilities**, especially in the area of policy development.

Top Management Responsibilities

One of the most important responsibilities of Top Management is the creation of a **Risk Policy**.

Top management is responsible for establishing this policy which defines the acceptable level of risk associated with your products or services.

This risk acceptability criteria will be utilized during the Risk Evaluation phase of the Risk Assessment process to determine if your identified risks & their associated risk levels are acceptable or not.

This determination of risk acceptability should occur before you design a product or perform a risk assessment.

This level of risk acceptability essentially defines your organizations appetite for risk. That is, how much risk you're willing to accept, or how much risk you're willing to subject your customers to before you take action & reduce risk.

Supplier Management

Our suppliers can be a major source of risk that should be managed.

When suppliers provide us with non-conforming parts, those components can result in a product failure or unsafe condition for our end user. This is where our supplier management program can improve quality and reduce risk at the same time.

You can find elements of risk management within the Supplier Management Process already. For example the supplier evaluation & selection process is meant to determine which supplier is the most capable of providing high quality, low risk components.

Then, the idea of supplier monitoring & improvement is all about managing & controlling the risks associated with your suppliers & their supplied components.

A risk based approach to quality can also be found within the supplier scorecard tool.

The entire idea of a supplier scorecard is similar to the risk assessment process meant to determine your highest risk suppliers that require auditing or corrective action.

Communication

The next important topic we need to discuss are the best practices surrounding Risk Management & Communication.

If you look back at the overall risk management process, there are multiple points where communication is recommended or required.

This communication & reporting is beneficial in that it ensures that all of your key internal stakeholders have the appropriate level of aware to the on-going risk management process, etc.

Communication also encourages more accountability & ownership of the risk management process and the resulting level of risk associated with your product.

Good communication also opens up a dialogue between the risk management team and the internal stakeholders that might have relevant input or be able to provide consultation on the overall product or process.

Risk Management & The Quality System

Within the Quality System pillar there are many different topics that are intertwined with the risk management process.

For example, documentation & training are two of the primary tools used within the quality system that contributes to risk management.

As we create documentation (Procedures or Work Instructions) for our processes, we're mitigating the risk that our process will be performed incorrectly, which could potentially result in product that doesn't meet our customers' needs.

This is where training comes into play.

Once we've documented how our processes should be executed, it's important to training our employees on the procedure to ensure that they are knowledgeable & capable of fulfilling all of the requirements within the procedure.

You could also utilize a risk-based approach to determine the proper level of initial & on-going training required for your employees.

This same thought process could be applied to the identification of required experience, qualification, education & training level for particular roles within the organization.

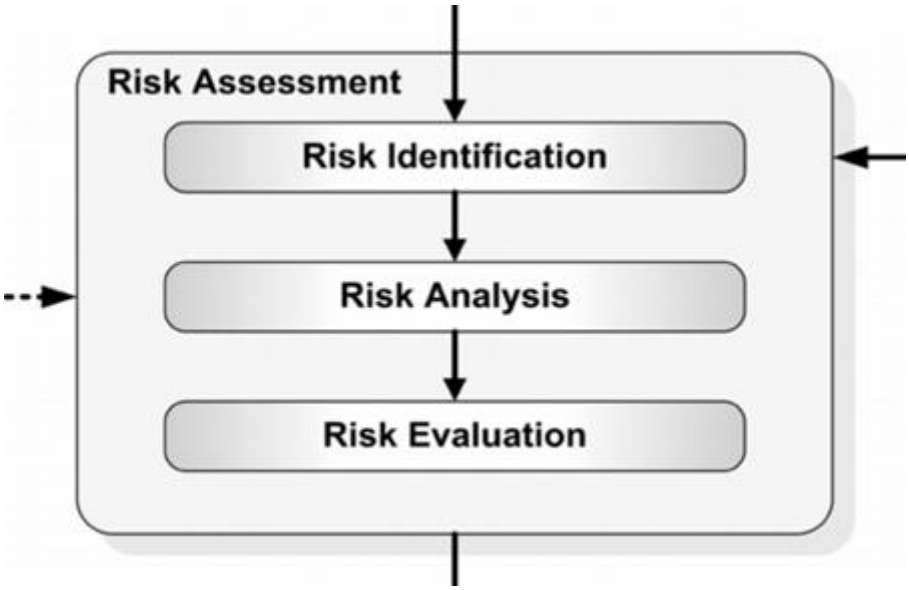
For example, it would be extremely important to train your employees on how to apply the risk management techniques that we're able to discuss so that they're capable of using them properly.

Without the proper training, critical elements of the risk management process might be overlooked, resulting in the incorrect assessment of risk and the potential exposure of your customers to an unacceptable level of risk.

The Design Process & Risk Management

Risk Management is HUGE in the Product & Process Design stage of your products lifecycle.

One of the most important steps in the design process is to perform a Risk Assessment for your new product or service to identify hazards and feedback the analysis into your design process to achieve "Quality or Safety by Design".



Your design efforts could also include a Design FMEA to identify & mitigate any high risk failure modes associated with your product.

Your design efforts should also include the identification of CTQ's (Critical to Quality), or CQA's (Critical Quality Attributes). These are features about your product that, if they were to fail, would result in a serious impact to the end user.

As such these attributes have an element of risk to them and should then be monitored & controlled as part of your risk mitigation strategy.

Your technical drawings are similar to process documentation discussed earlier. By accurately defining your design using technical drawings you're creating a tool that can be used to ensure product quality throughout the lifecycle of your product.

This will ultimately reduce the probability of a failure of your product and helps mitigate the risk associated with those failures.

Also during the design process is when you would first perform a Process FMEA.

This Process FMEA would help you assess the risk associated with your process and identify any areas of unacceptable risk that requires mitigation.

Your Design V&V process is also meant to be one last checkpoint to ensure that your product functions per your specifications; meets your customers needs and does not result in an unacceptable level of risk to your customer.

Process Validation is very similar here too. By validating your process you're confirming with objective evidence that your process performs as intended and results in product that meets your specifications.

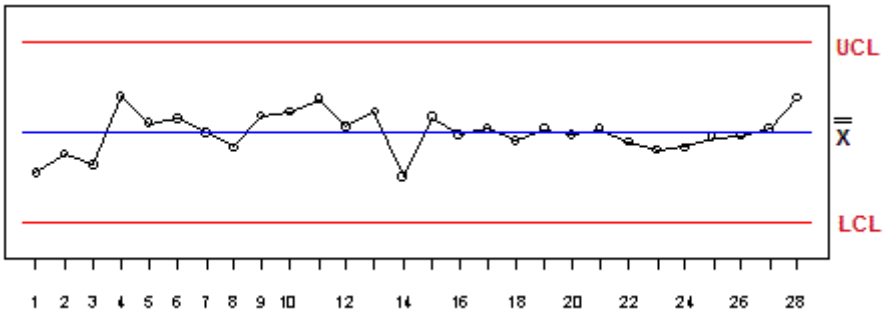
The success of your Design V&V & Process Validation work should cumulate in the creation of a process control plan that defines all of the necessary testing, inspection & sampling steps to ensure that your process is in a state of statistical process control and is capable of producing conforming parts.

Product & Process Control & Risk Management

Once you've designed a product that is low risk, you now must go through the process of ensuring that same level of low risk throughout the lifecycle of the product.

This is achieved through Product & Process Control.

By controlling & monitoring your various manufacturing processes and ensuring that they're operating within a validated state, you're ensuring that your producing parts that meet your customers needs and requirements.



This includes all of the topics within this pillar which include your control plan, your control non-conforming material, your testing & sampling plans, and your measurement & calibration (metrology) program.

For example, we calibrate equipment to ensure it is accurate and capable of discerning good products from bad, thus reducing or eliminating the risk of accepting bad product. This is also true when we're determining the capability of our measurement system.

Similarly, we control non-conforming material to prevent it from being distributed to our customers to mitigate any risk there.

Risk Management & Continuous Improvement

The biggest relationship between risk management & continuous improvement can be found in CAPA.

When a non-conformance occurs, you've essentially identified a potential risk. If it's a new & never before seen non-conformance, you can perform a risk assessment to determine if the risk associated with that event is acceptable or not.

Regardless of your risk assessment, your corrective action & the CAPA process is one of the biggest tools for Risk Reduction within the Quality toolbox.

Another strong relationship exists between the risk management tools like the FTA & PFMEA and a handful of the Quality Control Tools.

For example, the Flow Diagram, Cause & Effect Diagram and Check Sheet are common tools that facilitate the risk assessment process.

Control Charts are another Continuous Improvement tool that is meant to monitor your process to mitigate the risk of non-conforming product being produced and ultimately distributed to your customer.

The last comment I'll make is about the continuous improvement tools like lean & six sigma.

Most of the time these projects are meant to improve your process and reduce risk; especially in the world of six sigma where the goal is to reduce your process variation and thus improve process capability and eliminate defects.

However, some improvement projects and other various changes to your process can introduce new sources of risk.

So I would strongly caution that you perform a risk assessment when planning your changes to ensure that you're not introducing any new sources or opportunities for risk.

Risk Management the Quantitative Methods & Tools

Alright - on to the last pillar of the CQE Body of Knowledge - Quantitative Tools & Methods, otherwise known as Statistics.

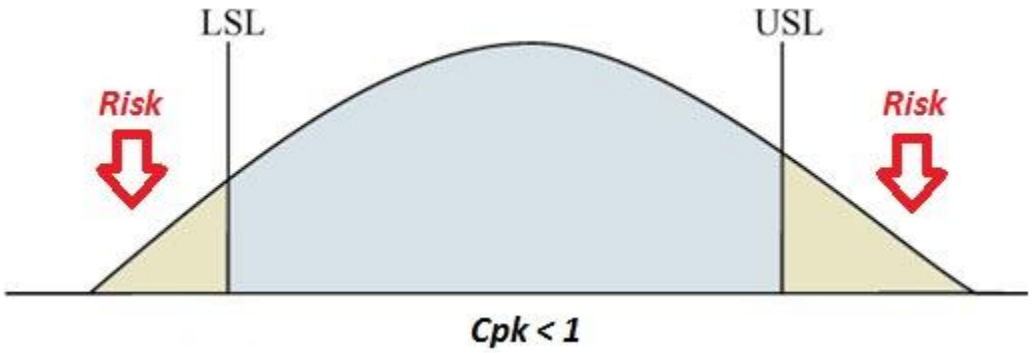
Within this pillar there are two key tools that are related to Risk Management; that is Process Capability & Statistical Process Control.

We've already touched on the concept of a Control Chart and its relationship with the Risk Management process.

So we will focus here on the idea of **process capability** and its relationship with risk; specifically, the "likelihood" element of risk.

When process capability is poor, the likelihood for non-conforming material increases, thus risk increases.

As you can see below, if the tails of your distribution drift past the specification limit, that portion of your population is non-conforming and thus has an element of risk to it.



If that product is 100% inspected and scrapped during your manufacturing process, then you've introduced business risk. The financial performance of your company has decreased due to your poor process capability.

If that product is not 100% inspected and it is distributed to your customer, then you've potentially introduced User Risk or Product/Reliability Risk.

Lastly, when a non-conformance reaches your customer, it introduces business risk in the form of lost goodwill or brand reputation.

Conclusion

Alright - time for a quick recap!

So the purpose of this chapter was meant to introduce the concept of risk, and discuss the different types of Quality Risks.

Additionally, we wanted to discuss the process & framework for the entire risk management pillar, and how risk management should be integrated into the Quality System(QS).

To do this, we introduced the concept of Risk as the combination of the probability of occurrence of a negative event, and the severity of that negative event.

We then moved on to discuss the different types of Quality Risk; those being User Safety Risk, Product/Reliability Risk & Compliance/Regulatory Risk.

We then moved on to the concept of **risk management** which is defined as the *systematic application of management policies, procedures & practices to the tasks of assessing, controlling, monitoring, communicating & reviewing risk throughout the lifecycle of a product or service.*

From there we discussed the relationship between Risk Management & Quality Management; and how risk management can be integrated into each of the various topics within the CQE Body of Knowledge.

This is where we went in-depth and discussed how risk management is related to or integrated into each of the various topics within the CQE Body of Knowledge.

The Risk Assessment Process

Risk can only be effectively managed when it is identified, analyzed & considered for mitigation.

The collective process of **identifying**, **analyzing** and **evaluating** risk is known as a **Risk Assessment** & *this process can be summarized into three questions:*

1. What might go wrong?

This is the **Risk Identification** question; what are those or sources of failure or failure modes that could reasonably occur.

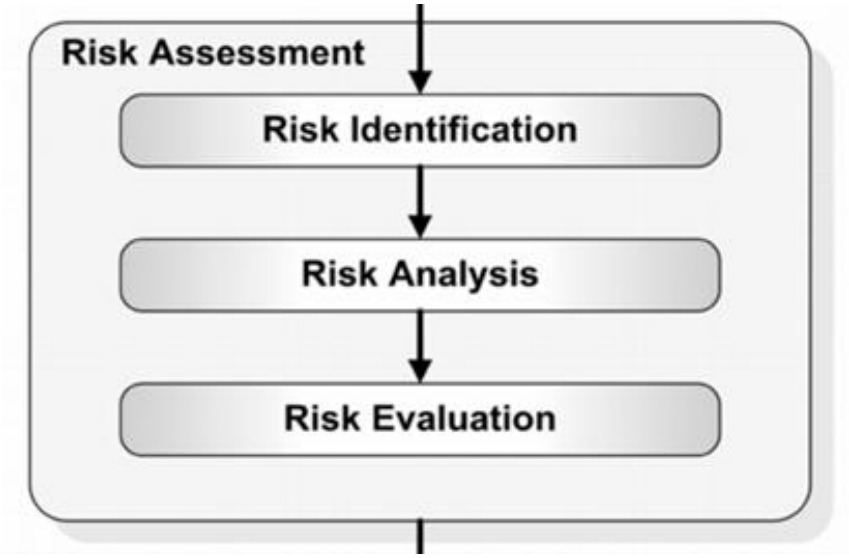
2. What is the likelihood that individual something might go wrong, and what are the consequences when that something does occur?

This is the **Risk Analysis** question and it seeks to quantify or analyze the risk for each identified failure mode.

As we will discuss, Risk is considered the combination of both the likelihood of occurrence of a failure & the severity of that failure.

3. Finally, Is that risk ok?

This is the **Risk Evaluation** question. Once you've estimated the risk associated with each potential source of risk, you can then determine if any mitigations are needed to reduce that risk.



These three Risk Assessment process steps - **Risk Identification**, **Risk Analysis** & **Risk Evaluation** are the focus of this chapter and will be discussed in detail.

We will wrap up this chapter with a quick discussion about **risk communication**, **risk facilitation tools** & the **level of effort** associated with the risk assessment process.

Risk Identification

Step one in the Risk Assessment process is to identify *actual & potential* risks.

This answers the question - *what might go wrong?*

This identification of risks cannot be done haphazardly; and often requires a tool like the FMEA or FTA to assist in the analysis of your complex supply chain (various suppliers), manufacturing process, and distribution channels.

Your risk identification process should be comprehensive and include failure modes that are **outside of your control** (suppliers, etc) and should also include consideration for potential failure modes that have not yet occurred.

The identification of risk should be a continuous process that starts early in the development of your product, and continues through into your process control phase.

As such, I wanted to walk through those 2 distinct lifecycle phases (Design & Production) to discuss the various activities where risks can be identified.

Identification of Risk During the Design & Development Phase

As I mentioned earlier, the identification of risk should start early in the design & development process.

In fact, one of the primary jobs of a designer is to ensure that the design is robust and free of as many risks as possible.

This is there a tool like the **DFMEA** can be extremely powerful. The DFMEA tool is a systematic method for evaluating your design to understand the various risks that exist.

The DFMEA is also a method to compare design alternatives against each other. This allows the designer to make better informed decisions about which design alternatives have the lowest risk.

There are also a number of other tools & techniques used within the design process where risks can be identified including; Simulation testing, Prototype Manufacturing & Testing, Designed Experiments (DOE), Process Characterization, Reliability Testing, Design Verification & Validation and/or Process Validation.

At any point during these various design activities, the design team may identify a risk associated with the current design and feed that information back into the DFMEA.

These process can be used to not only identify risk but can also support the analysis of risk, which is discussed below.

These risks should be used to setup your quality control plan to ensure they are adequately mitigated and or monitored during the production phase.

Identification of Risk During the Production Control Phase

The identification of risk also occurs after a product is designed and in production.

These risks are routinely identified through the various quality control techniques including your supplier management, sampling plans, control charts, measurement & testing, control plans & the CAPA process.

These various quality control techniques are in place to identify risks within the starting material (raw material), the production process, production equipment, human error, production facilities, the labeling & shipping process, product distribution & the final use of the product.

Similar to the DFMEA, the PFMEA offers a nice tools to systematically analyze your production process in order to identify these types of risks.

The Risk Analysis Process

Alright - now that we've identified all of the risks associated with our product & process, it's now time to analyze those risks.

Before we jump into the mechanics of a risk analysis, let's step back and review the definition of risk, so that we can properly analyze all of the risks we just identified.

Risk is defined as the likelihood that an event will occur, combined with the severity of that failure when it occurs.

$$\boldsymbol{Risk = Severity * Occurrence}$$

So if you've got a failure mode that occurs often (25% of the time) and results in an injury to your customer then you've got a serious risk on your hands.

On the other hand if you've got a failure mode that happens once in every 1 million units you produce that the customer barely notices then there's a lot less risk there.

The first of these two examples has much higher severity (Injury v. barely noticeable) and a higher occurrence rate (25% v. 1 part per million).

Make sense?

Ok, so now we're going to go in depth for each of those elements of risk (Severity & Likelihood of Occurrence), so that we can properly analyze our risks.

Let's start with the Severity half.

Severity of the Identified Risk

Severity is as *a measure of the consequence of the failure mode*, or the degree to which your customer is impacted by a failure mode & its effect.

For example, some automobile failure modes can lead to serious injury while others are simply an inconvenience for the customer.

These failure modes are much different because one impacts the customer significantly and the other does not.

Severity can also be assessed from other perspectives beyond customer safety or customer satisfaction.

For example, for those who work in regulated industries there are failure modes that don't impact the end user but might introduce some element of regulatory risk, then that would also have an impact on the severity of a failure mode.

Another example would be a failure mode that has an impact on your internal operations.

For example, if a failure mode creates a safety risk for your internal employees, or has the potential to damage your production equipment, than the failure mode could be considered high on the severity scale.

Severity Scales

To adequately assess the severity of your various failure modes, you need a scale, and there are various types of scales you can use.

The first type of scale can be described as a qualitative scale.

So you could assess the severity using terms like "inconsequential", "very minor", "minor", "marginal", "major", "critical" or "catastrophic" to describe the severity of the failure mode & its effect on the customer.

You can convert t hose terms into a semi-quantitative scale using a 1-6 rating with the lowest value (1) being the least severe and the highest value (6 in this case) being the most severe.

The 6-scale is not universal however, and you can basically use whatever scale you want.

Below is an example table showing both a semi-quantitative 1 - 6 scale (ranking) with its qualitative terms (Category) for Severity from Wikipedia:

Quantitative Score	Qualitative Score	Definition
1	None	No relevant effect on reliability or safety
2	Very Minor	No damage, no injuries, only results in a maintenance action (only noticed by discriminating customers)
3	Minor	Low damage, light injuries (affects very little of the system, noticed by average customer)
4	Moderate	Moderate damage, injuries possible (most customers are annoyed, mostly financial damage)
5	Critical	Causes a loss of primary function; Loss of all safety Margins, 1 failure away from a catastrophe, severe damage, severe injuries, max 1 possible death
6	Catastrophic	Product becomes inoperative; the failure may result in complete unsafe operation and possible multiple deaths

Likelihood of Occurrence of the Identified Risk

The next step in the process is to assess the likelihood for occurrence for each potential failure mode.

The Occurrence ranking is generally defined as the ***likelihood*** or ***probability*** or the ***frequency*** that a failure is expected to occur at.

Sometimes you'll have solid data to very accurately estimate the frequency of occurrence of a failure mode. This may come from Reliability testing or failure rate data like DPMO (Defects Per Million Opportunities) data, etc.

This likelihood for occurrence can also be estimated indirectly from your process capability studies captured during the development process or on-going production.

In other situations where you're assessing a new or potential failure mode, you may have to use your best judgment to estimate the likelihood for failure.

Occurrence Scales

Similar to Severity, the Occurrence can be assessed in qualitative terms, semi-quantitative terms, or quantitative terms.

In qualitative terms, this can mean assessing the likelihood using words like "Never", "Extremely Unlikely", "Remote", "Occasional", "Sometimes", "Often", "Frequent", etc.

From a semi-quantitative perspective, this can be a simple 1 - 6 scale, with one being the least frequently occurring failure mode and 6 being the most frequently occurring failure mode.

From a quantitative perspective, you can link your 1-6 scale directly to your known Process Capability or measured DPMO for your process or failure mode.

Ranking	Qualitative Term	Semi-Quantitative	Quantitative
1	Extremely Unlikely	1	Less than 1 in 1,000,000
2	Remote	2	Between 1 in 1,000,000 & 1 in 100,000
3	Unlikely	3	Between 1 in 100,000 & 1 in 10,000
4	Occasional	4	Between 1 in 10,000 & 1 in 1,000
5	Frequent	5	Between 1 in 1,000 & 1 in 100
6	Often	6	Greater than 1 in 100

Risk Evaluation

Alright, time to bring everything together for the final step, the risk evaluation.

The Risk Evaluation step is where you compares the risk that you just analyzed against a predetermined risk criteria for your product.

This is a good time to have a quick reminder about the **Risk Policy**.

The Risk Policy defines the acceptable level of risk associated with your products or services and is established by Top management prior to the Risk Assessment process.

This risk acceptability criteria is used during the Risk Evaluation process to determine if your identified Failure Modes & their associated risk levels are acceptable or not.

This level of acceptable risk defines your organizations appetite for risk.

That is, how much risk you're willing to accept, or how much risk you're willing to subject your customers to before you take action & reduce risk.

Below is an example of a 6 x 6 risk matrix that could be used to analyze your various failure modes and their associated risk levels.

You could, as an example, say that your threshold for an unacceptable level of risk is the score 13. So all risk scores that are 12 or less are acceptable and any that are 13 or great are unacceptable.

		Occurrence					
		1	**2**	**3**	**4**	**5**	**6**
Severity	**1**	1	2	3	4	5	6
	2	2	4	6	8	10	12
	3	3	6	9	12	15	18
	4	4	8	12	16	20	24
	5	5	10	15	20	25	30
	6	6	12	18	24	30	36

Risk Communication during the Risk Assessment Process

Alright - on to the last topic within the risk assessment process, which is **risk communication**.

Like in every other process in the world, communication is key.

First we should discuss the **stakeholders** that should be considered when it comes to communication.

From a risk management perspective, a stakeholder is *any person or group that can affect, be affected by, or perceive themselves to be affected by a decision, activity or risk.*

This definition should not be limited to stakeholders within your organization (internal stakeholders) and should include stakeholders outside of your organization (external stakeholders).

These external stakeholders include suppliers and customers as they can affect or be affected by the risks associated with your product.

Communication with these stakeholders can and should occur at each of the various stages within the risk assessment process, depending on the complexity of the analysis.

During the *risk identification* stage it is important to communicate to each stakeholder to ensure that all risks are identified and considered.

During the *risk analysis* stage communication should be used to ensure that the appropriate severity & likelihood are assigned to each identified risk.

During the *risk evaluation* stage communication should be used to ensure all stakeholders are aware of the final risk associated with each identified risk. This is especially true if any risk is identified to be at an unacceptable level.

Facilitation Tools & Risk MGMT Tool

Now that we've covered the three primary steps within the risk assessment process, I wanted to quickly talk about a handful of quality tools that can be used to facilitate this process.

These tools include the **Flow Diagram**, the **Check Sheet** & the **Cause & Effect Analysis**.

These tools are used during different phases of the risk assessment process.

The Flow Chart is primarily used during the Risk Identification process and it provides you with an overview of your process as a starting point for your analysis and ensures that you don't overlook any step within the entire process.

Similarly, the cause & effect tool will aid you in identifying risks by considering the various ways in which a process can fail.'

Think back to the 8M process - **Man, Machine, Method, Materials, Mother Nature, Measurement, Management & Maintenance**. Using this tool will aid in a thorough assessment of your various process steps and their potential failure modes.

The Check Sheet is a data collection tool that can assist you in the risk analysis phase to determine the frequency of occurrence of a given failure mode.

Risk & Effort / Formality.

The last comment I want to make here about the risk assessment process is about effort, formality & documentation.

Most industry specific risk management standards (ISO 31000, ISO 14971, ICH Q9) all make a similar comment on this topic and it's worth discussing here. These standards all say something like:

"The level of effort, formality, and documentation of the risk management process should be commensurate with the level of risk" - **ICH Q9**.

This is a key point to repeat.

Your level of effort, formality & documentation should be commensurate with the level of risk.

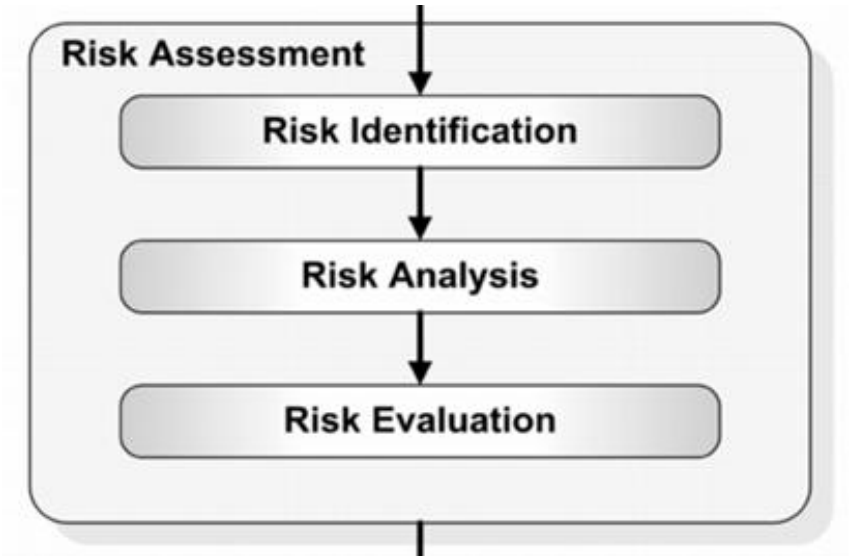
This comment applies to things like facilitation tools & risk management tools (FMEA, FTA). If you've got a complex process that an appreciable level of risk to it, you should be using those tools as part of your due diligence effort.

Conclusion

Alright, we're done!

Let's review the Risk Assessment process.

As we learned, the risk assessment process is made up of three distinct activities -- Risk Identification, Risk Analysis & Risk Evaluation.



Risk Identification is answering the question - "*What might go wrong?*"

This process should include all steps within your process and result in the identification of all known or potential failure modes that could reasonably occur.

Risk Analysis answers the question - "*What is the likelihood a failure will occur and what are the consequences of that failure?*"

Risk is the combination of Severity (Consequence) and the likelihood of Occurrence; both of which are independently assessed in the Risk Analysis process for each identified failure mode.

Risk Evaluation answers the question - "*Is that risk ok?*"

Once you've analyzed the risk associated with each potential source of risk you then must determine if that risk is acceptable or unacceptable per your risk policy.

We wrapped up this chapter with a quick discussion about **communication**, **facilitation tools** & the **level of effort** associated with the risk assessment process.

As you move through the three steps of the risk assessment process you should be aware of the various **stakeholders** involved and communicate with them appropriately.

Also, the risk assessment process if facilitated by three other quality tools; the **flow diagram**, the **check sheet** & the **cause & effect analysis**, which assist in ensuring thoroughness at each step in the process.

Lastly is the effort piece where we learned that the **level of effort, formality, and documentation** of the risk management process should be commensurate with the level of risk.

Risk Control & Risk Review

Here we are on the last chapter of the Risk Management which is dedicated to the Topics of **Risk Control** & **Risk Review**.

This chapter is broken down into two sections - **Risk Control** & **Risk Review**.

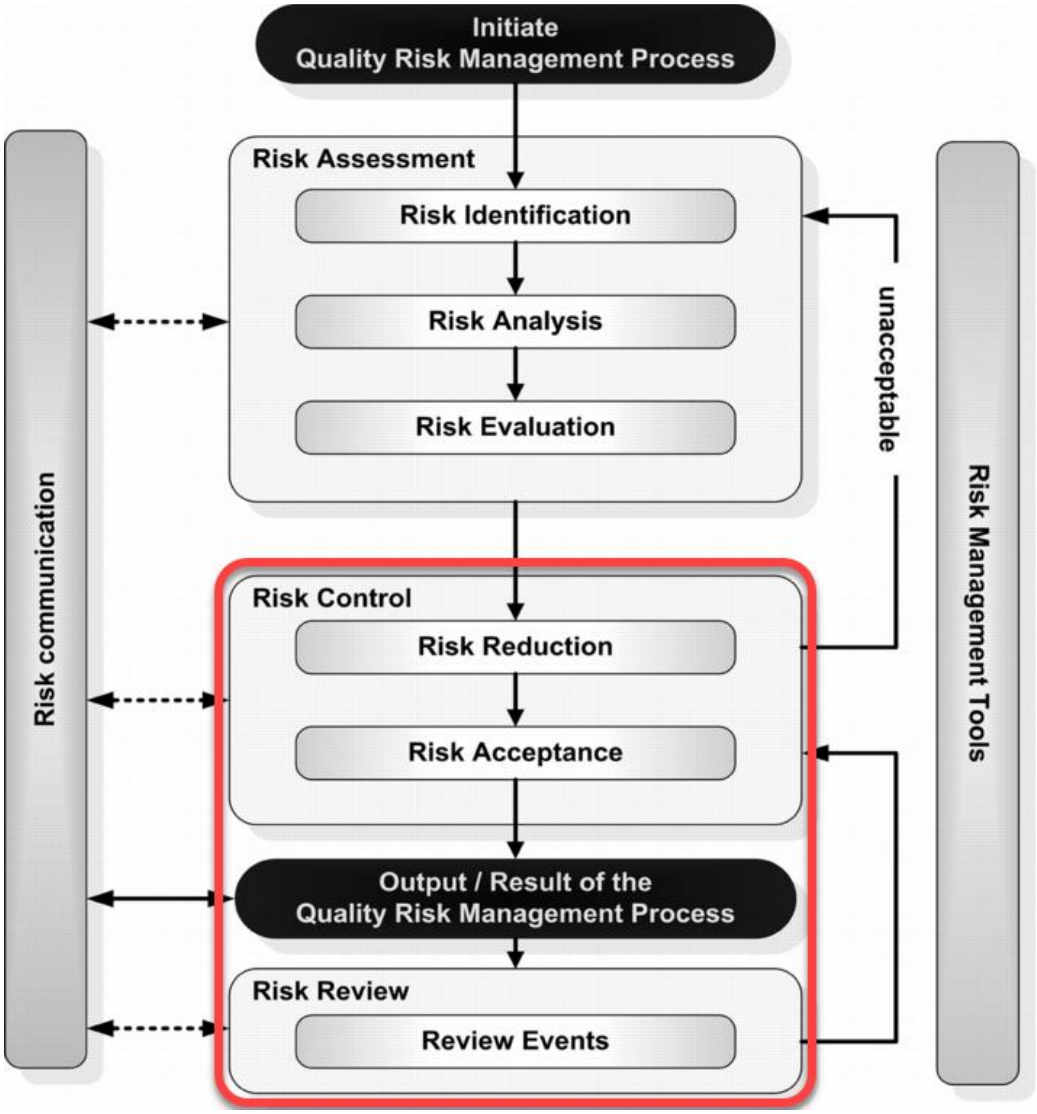
The first is **Risk Control** where we cover the concept **of risk reduction** and **risk mitigation** where you'll learn the **4 step process** to an effective risk reduction effort.

Within this section we also discussed many of the common **Quality System Processes** & how they can also contribute to your Risk Control strategy - including topics like Product Design, Process Design, Process Validation, Process Control, Supplier Management & the Control of Measurement Equipment.

This first section will close out with a discussion of **Risk Acceptance** & **Residual Risk**.

The second major section of this chapter is the concept of **Risk Review** process & and on-going monitoring of the risk management process including **Risk Events**.

Below you can see how Risk Control & Risk Review fit into the overall Risk Management Process.



Risk Control

Risk control is defined as the *process in which decisions are made and protective measures are implemented to reduce or maintain risks with, specified levels.*

This definition has two main activities associated with it, reducing risk & maintaining risk.

Reducing risk naturally follows the risk assessment process and it meant to mitigate or reduce any unacceptable risks identified during the risk analysis.

Maintaining risk is all about your on-going Quality System Activities & their contribution to Risk Control.

Risk Reduction

First let's talk about Risk Reduction.

Risk Reduction focuses on processes for the reduction of risk when it exceeds a specified (acceptable) level.

As you recall from the previous chapter your risk assessment will result in a comprehensive assessment of your product or process and all potential failure modes & their associated Risk (Severity & Likelihood of Occurrence).

You should also know, based on your Risk Evaluation, which of those risk are acceptable or unacceptable.

If any risks have been found to be unacceptable; then risk reduction is required.

It should also be noted that risk reduction is often also desired even if the risk is acceptable. This process is required when risk is found to be unacceptable, however it can also be used as part of your ongoing continuous improvement process.

Using a Risk Ranking matrix along with your risk assessment will aid you in prioritizing the risks that require some sort of reduction or mitigation.

4 Steps of Risk Reduction

There are 4 steps to the risk reduction process, and these are shown below.

1. Planning & Analysis of Risk Control Options
2. Implementation of Risk Control Measures
3. Residual Risk Evaluations
4. Risk Analysis of Risk Control Measures

Step 1 - The whole process starts out like many other processes - with a planning phase.

This step answers the question - What risk reduction options are available?

As you're planning your risk reduction, keep in mind that there are various ways to reduce risk.

The holy grail of risk reduction is inherent safety by design.

If you're able to "design out" the failure mode that you've identified in your risk assessment, that's the best option.

However this is not always feasible, and often times you'll have to attack one or both sides of the risk equation.

$$Risk = Severity * Occurrence$$

By this I mean that risk can be lowered by reducing the likelihood of occurrence of a failure mode or reducing the impact to the customer (severity).

In general, the impact to the customer (Severity) is usually harder to change than the likelihood for occurrence of the failure mode.

Air bags are a good example of a design feature that's meant to reduce the severity side of the risk equation.

Air bags don't reduce the likelihood of a car crash, but they can reduce the injury to the driver/passengers when an accident does occur.

The other option is to reduce the likelihood of occurrence of a failure mode.

This can include activities like improving your process capability for a given step in your process to reduce the frequency of a given failure.

Or improving the detection of failure modes by adding additional inspection/testing, etc.

Step 2 in the Risk Reduction process is to implement the risk reduction measure that you've identified.

The implementation of a risk control measure should be captured within your CAPA system and also be made a part of you Quality Management System in terms of documentation, etc.

This will support the long term effectiveness of your risk control measure.

Step 3 in the Risk Reduction process is to demonstrate the effectiveness of the risk reduction measure.

You'll want to confirm that the risk reduction measure that you've recently implemented is effective at actually reducing risk.

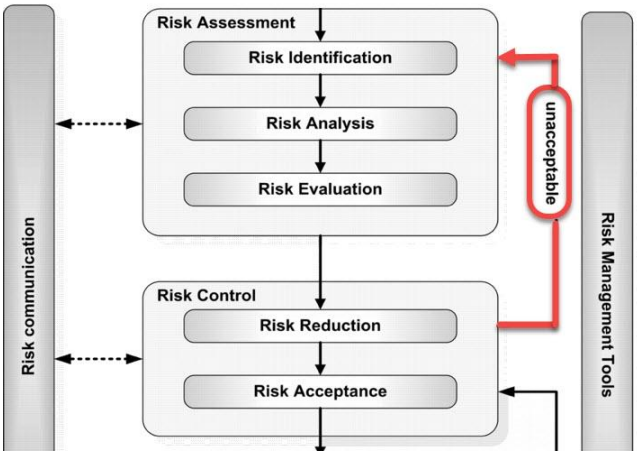
This is essentially a repeat of the Risk Analysis & Risk Evaluation steps of the Risk Assessment process, for the risk you're attempting to mitigate.

The results of this analysis will give you your **residual risk**.

By that I mean that your risk reduction measure will likely be unable to fully eliminate the identified risk, so there will naturally be some residual risk (risk left over).

If the residual risk has been found to be lowered and acceptable then your risk reduction activities are a success.

If the residual risk is still found to be unacceptable, additional risk reduction actions may be required; this can be seen in the overall flow diagram below.



The last step in the Risk Reduction process is to ensure that there are no new risks that have arisen from your risk reduction activities.

Sometimes, risk reduction efforts (changes to the process/product) can introduce new risks.

Therefore, it's always recommended to perform a quick risk assessment to ensure there have been no unintended consequences associated with your risk mitigation/reduction changes.

Oftentimes, one new risk that arises from a risk reduction action is the failure of that risk control step.

So if you implement a new inspection, if that inspection were to fail, then your risk reduction would essentially be lost. So you need to evaluate the likelihood that your new inspection process will failure and understand the risk there.

Risk Mitigation

The second half of risk control is a what I'm calling risk mitigation.

What we're going to cover in this section is the collection of activities throughout the Quality System (QS) that also plays a big role in controlling risk.

The important thing to know here is that **Risk Control is a lifecycle activity** in that it starts early in development and continues through manufacturing and any on-going servicing or maintenance of your product through to retirement.

So I'm going to spend a few seconds talking about many of the different areas of the Quality System & it's relationship to risk management.

Risk Mitigation & the Design & Development Process

As we've discussed before, the holy grail of risk control happens when your product is inherently "safe" by design.

Safe meaning free of unnecessary risk.

One of the major goals of the quality engineer during the design process is to ensure that the Risk Management process is followed and that the final design has the lowest risk possible.

This is also where concepts like Robust Design, Quality by Design & Design for Six Sigma come into play. One of the major goals of these different design philosophies is to **eliminate defects or failure modes.**

This is akin to *reducing the frequency of occurrence of a failure mode,* that ultimately reduces the risk associated with the product.

Risk Mitigation during the design process is analogous to the Cost of Quality concept that Preventing a problem is always cheaper and easier than correcting that problem later on down the road.

Risk Mitigation & Supplier Management

Think back to the Supplier Management process, with its 4 key steps - Supplier Evaluation, Supplier Qualification, Supplier Selection, Supplier Monitoring, etc.

These steps play a big role in managing risk.

First off, similar to the design of your product, the evaluation, qualification & selection of your suppliers ensures that you're working with the best suppliers who are capable of consistently delivering products that meet the specification.

Then you've got your on-going supplier monitoring, which is a combination of Supplier Audits, Supplier Surveys & whatever raw material inspection you perform on a routine basis.

All of these activities are meant to detect when your starting materials are non-conforming, which might impact your final product & introduce unwanted or unacceptable risk.

This is why we manage & monitor both our suppliers & their quality systems, as well as the starting material that they provide.

Risk Control & Measurement Equipment

Similar to your suppliers, the selection & qualification of your measurement equipment plays a big role in Risk Control.

If you have equipment that is not suitable for its intended use then it introduces the risk of **measurement error (False Acceptance)** that could result in the acceptance of non-conforming product resulting in risk.

Now is a good time to mention topics like **Calibration** (Metrology) and **Preventative Maintenance** of measurement equipment, both of which are forms of risk control because they prevent failures from occurring.

These activities ensure that your equipment is operating in a validated state; and we're preventing the false acceptable of bad product.

Risk Control & Validation + Process Control

If you recall back to the chapter on **Process Validation** it is the combination of 3 stages, **Process Design, Process Validation & Process Monitoring**.

Each of these three phases is geared towards the creation of a process that is stable & capable in producing products that meet your specifications.

This is how you design a process that is low risk (low frequency of occurrence).

Then, once your production process has been validated, you should be monitoring that process continuously to ensure that your process is operating in a validated state. this is a huge part of your on-going risk control strategy.

As you collect data on your production process you can feed this data back into your risk assessment to ensure that your initial assessment is accurate, etc.

This where your **Control Plan** should include a list of your product quality attributes and their relationship to you process and how you plan on controlling for each quality attribute.

Because the failure to achieve your quality attributes will result in an element of risk. So your control plan is directly related to risk reduction.

Risk Acceptance

Alright, on to the next important topic within Risk Management which is Risk Acceptance.

What you absolutely must understand is that even the most brilliantly designed & manufactured products have some element of risk to them. This risk is known as residual Risk.

Residual Risk

Residual risk is the risk that remains after all risk control & risk reductions measures have been taken to reduce risk.

Residual risk can include both known and unknown risks; where unknown risks are those not yet identified.

For example, driving a normal car everyday has a small level of residual risk that simply cannot be eliminated.

As discussed above, once you implement a risk mitigation step, you should analyze the residual risk that remains to determine if it is acceptable or not.

So if you've got a failure mode that was originally occurring at a 1% rate, and then your risk mitigation implementation it is now occurring at a 0.1% rate, you should confirm via a risk assessment that the residual risk (1 in 1,000 or 0.1%) is acceptable.

Risk acceptance is the decision to accept that residual risk. This decision can be either a formal documented decision or a passive decision.

We discussed residual risk above in the risk reduction section, because once you've implemented a risk reduction action, you must also analyze & evaluation the residual risk.

If the residual risk is acceptable then the risk reduction effort was effective; if it is not acceptable, then perhaps the risk mitigation was not effective or additional mitigations are needed.

And with this, you're done with the Risk Control Process; however you're definitely not done managing risk.

Risk Review

Risk Review is the on-going review or monitoring of output/results of the risk management process considering (if appropriate) new knowledge and experience about the risk.

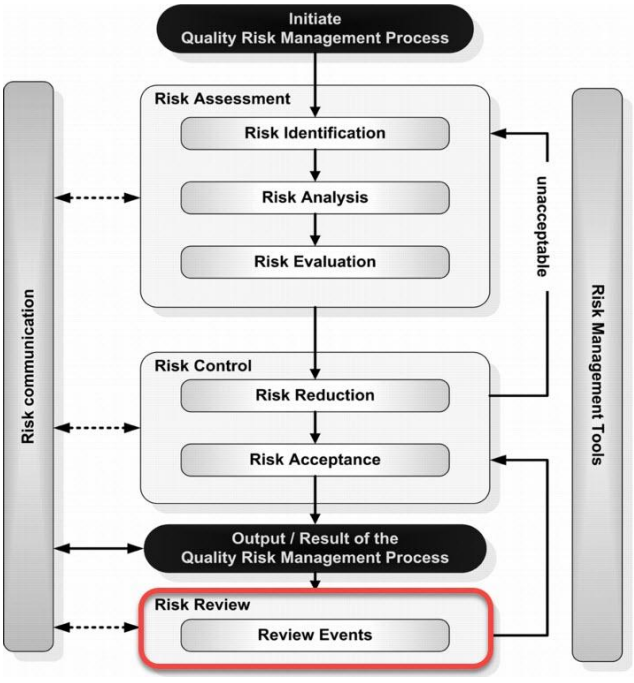
So at the end of your Risk Control activities, you should have moved through the Risk Reduction process, where you've planned & implemented your risk control measures.

Then you've assessed the residual risk that exists after the implementation of your risk control activity & also analyzed any new potential risk that came along with your new risk control measure.

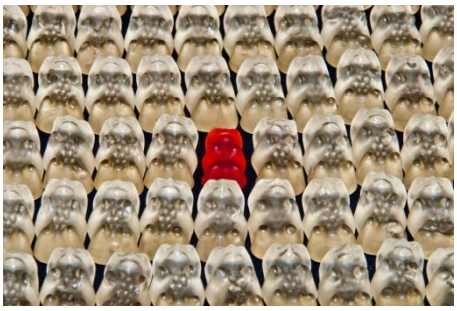
All of this information should go into your Risk Output - The Result of the Quality Risk Management Process.

If you're using an FMEA, it can be the final FMEA Report. If you're using some other type of Risk Management Report, it could go there as well.

Now you've got to go into Monitoring & Review Mode to ensure that all risk controls are effective & efficient.



Risk Events



The highlight of the Risk Review process is the idea of **Risk Events**.

These Risk Events might take the form of a *customer complaint* or a new *non-conformance* (failure mode) or a change in the occurrence rate of a previously identified failure mode.

Beyond the discrete events like non-conformances & customer complaints, the Risk Review period should also include the collection & analysis of other various data points to improve your initial risk assessment.

All of this new information would be fed back into your Risk Output Document, which should be periodically reviewed & updated as necessary for these Risk Events.

This periodic review should confirm your initial assessment and any assumptions made regarding failure rates, etc. This review should also account for any new information obtained since the initial assessment.

I can't stress this enough - the Risk Management process is dynamic & iterative.

Your initial risk assessment will require updates as you receive new information - and you will receive new information.

The Risk management process is NOT a one-time activity, and your Output Document should be treated as a living document.

This is where your CAPA system can be intertwined.

When non-conformances occur, the CAPA system provides a structured opportunity for you to review your risk management output document to ensure that it is still current & accurate.

There are also other key inputs to the risk review process including internal audits or any change management programs that you're currently using.

Risk Events should also include the assessment of any changes to your process, design, equipment, facilities, suppliers, etc.

When changes are made it can introduce new risks or change the risk of existing failure modes.

As you make changes to your product or process you must ensure that the change doesn't have an impact on the risk associated with your product.

Risk Control Conclusion

Alright - time to wrap this whole thing up with a quick review of the Risk Control Chapter.

This chapter was broken down into two sections - **Risk Control** & **Risk Review**.

The first section covered **Risk Control** which included ideas like **risk reduction** and **risk mitigation** and included the **4 step process** to an effective risk reduction effort.

Risk control is formally defined as the *process in which decisions are made and protective measures are implemented to reduce or maintain risks with, specified levels.*

These protective measures are implemented following a simple 4 step process:

1. Planning & Analysis of Risk Control Options
2. Implementation of Risk Control Measures
3. Evaluating the Residual Risk
4. Analysis of new Risks associated with Risk Control Measures

Within this section we also discussed many of the common Quality System Processes & how they can also contribute to your Risk Control strategy - topics like Product Design, Process Design, Process Validation, Process Control, Supplier Management & the Control of Measurement Equipment.

We closed out this section with a discussion of **Risk Acceptance** & **Residual Risk**.

Residual risk is the risk that remains after all risk control & risk reductions measures have been taken to reduce risk.

Risk acceptance is the decision to accept that residual risk.

The second major section of this chapter is the concept of **Risk Review** process & and on-going monitoring of the risk management process including **Risk Events**.

Risk Review is defined as the on-going review or monitoring of output/results of the risk management process considering (if appropriate) new knowledge and experience about the risk.

One key concept in the Risk Review process is the idea of **Review Events** which include non-conformances, customer complaints, key process changes, new data or trends in existing data.

All of this new information is fed back into your Risk Output Document, which is periodically reviewed & updated as necessary for these Risk Events.

Essentially this last step in the process is meant to remind us that the Risk Control process is iterative & dynamic and that we have a responsibility to continuously consider risk.