Strategies, Tools for Success and Other Insights

THE RISK MANAGEMENT GUIDEBOOK

EtQ

Table of Contents

4 Risk Management Techniques for Reducing Defective Products

Recalls over product defects are a major concern in many industries, often creating millions of dollars in costs and brand damage. Part of the problem is that so many companies don't effectively integrate risk management into their processes, allowing small issues to persist unmanaged.

With that in mind, here's a list of 4 risk management techniques that can help reduce product defects.

1. Managing Risk at the Design Phase

Rather than just responding to problems as you discover them, risk management can help you reduce them from the outset, particularly in the design phase.

There are several ways to do this:

- **Tools like Failure Mode and Effects Analysis (FMEA)** identify potential failures before you invest in production.

- **If you work with contract manufacturers**, you can leverage their expertise at the design phase. An integrated Quality Management System (QMS) will include tools that let you share plans and communicate with suppliers while protecting sensitive information.

- **Leveraging other Risk Assessment tools** can provide critical design insight. For example, bowtie risk assessment has long been used in the aviation industry to prevent and mitigate the effects of rare, high impact events. Some in the life sciences industry also use this model in certain circumstances, since product defects can have similarly large consequences.

2. Supplier Risk Management

Suppliers can be valued partners in your organization, but they also introduce risk. This is especially true if your organization manages a large supplier landscape. Quality issues with even a single supplier could lead to a recall, which is why it's so important to have processes to mitigate supplier risk.

Supplier Management tools can help in areas like:

- **Receiving and Inspections.** Automated Receiving and Inspection protocols and QMS updates help reduce shipments of poor quality materials. You can even make suppliers responsible for performing inspections to your checklist before releasing products for shipment to your facility.

- **Corrective Action tracking.** Effectively handling problems is key to effective risk management. Not only does an integrated QMS allow suppliers to view and track corrective actions in your system, you can also filter by risk to prioritize them.

- **Benchmarking performance.** Detailed Supplier ratings can roll up all of this data, also helping you track costs and risks associated with individual suppliers.

3. Making Corrective Action More Effective

In addition to risk-based corrective action filtering, a QMS with automated Reporting makes it simple to analyze root cause corrective action findings on a large scale, helping identify underlying trends that could lead to new controls.

Just as important, it's not enough to simply run a corrective action through the process of review, root cause analysis and action taken. There's also a critical final step—assessing whether the corrective action was truly effective.

How can you tell? By measuring residual risk. Quantitative Risk Assessment tools eliminate the guesswork, helping you see if what you did actually worked, or if you need to take further steps. Because as we've seen time and again, many disasters are the result of ineffective corrective action where someone cleaned up the mess without addressing its source.

4. Leveraging Post-market Feedback

Customer complaints and post-market feedback contain a treasure trove of information you can use to improve products. What's more, companies that don't effectively manage this information face increased risks of product defects down the road.

If you have an integrated QMS, you can easily launch corrective actions and run reports from the Complaint Handling module, ensuring all issues submitted to your company receive the proper attention.

These are just a few of the ways more effective risk management can reduce defective products. In truth, a truly integrated QMS will let you apply quantitative Risk Assessment tools to any process, whether it's equipment monitoring and maintenance, Job Safety Analysis (JSA) or Change Management initiatives.

An automated system is what ties the entire process together, allowing you to keep your focus on what matters—protecting the public and your company's reputation.

Learn more about how to reduce risk at your company by watching our webinar,

The Risk Management Primer: Getting Started with Risk in ISO 9001:2015.

Risk Management Strategies for the Supply Chain

The dynamic of business today is more complex than ever before. Globalization, product competition and the increasing of the supplier network has driven companies into far more directions. How can companies navigate the complexities within their organization, while keeping a strong level of compliance?

The key becomes one of risk-based thinking in supply chain quality. We recently held a webinar on this topic that gave advice on implementing risk strategies for the supply chain.

Here are 3 takeaways:

1. **The biggest gaps and risks in the supply chain center around communication:** A lot of the challenges around supply chain risk center around having a more traceable, visible way of communicating our key processes, and receiving timely responses to our processes and relationships with the suppliers. The concept of a supplier network is something that is not new, but the execution of this network often is elusive. There are solutions that exist to help us mitigate risk. Most notably, the ability to implement a piece of our system that is separated from our internal systems, but is interlinked in such a way that we can send information to suppliers, showing them only the elements they need to see, is becoming a key realization to achieving supply chain operational excellence. This, built along with a focus on risk mitigation becomes a cornerstone to getting to where we want to be.

2. **Risk is still a challenge, but the market (and standards) are moving in the right direction:** Risk management, like anything else, is a process. If you can define the steps and logically go about it, you'll be able to build a strategy that doesn't impede on your existing processes, but simply enhances them. Risk management starts with identification of any relevant risks. We want to look at our operations, and determine where the hazards are, and what the risk of those hazards might be. This is not done in a vacuum; you want to assemble a risk team to help identify these risks throughout your operations. Some of the risk management elements are available to us, and we just need to recognize that risk management in itself is a process, one that if followed, and inserted into our daily operations, can uncover more data, decision-making capabilities, and insights into redefining our supplier relationships. With these tools in place, we can effectively take our compliance and quality operations outside of our four walls and extend to a larger supply chain network.

3. **The key to success is using risk-based thinking to align our supplier management:** While risk management helps us plan and put controls in place, it also requires the proper onboarding, selection and review process within the supply chain. We need to make sure that our supplier approvals are based on more than just specification and cost. We need to shift our thinking to a standard supply chain, to a supplier network. This means that we leverage more suppliers, with risk-based metrics to assess the supplier performance, their viability as an organization, their vision alignment, their regional differences, and select from not just a few, but a whole host of suppliers within the network, based on a risk ranking.

We need to invest in technology to streamline the process. This isn't about connecting the suppliers to our systems alone; this is about building a way for us to create a secure, two-way collaboration with the supplier network to empower them to give us visibility and control over the process, create a seamless link from event detection to event correction across the supply chain, and be able to apply risk-based thinking to the process of supplier management. The supplier network solutions that connect the supply chain to your QMS can go both ways, and it involves the process of breaking down the silos from your processes to the supply chain, making it really one, centralized and standardized process. This is all great from an operational standpoint, but what you want to build in addition to this is a risk management strategy. This helps to truly define the levels in which a supplier is performing and provide you with more decision-making capabilities around the process.

Learn More by Watching the Webinar!

Creating a Risk Matrix: 3 Examples

Two things are true when it comes to making important decisions that impact your company. One, you need a way to quantify risk to make the best choice, and two, you need to be able to explain that choice.

A risk matrix helps you do both, calculating risk across various outcomes to give you clear guidelines on whether risk is acceptable or unacceptable. Let's take a look at the process.

How a Risk Matrix Works

In simple terms, risk is defined as the probability of an event multiplied by its impact. Levels of probability and impact can be broken up into verbal and numerical scales like so:

Severity		
Verbal	**Numeric**	**Description**
Catastrophic	5	Likely to result in death
Critical	4	Potential for severe injury
Moderate	3	Potential for moderate injury
Minor	2	Potential for minor injury
Negligible	1	No significant risk of injury

Frequency		
Verbal	**Numeric**	**Description**
Frequent	5	Hazard likely to occur
Probable	4	Hazard will be experienced
Occasional	3	Some manifestations of the hazard are likely to occur
Remote	2	Manifestations of the hazard are possible, but unlikely
Improbable	1	Manifestations of the hazard are very unliklely

The risk matrix then plots these variables in a color-coded chart to show overall risk for different situations (in the next column).

The quantified risk falls into one of three zones:

- Low risk that's considered acceptable (green)

- High risk that's considered unacceptable (red)

- Moderate risk which may or may not be acceptable (yellow)

Deciding whether risk is acceptable or not often comes down to a cost/benefit calculation. For example, it would be difficult to justify spending $2 million to prevent an ergonomic injury, whereas it would be worth it to prevent a chemical explosion.

There's a lot of variability in how to use a risk matrix, so here's a quick look at some examples.

1. Environmental Health and Safety

Let's say your company is trying to determine whether you need additional controls to prevent leakage of waste during transport via pipeline to a storage location.

The pipeline has had multiple maintenance issues, and it's located next to a regulated stream. You think it's likely some leakage may occur, and if it leaked you could end up killing off a population of endangered salamanders that live there.
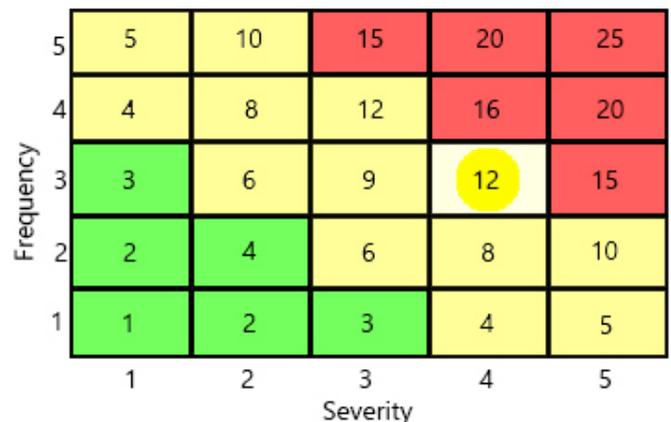
Automated risk matrix tools in your EHS Management System tell you this borders on unacceptable risk, so you decide to move forward with additional controls.

2. Quality Management

Let's say a supplier failure recently caused a problem at your company, and you've been tasked with identifying high-risk suppliers who need improvement (or who need to go altogether).

Your Quality Management System calculates each supplier's risk for you, showing that Supplier A has more incidents than Supplier B but actually poses less risk. This could be because Supplier B's product plays a strategic role in your process or consumer safety, while Supplier A's incidents have an overall negligible impact. You decide wisely to focus your efforts on Supplier B.

3. Food Safety

Here we'll use an example of a pathogenic hazard at a step where you're trying to decide whether you need another Critical Control Point (CCP) .

In this case, you've set up your Food Safety Management System (FSMS) to use a weighted scale rather than straight multiplication, with lower numbers representing a higher risk. Let's say internal policies dictate that anything receiving a risk rating of 1-10 needs a CCP. Based on how the scales were plotted, you can see high risk at top left and low risk at bottom right.

Since serious illness could occur and the situation is rated an 8, you will need an extra CCP. Your FSMS automatically feeds the information into your hazard analysis so you can record your decision.

It's important to remember the risk matrix is just a tool, not a solution. For true effectiveness, you need people on the other end interpreting the results, asking questions and vetting your risk matrix by testing it against historical data. With these pieces in place, the results are very powerful, helping standardize your decisions and providing quantitative justification for them.

Learn more about reducing risk in your company in our white paper: Building a Compliant Risk Management Program.

Where does Risk fit into ISO 9001:2015? 5 Takeaways from our Webinar

The dynamic of risk management in compliance today is experiencing a shift—one that is drawing more attention to leveraging risk management in operations. However, the biggest question I am often asked it that "I know I need to do risk, but I don't know where to start, and I don't know how to put it into practice." It's the practicality in daily operations that folks struggle with.

We recently held a webinar on getting started with risk management in ISO 9001 and this post will outline the key takeaways from this webinar. We will consider the context of "why risk" and how we look at risk management within operations, where risk fits into the new ISO 9001:2015 standard, some common tools you can leverage to make risk management a practical option for your business and more.

1. Risks and Hazards are Two Different Things

The terms hazard and risk are often used interchangeably; however, risk and hazard are two distinct terms, and do not necessarily equal the same thing.

Whether you are looking at quality, safety or any other business context, a hazard is a condition or situation that creates the opportunity for a problem to occur. They are the events we encounter each day that raise the potential for something "bad" happening. In business, hazards are everywhere and there are many types, but they only create the chance for something to go wrong—it is a potential, and not an actual possibility.

So...what is risk then? Risk is the likelihood that the hazard will lead to that negative consequence. Risk is the hazard multiplied by the probability of exposure to that hazard. So risks are not hazards—for this reason you can have a hazard that poses no risk, if there is no probability of exposure to that hazard.

The takeaway here is that risk is not just something that stands on its own and is automatic; it is a calculation of hazards and the likelihood of that hazard manifesting itself.

The key is that when you know your hazards, and you can estimate the probability of those hazards, then you have risk management in place.

2. Risk in ISO is Simply-Stated

Currently, the risk view on ISO 9001:2015 is simply stated. This means that it is not a directive to build an enterprise risk management program, or to change your entire processes to accommodate Governance, Risk and Compliance (GRC) initiative. It's part of the whole "broadening" of the standard, one that puts you in a mindset of risk over traditional terminology. The goal is to promote risk-based-thinking, which is fairly broad, and open to interpretation. so when we go through these next areas, keep in mind that this is designed to be an outline of a common method for risk-based thinking, and a generally accepted process. Every company should evaluate their own processes around the standard.
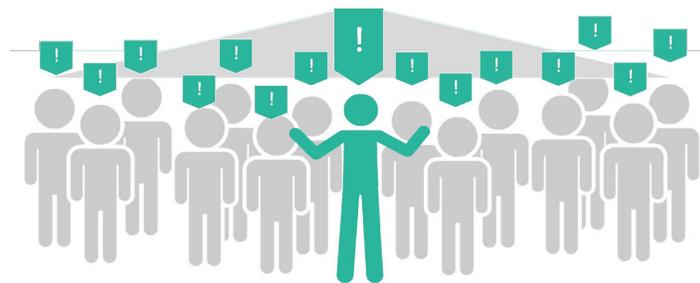
3. Where Do I Start My Risk Journey?

One of the most common things I am asked is, "how do I start identifying my risks?" First, you need to examine your operations, seek out potential hazards within those operations and categorize them.

How do you do this? By asking.

You can survey and audit your operations, like you normally would, but figure out the potential hazards from all areas of the business. Think about the problems that could occur, and how likely they are to occur. You'll probably get a lot of hazards, and a host of probabilities. The key is to collect and analyze the hazards and then categorize them. This is called a taxonomy of risk—general areas of hazard types in broader categories, and then you can make better sense of everything. Then, you can create general scales of severity of hazards and their frequency (likelihood to occur). Then you can have more variability, but it's the easiest and most logical way to identify and organize the overall risk levels.

Once you have that you can start evaluating the risk.

The next step is to calculate your risk. There are several ways to assess risk, but the bottom line is that you are doing the calculation on the components to quantify the risk. When doing this, keep in mind that risk evaluation and risk assessment are not automatic. Math is tricky; it doesn't always solve the problem, especially in operations. Too often, we hear of people implementing risk assessment tools that calculate risk, and they just leave it to the tool to determine the risk. The reality is that the tool is there to help you guide your decisions and risk calculations, but the ultimate decisions on how to handle risk should come from people. The tool is there as a guide, but most people will test their risk tools with real-world data. This is done by gathering as a risk team and reviewing risk calculations to confirm that the calculations actually reflect what would be done in the real-world. Some tweaking to the math may be necessary, but the treatment of risk should be a combination of people, process and tools.

The next step is to determine what you're going to do if there is a risk. This is where a cross-functional team comes in handy to review the different risk outcomes, and then determine how you're going to handle different risk levels.

Risk treatment typically falls into these broad categories:

- Acceptance—leave it if it's worth the risk

- Reduction—take steps to mitigate the risk

- Compensation—take steps to insure yourself against the risk

- Transfer—outsource the risk to a partner/supplier

- Avoidance—stop the process altogether

Each company has a different way of treating risk, and it's up to your risk team to determine which ways to interpret risk levels... but once you do, you need to take action on it.

This is where you need to incorporate your Quality Management processes to the dynamic. This is where you can kick off Corrective or Preventive Actions based on a risk level or risk treatment. You can also launch actions from Risk levels, taking specific management of change, or action plans to address the issues. Finally, you want to have reporting in place to analyze risks over time, so you can see where your top risks are and how you are doing overall as an organization in mitigating risk.

4. Use Risk Management for Opportunities, not just Risks

The ISO standard mentions opportunities as well. What this process does is not only look for the threats to your compliance, it also helps to uncover potential, but not yet realized hazards. Things that might not be risks today, but could potentially be risks in the future. For example, you can have a hazard that has a low probability, and thus the risk is inherently low. Does that mean you ignore it? Hopefully not—you take this as an opportunity to mitigate any potential risk, and seek ways to continuously improve. There are risk tools, such as Failure Mode and Effects Analysis (FMEA) and Bowtie analysis that deal more specifically in preventive aspects of Risk. So you should always take hazards, and identify whether this becomes a risk, or it may be an opportunity for improvement, in a more preventive way.

5. Documentation is Key

How can you document your risk management process and prove it in an audit? Here you have a process of risk management, one that might be incorporated into your existing processes. So the generally accepted practice is to document what you're doing and then document when you do it. So the whole risk management process should be documented, controlled, and built with work instructions and roles. This should be standard, especially when you introduce new elements to the existing process. For each step, you should be conducting activities that will be documented, have traceability, and can be tied to your overall Quality Program. So, when you're looking to identify the hazards, categorize them and build out the risk for them, this should be recorded in the results of the audits, surveys and analysis.

You should also be documenting the process by which you've built this risk measurement. Then, when you are building the evaluation and treatment of the risk you need to control the tool you use, you also need to document each time it's incorporated into a record. This is all about having traceability. Whether you're doing this manually, digitally, or through a technology solution, the traceability of the process, and the practice of that process is key. This also rings true when taking action.


This is all part of a process, and it's one that is fairly simply-stated in the standard. Any one of these steps can be considered "risk-based thinking" and applies to your Quality Systems compliance.

There's a lot going on these days—we have a new level of complexity in the marketplace, and it won't get any easier. So this complexity breeds a need for a new way of looking at compliance, and risk is that universal concept that is being pushed to be that new way. Even ISO 9001:2015 is picking up on this new way of thinking—we need to enroll everyone in quality, but we need risk in order to make it more digestible to all operations.

Risk in ISO 9001:2015 is a great way to look at risk management at a high level. We went through the path to success on risk planning, and it's really just a matter of taking these concepts, and applying them to your unique business. There are tools that can help. but remember, a tool is just there to help you— the risk journey starts with your people and teams that know the business, know the hazards and can help determine how to make risk work for your organization.

To quote one of my favorite books, "don't panic." You're not alone in the risk management journey, and by breaking it down into a more logical path, you can ensure risk can be implemented into your processes easily and effectively.
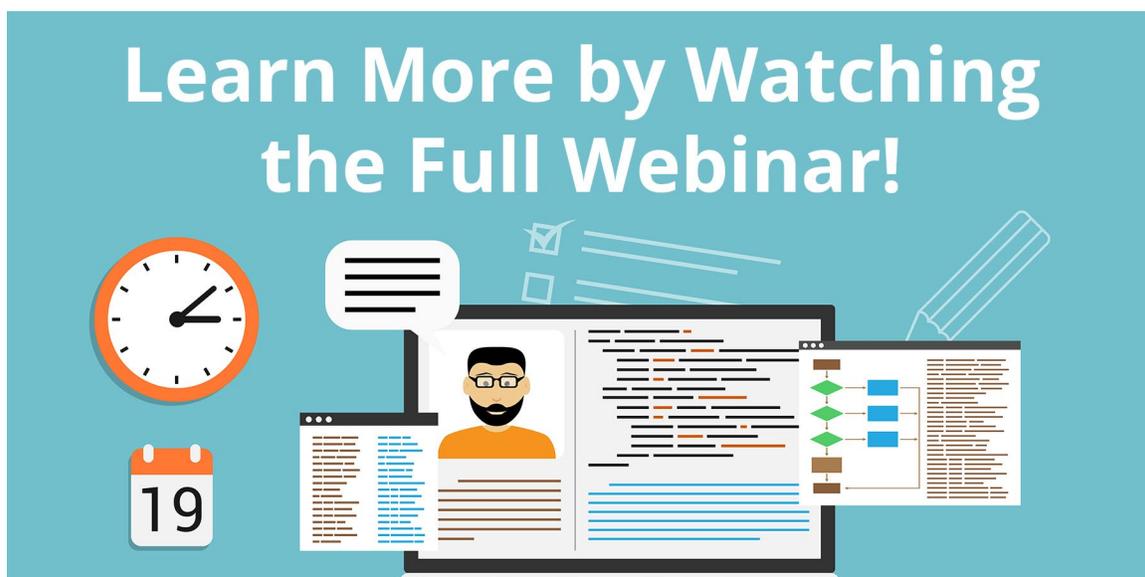
Risk and Reporting: 3 Hidden Problems with Point Solutions

Many companies today are highly specialized, from auto mechanics to home contractors to staffing agencies. "That's all we do," they say, whether it's repairing foreign cars or rehabbing 1920s Craftsman bungalows.

From the company's perspective, it makes sense—focus on what you do best. And in many cases, it's good for those on the purchasing end, too. I know I'd rather work with a contractor who has experience remodeling post-war homes in my specific neighborhood, just as an energy company might hire a consultant who works exclusively with the oil and gas industry.

But when it comes to building your quality, safety or environmental management system, cobbling it together with different software platforms—even if each is designed specifically for your industry—is a dangerous game.

Let's look at a few of the hidden risks associated with using point solutions this way.

Hidden Problem #1: There's No Big-Picture View

If you're using a mishmash of different point systems—say for Employee Training, Document Control, Supplier Management and others—it's unlikely they all take the same approach to quantifying risk (assuming each one incorporates risk at all).

Plus, risk affects every area of the business, from EHS to Quality, Finance and Human Resources. As much as we like to silo these areas, the truth is risk in one department usually connects to risk in another.

Without a standardized way to view, analyze and solve risk items, you inevitably create even more risk by constantly jumping manually between systems. There's no visibility, and things fall through the cracks.

Instead, you need a high-level view of risk across all your processes and departments, allowing you to better spot problems and how they affect other areas. A unified quality or EHS management system lets you do just that, with Enterprise Risk Management tools like:

- A Risk Register that serves as a central repository for all risk items and controls

- Risk templates you can drag-and-drop into any application to calculate risk at different points in the process

- Centralized Reporting that pulls data from multiple departments, allowing you to identify broader trends affecting the company

Hidden Problem #2: Corrective Actions are Like Swiss Cheese

A solid process for handling Corrective and Preventive Actions (CAPA) is one of the foundations of a strong quality or EHS management system. That's because if you don't have a way to effectively handle problems, they inevitably get bigger over time.

Corrective Actions touch every quality and safety process, and each one has its own level of associated risk. Point systems don't give you the visibility you need to prioritize CAPA requests, nor do they let you integrate action items across your processes.

A comprehensive system solves these problems, letting you:

- Use reporting tools that filter CAPA requests by risk, so you can prioritize high-risk items

- Launch Corrective Actions from any application, like Job Safety Analysis or Supplier Management.

- Trigger related applications from within the CAPA system itself, such as when root cause analysis uncovers a problem with Document Control or Employee Training.

Plus, a unified system minimizes risk by helping you report on Corrective Actions throughout the entire journey, from review to root cause, action taken and verification—even when these steps span multiple processes or departments.

Hidden Problem #3: Change is a Minefield

There's no question that executing change nimbly is a requirement to stay competitive in today's business world. The increasing pace and complexity of the global marketplace demands it, and you either move forward or get left behind.

The Risk Management Guidebook: Strategies, Tools for Success and Other Insights
www.etq.com · 800.354.4476 · info@etq.com

EtQ

Unfortunately, if your company uses a collection of point systems to manage the quality and safety process, Change Management is a difficult and risky prospect, and may lead you to avoid change. On the other hand, a comprehensive system eliminates a lot of questions, giving you better visibility through reporting to achieve change at minimal risk and cost.

Integrated Change Management capabilities help you:

- Use Decision Trees to determine the right type of change to minimize risk.

- Track change requests from start to finish according to pre-defined action plans

- Ensure appropriate changes are made to related areas, like key documents, Employee Training requirements and supplier specifications.

Choosing the right quality, safety or environmental management software is a serious challenge, especially considering all the specialized options out there. But ultimately, making sure everything runs smoothly simply can't happen if you silo your various responsibilities into different point solutions.

It's ineffective and risky, because it doesn't give you the reporting capabilities you need for a high-level view of how processes—and their risks—interact. Just like all the elements of the production process, you need a solution whose components work together, so you know all your quality and safety efforts are moving towards a unified end goal.

Why the Star Wars' Empire Needed Better Risk Management

As a business and risk professional, I can't help but wonder—what could have been if the Empire had more operational risk management processes put in place? You say, "it's a movie—get over it" and no one is more aware of that than myself but, just for fun, let's break down some of the concepts around the Empire's ambitious plans, and what they could've done if they applied some simple risk management methods.

Designing the Death Star

Aside from the fact that this was an incredibly inefficient means of weaponry, the Death Star was a deterrent on a scale no other sci-fi villain had ever undertaken. While I appreciate the magnitude of the space station, there were some inherent issues with the design. First, let's look at the initial Death Star. They clearly had a design team that wasn't looking at a small-scale assault. They figured that only interplanetary starships would take this weapon head on, so a small exhaust port would mean nothing to them, even if it was only the size of a womp rat. I would think that by using a basic risk in design process, like a Failure Mode and Effects Analysis (FMEA), they would've been able to create a list of potential failures, both small and large, to identify their core weaknesses and build controls around them.

The FMEA identifies potential failures in the design of a product before it enters production. What the FMEA does is break apart the product design into many of its components, and each component is analyzed and potential risks are assessed at the component level. You're looking for where the product can break, where it can fail (or where a Rebel pilot could jump in and launch a torpedo). The FMEA uses three dimensions of risk calculation—severity, frequency (or likelihood/occurrence) and detectability. Using those dimensions, it comes out with a Risk Priority Number (RPN). Based on this assessment, they can then effectively allocate their resources to those areas with the highest risk, or highest RPN for failure. This helps you prioritize your work more efficiently.

Maybe an FMEA could have helped the Empire identify potential failures to the Death Star. Then again, how BIG would that FMEA be, for a moon-sized product? Makes you think about the paperwork involved.

Job Safety on the Death Star

Let's continue with this thought process and think about the workers. Now, I'm sure the Emperor cared about as much for his workers as he cared about the furry little Ewoks that took him down (seriously, Ewoks?!?!).

But let's consider this exchange, as seen in Star Wars: Episode VI—Return of the Jedi:

Moff Jerjerrod: I assure you, Lord Vader, my men are working as fast they can.

Darth Vader: Perhaps I can find new ways to motivate them.

Moff Jerjerrod: I tell you that this station will be operational as planned.

Darth Vader: The Emperor does not share your optimistic appraisal of the situation.

Moff Jerjerrod: But he asks the impossible! I need more men!

Darth Vader: Then perhaps you can tell him yourself when he arrives.

Moff Jerjerrod: The Emperor's coming here?

Darth Vader: That is correct, Commander, and he is most displeased with your apparent lack of progress.

Moff Jerjerrod: We shall double our efforts.

Darth Vader: I hope so, Commander, for your sake. The Emperor is not as forgiving as I am.

The poor guy was faced with the prospect of a smack down if he didn't push his workers to the limit. He needed to consider the potential hazards and their impact on not only the workers but the finished product. This is where a hazard analysis and job safety program could have helped.

Through the use of a Job Safety Analysis (JSA), the Empire could have looked at the job steps the workers take and determine the risk of each step. Through a risk matrix, they could've seen what areas have the highest risk for failure, and put in controls to make the job safer and more efficient. Then, by streamlining safety, the workers would've been more efficient and safer with reduced errors and incidents. However, as I said before, the Empire seemed to care little for the safety and well-being of their workforce, so it's likely this would never have happened. But, you can do it in your organization, so your own personal "Darth Vader" doesn't have to come to put YOU back on schedule.

Bowties Might Have Saved the Empire

No, formal wear is not what we're talking about here. In this case, we are talking about the risk management modeling tool that helps to map our potential risks, build preventive and reactive controls and mitigate risks before they happen.

Unlike the previous tools, Bowtie is considered a proactive risk assessment tool in that it looks to mitigate risk before it even happens. This model really looks at the undesired effect (which is usually something bad, like the end of the Empire), and builds out controls as "barriers" to prevent that event from occurring. Here's how it works—you have an undesired event in the center and you analyze the impact of that event. You are effectively building out a scenario in which that event might occur and putting preventive controls in place to mitigate the risk of it actually happening. Similarly, you also want to build out recovery controls to minimize the impact if the event does in fact occur.

So let's think about this. What the Empire should have been doing is modeling their campaign to dominate the galaxy with risk in mind. Sure, the Empire never considered a rag-tag bunch of Rebels a threat, but that's why Bowtie exists—sometimes the most remote threats can have a cascading impact. By looking at the potential threats, such as a Rebel fleet amassing, a burgeoning Jedi coming up through the ranks, and Ewoks (yes, Ewoks) they might have been able to build out preventive controls. Maybe they would've caught the small-scale assault option; maybe they would have realized that their deflector dish was exposed to an army of teddy bears, and maybe they would have thought putting their Emperor in the middle of the battle was a bad idea.
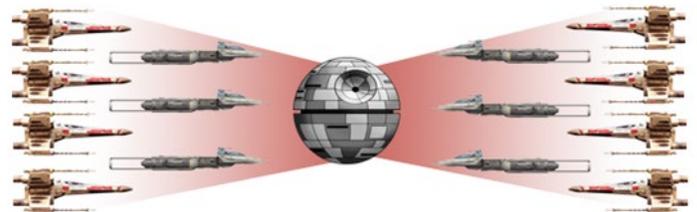
THE EMPIRE BOW TIE RISK MODEL

Moreover, Bowtie helps to build in control if in fact the undesired event happens. Let's say the Empire is attacked and is squashed, what then? Well, they could have cloned the emperor (which, if you're a fanboy like me, they technically did), they could have moved the Empire fleet away from the battle immediately, or they could have kept more senior staff in remote areas to ensure that the Empire continued on. It's a real-world problem addressing fantasy, so it's a little bit of a stretch, but it's something that most organizations plan for with Bowtie, and they become more effective in identifying, mitigating and preventing high-risk events.

So, the Empire was rife with risk, but you don't have to be. By implementing common risk management processes, you can ensure your products are designed with risk in mind, your workers are operating with safety and risk mitigation in mind, and you are protecting yourself against potential risks that may have not yet occurred.

Don't be like the Empire—build risk into your processes today!

5 Lessons Your Parents Taught You About Risk Management

Riding in the car as a kid, my mom would always warn me, "Don't stick your arm out too far, or it might go home in another car." Never mind this was a time when we roamed around the car freely, and forget about car seats past age three.

Parents have always been full of creative warnings, and while they can be funny, the truth is our parents actually did know a few things about risk management. Here are 5 things they taught you that are still true today.

1. Look Both Ways Before Crossing the Street

Identifying hazards is a crucial element of risk mitigation. Strong observational skills help you better spot hazards, but quantitative risk assessment tools are a must.

For example, Job Safety Analysis (JSA) lets you look at hazards on a granular level, applying quantitative risk scoring to every step of a work procedure. On a larger scale, Enterprise Risk Management (ERM) tools standardize risk assessment to identify trends and enhance visibility across the organization.

Making good decisions requires analyzing options according to the quantitative risk associated with them. An EHS management system or quality management solution gives you the tools to do it consistently and objectively.

2. Use the Buddy System

How come nobody ever asked what would happen if both buddies went missing on the field trip? In all seriousness, teaming up with others is practically a requirement for effective risk management. That's because new eyes bring fresh insight, often leading to process improvements that reduce risk.

Whether it's a safety consultant, an EHS Software vendor or an ISO auditor, working with outside experts helps you dig deeper when addressing risk. Plus, it helps you get more done in less time so you can better leverage existing resources.

3. An Ounce of Prevention is Worth a Pound of Cure

Many companies rely on manual processes to manage safety, quality or compliance. It's time-consuming and inefficient, keeping organizations stuck in reaction mode rather than proactively mitigating risk.

It's far better to take a preventive approach to risk management, but being efficient means ditching the old filing cabinets and moving to a system that ensures issues don't go unnoticed.

Predictive tools such as Bowtie Risk Assessment highlight the role of prevention in risk management. Companies in industries like chemicals or oil and gas use the bowtie method to reduce risks associated with rare, high-impact events like wellhead blowouts or toxic chemical releases. The bowtie diagram identifies controls to prevent the event, as well as ones to mitigate its consequences. Predictive tools are essential for incident prevention, especially for events where an organization has little data to go on.

4. Call and Check In

Just like the check-in call told your parents you weren't lying in a ditch somewhere, reporting to a third party mitigates risk by ensuring you meet certain safety or quality benchmarks. Whether it's OSHA 300 logs, ISO certification, Sustainability reporting or an internal meeting, increased visibility through reporting goes a long way toward mitigating risk.

In the past, reporting was a major hassle for companies. Now, Centralized Reporting tools in EHS and quality management solutions make it easy to gather data from across the organization, pulling info from multiple applications for an instant snapshot of important risk trends. Some systems can even alert you to events as they happen (or before), with automatic notifications for specific events like abnormal monitoring results.

5. Plan for the Worst, Hope for the Best

Being ready for the worst-case scenario is a critical element of risk management for any organization. This includes tools like bowtie diagrams (mentioned above), as well as Crisis Management and Emergency Preparedness plans. For most companies, these plans aren't just a good idea—they're also the law.

But you can't just haul out some overstuffed binder and try to pass it off as an Emergency Response Plan (ERP). To ensure your organization is actually prepared, you need an up-to-date record of who's responsible for certain procedures, the equipment needed and how to work with external parties like fire and hazmat teams. The right software will let you link all these elements together, also making it easy to collaborate with others on them.

Reducing risk can seem like a huge challenge, but the science of risk management is actually rooted in the common-sense lessons we were taught as children. As much as we hate to admit it, it turns out our parents were right—at least about some things.

EtQ

www.etq.com	**800.354.4476**
info@etq.com	**516.293.0949**