Building a Compliant Risk Management Program

THE RISK IN QMS & EHS GUIDEBOOK

Table of Contents

Steps to Building a Risk Management System: Influencing Compliance

As markets continue to evolve, organizations are evolving their definition of compliance. From an operational context, the speed and level of complexity within the market is driving faster product lifecycles, more extensive and complex supply-chains, and a need to remain competitive and compliant. For many, this task cannot be achieved through the methods of old; new benchmarks need to be implemented that have the agility and consistency to respond to market needs and make informed and logical decisions.

Risk Management is fast becoming this new benchmark for this decision-making paradigm. The concept of risk has spanned the entire enterprise, and fits many different aspects of business—financial, health and safety, environmental, Quality and Compliance, and more. What makes Risk so powerful in a changing world is its consistency—Risk is an objective, systematic and repeatable method for identifying hazards and assessing the level of the harm the hazard may incur. Whatever the event or hazard, Risk remains consistent; this is what makes it universal to all operational areas, and why it is a powerful means of analyzing and making better decisions.

Starting Points: How to Define your Risk

The challenge for many companies is not in the decision to manage risk, but in knowing where to start in building a Risk Management program. "What are my risks? Who determines the level of risk? Who needs to know? What actions need to be taken? What processes need Risk Management?" Questions like this and more plague many organizations, and they will spend more time and effort in this phase of their process than any other when building a Risk Management program.

Enterprise Risk Management: Taxonomy of Risk

Taxonomy is an important part of the Enterprise Risk Management (ERM) System process. Taxonomy is defined as the method by which we categorize and aggregate the risks within the company. The purpose of categorizing risk allows an organization to create a common set of risk types that can be utilized throughout the organization, not just in one operational area. This is the universal nature of Risk Management; it is able to translate itself from all levels of the organization, and is a stable way of benchmarking compliance from all operational areas. Some examples of common taxonomies are listed below—each category represents an area where a potential hazard or threat can exist.

With this taxonomy in place, we can begin to categorize any risks and hazards that we identify as we begin our risk journey.

Start with Hazards: The Hazard Register

Before you begin with any element of risk management, you need to know where the trouble is, or might be. A hazard is defined as any situation that poses a threat to life, health, property or environment—it's an undesired event. Every company would have these, and the key is to create a determination of what these hazards are.

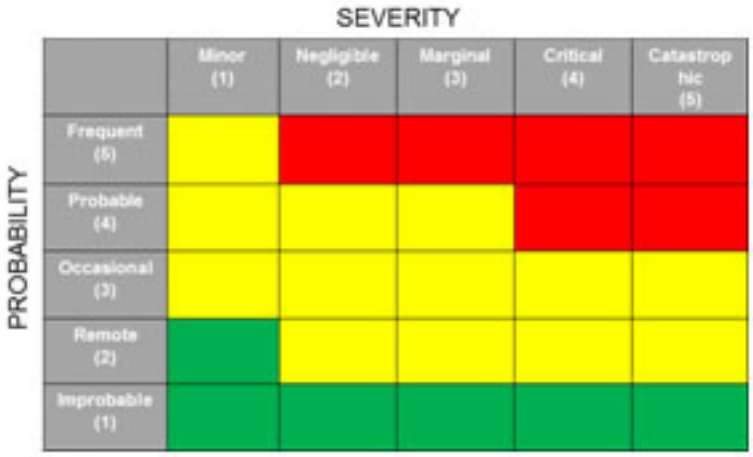
So, how do most organizations determine this? They simply go out and ask. Go to within the company and survey the operational managers of threats and hazards, gather a team together and create proposed hazards that may affect the organization, or go into the historical data and look at past events and the hazards that caused them. You can also seek external help for standard, common hazards within the industry, but take these with less weight—what may be a hazard for the industry may not necessarily apply to your organization.

Measuring Hazards through Risk Assessment and Risk Scenarios

With a library of hazards within the system, we now need to measure these hazards using Risk. Risk is defined as the potential that a chosen action or activity will lead to an undesired event. It is the conditions in which the hazard may present itself. Risk is essentially the severity or probability that a hazard would occur.

Examples of Common Taxonomies		
Business processes	Information management	Program design & delivery
Capital infrastructure	Information technology	Project management
Communications	Knowledge management	Political
Conflict of interest	Legal	Reputation
Financial management	Organizational transformation & change management	Resource management
Governance & strategic direction	Policy development & implementation	Stakeholders & partnerships
Human resources management	Privacy / Information stewardship	Values & ethics

If we have a library of our hazards, we can then use risk calculations to determine the level of risk each of these hazards presents. Having a library of hazards in the system enables you to more effectively assess and rank the risks you are calculating. This is usually done in the form of a Risk Assessment. A Risk Assessment is a formula or set of rules that determine how severe or frequent the hazard will be, and assigns a level to that threat—i.e. Risk Level. A Risk Matrix is the most common method for determining Risk levels, and provides a clear and easy-to-understand view of the risk of the undesired event.

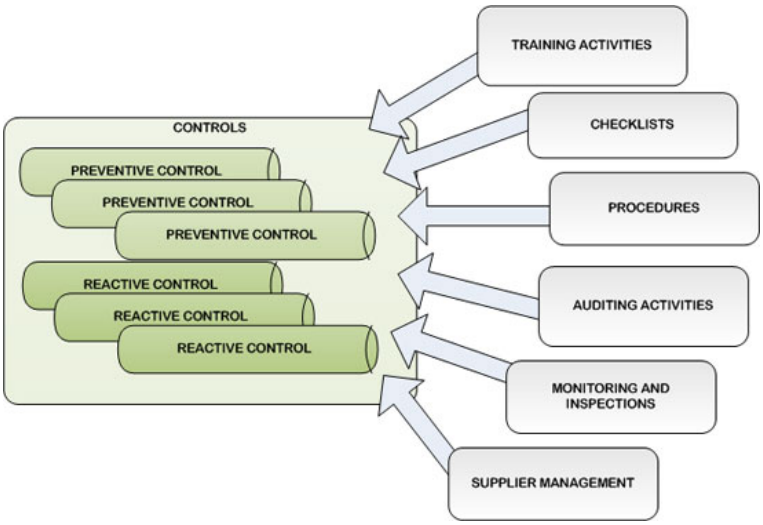


Risk Scenarios Provide the Complete picture of Risk Management

In order to truly be effective, Risk Management needs to be a collaborative process. Most organizations create risk teams to review hazards and conduct Risk Assessments, and the process must go through a review and approval workflow. In a risk scenario, hazards are flagged and Risk Assessments are conducted. Hazards can occur in many areas within the organization—financial, operational, quality, compliance, etc.—and each area must be flagged and assessed, providing a level of risk on many dimensions. The resulting calculations present the overall risk of that hazard.

Building Controls into Risk Scenarios

Now we've identified the undesired events (hazards) within the company, and we've assessed the potential of that undesired event occurring (risk), so how do we reduce the level of risk to an acceptable level? Controls are defined as the methods for evaluating potential losses and taking action to reduce or eliminate the potential for an undesired event. There are many ways in which organizations implement controls—new procedures, training, checklists, process changes, product strategies, business decisions and more – essentially these are processes that are designed with the reduction of the risk of that hazard in mind. Controls can be related to many hazards, and one control process or event can be related to many hazards, and vice versa. The goal is to reduce or eliminate risk before the undesired event occurs, and controls are put in place for this purpose. Controls can be preventive in nature, in order to prevent the hazard from occurring, or controls can be reactive to recover from a hazard that has already occurred, to mitigate the overall impact or outcome of the event.



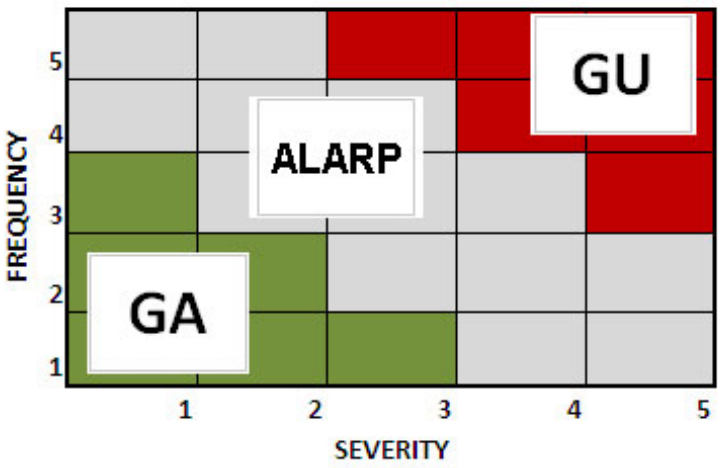
Acceptable Levels of Risk: Action Plans for Mitigation and Reduction of Current Risk

We've now created a roadmap for our current risk—hazards now have a risk associated with them, and we have controls in place to reduce the risk. But what if the risk level is higher than we'd like it to be? How do we take action to reduce the risk to a level we feel is acceptable?

The goal of Risk Management is not only to identify our risk, but to take steps to mitigate and reduce the risk to a level that is acceptable. This may not be the case in our current risk scenario; controls are in place to mitigate the risk, but what if we want to lower the risk beyond what it is today? Setting an acceptable level of risk is an important part in the Risk Management process.

However, what is considered "acceptable"? Many companies will interpret acceptable levels of risk differently. Most organizations will immediately know what is generally acceptable risk, and generally unacceptable risk. But there is a "gray area" in between those extremes that many companies will try and quantify. There is no such thing as "risk free"—there is always some level of risk in any hazard or event. What we can do to mitigate the risk is determine which levels we can continue to effectively and logically continue business operations, and set that as our lower threshold for risk. This term is usually defined "As Low as Reasonably Practicable" (ALARP), and helps to define the middle area of a company's risk foundation. This helps to define the various levels of risk within the organization, and then set the mitigation plan to conform to those levels.

Action plans are nothing more than projects; the tasks and deliverables necessary to ensure that actions we take over the course of time will bring those risk levels down to our acceptable level. This could be in process improvement, employee training, operational



change management, and many other ways that would impact the risk of the listed hazard.

Risk Scenarios Are Process-Driven

As stated before, Risk Management does not operate in a vacuum—it requires a team to review and collaborate on levels or risk and actions behind them. Risk Management is a continuous process, and requires a level of review and approval risk scenarios. Risk scenarios define risk for your organization, and these scenarios are not static; they change as your operations change and evolve. Any change in your business model, will have an impact on risk scenarios. These changes will affect how your interpret risk at every phase in your operation, so it is critically important that as you change processes, so too will the risk scenario change.

Risk Registers Become a Library of Risks

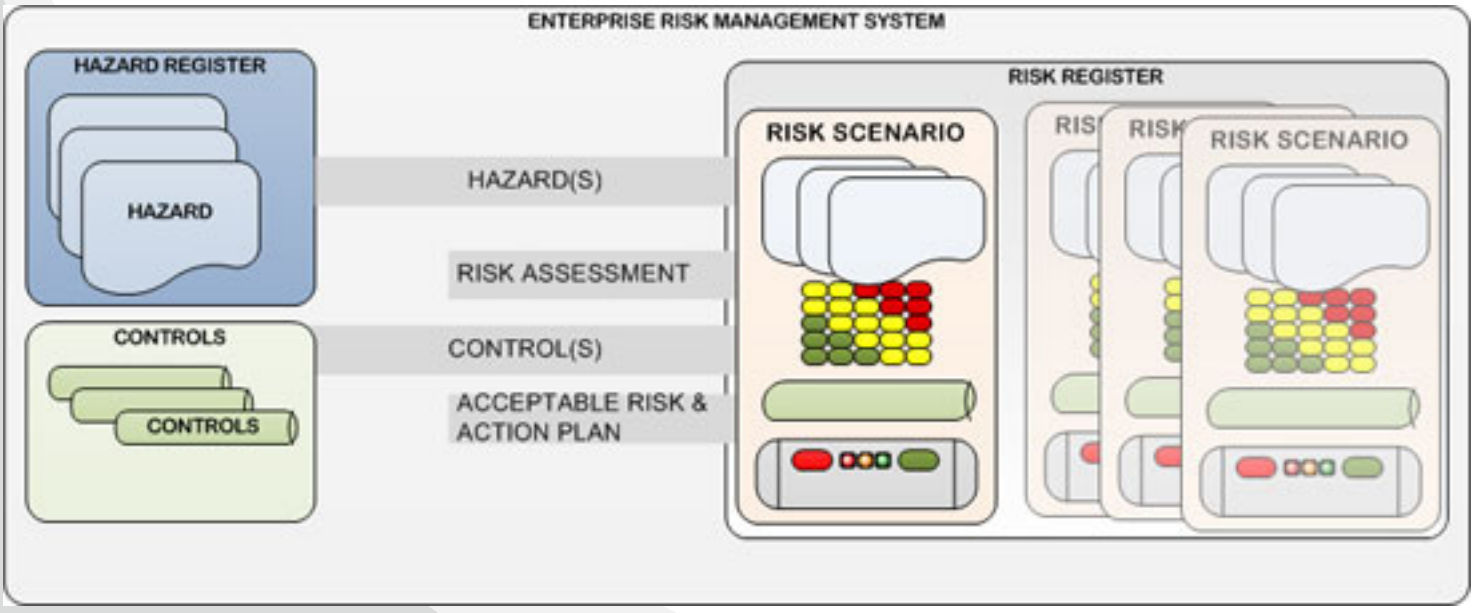
Taking our hazards and putting risk levels to them, and placing controls to mitigate them is all part of a risk scenario. This is only the first step, however, in a Risk Management System. Once we created a series of risk scenarios within the system, we need to have a place to centrally store these scenarios, so that when we actually encounter these events in our daily operations, we can reference them and take action. The Risk Register is a library of all our risk scenarios, that enables us to review all the risks within the organization and begin to do analysis and trending on the risks within the company. We can reference past risk scenarios to impact potential future risk events, and derive preventive actions towards future risk mitigation.

Risk Dashboard and Risk Reporting: With the Risk Register in place as a comprehensive library of risks, this level of data on Risk Management is a valuable tool for the entire enterprise. Building a library of hazards and risk levels is only one part of the story; in order to really be effective, you need to create a level of visibility into this data to analyze and interpret the data. Risk Reporting is a critical component of ERM, and uses the data within the risk register to generate reports and metrics surrounding risk.

Not only will you be able to uncover risk from one operational area, Risk reporting enables you to build risk reports that span operational area and uncover trends you may not otherwise see without visibility into this data. Risks from one area can easily be transferred to others—seeing the implications and proactively mitigating risk is all part of Risk reporting. Furthermore, you can build entire dashboards of risk ranking and risk scenarios, so that management can see what areas in the organization have the highest risk, or even monitor where risk levels are and make assessments to where to focus attention.

Putting it All Together: Compliance Management and Risk Management Activities

With ERM built into our system, organizations can plug the risk data into all the processes within any operational areas where the common threats are known. Risk built into the process ensures

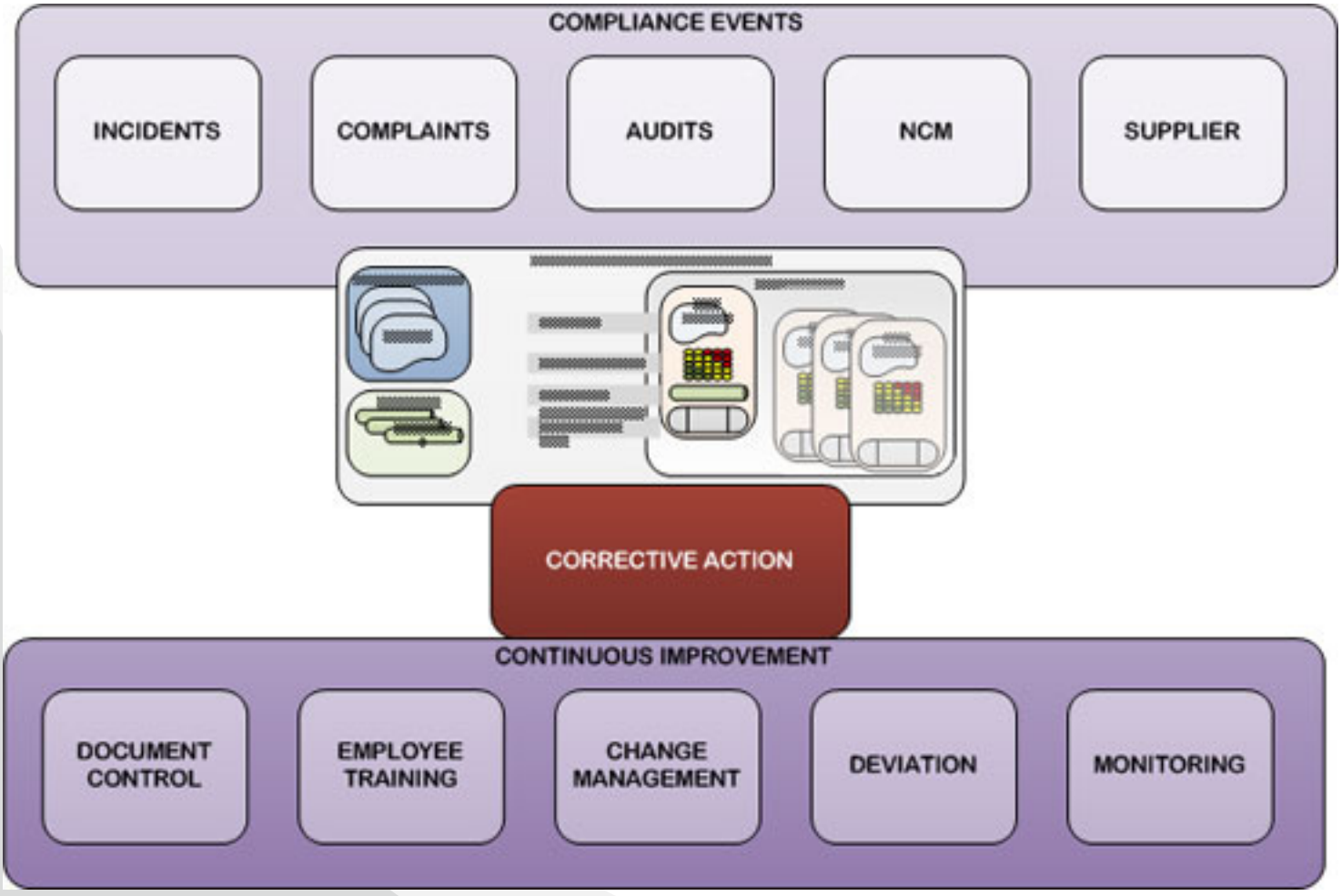


that normal operations take into account not only the daily operational needs, but also add a new dimension—risk—to the process. As events enter the various compliance systems, you can draw from the Risk Registers and risk scenarios to assign levels of Risk and make better decisions to each event. Once risks are quantified and decisions are made, you can influence change more effectively, and seek to mitigate or prevent risks from occurring (or recurring). Below is an example of how the ERM System is built within a Compliance Management framework.

Risk Management is not an automatic process. It requires a level of collaboration and communication from all areas of the enterprise to determine the level of risk, and how to control the risks within your company. Many organizations will assemble risk teams from all operational areas to determine hazards and threats, derive risk levels for hazards and put in place appropriate controls to mitigate those risks.

Conclusion

ERM Systems attempt to build a framework for these risk activities and create a library of existing and potential risks, so that as you conduct operations within the business, you can incorporate risk into these processes to make more informed and better decisions.



What You Don't Know CAN Hurt You: Risk Registers Are Key to Compliance Management

There's a lot of talk around compliance these days. Compliance is a broad term in itself; it covers many operational areas—Quality Management, Environmental Health and Safety (EHS) Management, Governance, Supply Chain—the list goes on. Compliance encompasses a lot, and it's really at its definition an adherence to any policy, standard or regulation set forth by an organization or regulatory entity.

Compliance, however, isn't really the whole picture. Compliance doesn't help you prevent adverse events, it provides the guidance for proper avoidance of those events. Typically, changes to policies and procedures are a result of a non-compliance event—Corrective Actions, adverse events, Audits, or similar processes. What aren't covered are the predictive methods to look at your existing operations and determine areas where potential non-compliance can occur. The reality is, if you are not looking at these potential problem areas, you are facing threats to compliance. How can you effectively look at your existing system and search for data points that might threaten compliance. The answer is Risk.

Risk Management is a larger component of Compliance—in fact, you could argue that without some level of risk management, you are not effectively tracking compliance. Risk is the ability to perceive potential threats and hazards and make decisions to positively impact your compliance to whatever standards, policies and regulations you are striving to adhere to. Risk Management is a method for looking for hazards and threats, making decisions on how to handle those threats and hazards, and then focus on controls and preventive measures to mitigate risk and maintain compliance.

The Risk Register: Your Window to Assessing Compliance

In any system, QMS, EHS, GRC or others, data is king. Every system is a wealth of compliance data—trouble in, corrections out, and the data and history of every event in between. With all the data within the system, you can analyze, trend and predict similar events in the future. The Risk Register takes the data, and applies common risk methodologies to it. It takes the historical data and assigns risk rankings to each event, so that you can effectively build a "risk portfolio" or past events to help dictate future occurrences.

Like many things in life, we look to the past to determine our future—this is the Risk Register.

Risk Register Data Proactive Analysis to Impact Events before they Occur

Having a portfolio of compliance risk can provide a risk history that will help organizations assess their current operations and improve similar conditions before they potentially occur.

The Risk Register collects data from many operational areas, and compiles them into a risk portfolio. From this risk history, organizations can make decisions, and anlyze and trend to mitigate future adverse events.

Consider the following example:

> *Company XYZ had a series of adverse quality events at site A, arising from a faulty machine. The Corrective Action indicated that maintenance was only performed monthly, and if weekly maintenance was performed, the risk of failure would be lowered within acceptable risk parameters. Sites B, C and D have the same machine, and still perform monthly maintenance. By viewing the Risk Register, the company can update maintenance schedules to weekly for all sites, and mitigate risk of adverse events for all sites, saving potential Quality issues going forward.*

A basic example, but it make sense—looking at data from one series of data points, you can impact other areas within the organization. Risk histories are good for this purpose. Look locally, and act globally.

Risk Registers Provide Cross-Operational Reporting

In the real world, and more poignantly the business world, Risk is the universal translator for an organization. Operational areas speak their own language—Quality doesn't have the same terminology as EHS, nor does GRC and Supply Chain Management. To roll up reporting from each functional area would be a mess of jargon and nomenclature—executives would need a glossary for each decision they had to make.

Risk registers roll up Quality, EHS, GRC and other data into a single common language—Risk. This way, you can see top risks within the organization and the events that are causing these risks. Risk data makes for easier decision making, and it also fosters the ability to implement changes that span these functional areas. A risk stemming from a Quality operation can have an impact on Safety processes. By creating a cross-functional approach to Risk and Compliance, you can make decisions that will impact many areas all at once.

Knowledge is key to compliance; the knowledge is hidden in the data, and the best way to uncover the knowledge and make compliance decisions across the enterprise is through Risk. Let's recap:

1. **Compliance is the result of a good risk mitigation strategy.**
2. **Risk Registers are the key to collecting risk-based events from the entire enterprise.**
3. **Visibility into top risks can help make better decisions; past event can help dictate future actions.**
4. **Risk is a universal language that everyone can understand.**
5. **Key elements of change and compliance management arise from knowing our past risks and making informed decisions to impact the business.**

Conclusion

So, what you don't know CAN actually hurt you—implement a risk register, and start collecting risk to help "futureproof" your enterprise.

The Risk and Compliance Paradigm: Risk Management's Impact on QMS

We continue to write about and develop solutions centered around Risk Management, and Risk remains this enigmatic and elusive concept. The perception is that they are so concerned with operational issues, that conducting risk, while strategically significant, seems way off in the future for them. This is far from the reality—in fact many companies are already doing risk in some way or another, and not even knowing it.

Risk Management is everywhere, and is not some lofty strategic element that is limited to top floor suits making enterprise-wide decisions. Risk is just another tool in the quiver of the compliance process; it is a method for streamlining your business, like any other compliance process. The ISO group has seen this for many years, and is looking to push Risk into its various standards.

Risk Management is becoming an integral part of the compliance process. Like anything else, Risk Management is simply a process. It's a means of looking at potential hazards, assigning a weight to those hazards, and taking steps to control those hazards. *(See figure 1)*

ISO Standard	Risk Management Elements
ISO 31000	– Guidance for risk management in any organization – Not industry specific; applies to any risk; not intended for certification
ISO 14971	– Guidance for risk management in Medical Devices
ISO 14001 & OHSAS 18001	– Identify and assess every risk – Mitigate significant risks and control minor risks
ISO 13485 & ICH Q10/Q9	– Med Device and Pharma: Explicit reference to risk management
ISO 27000	– Primary focus is risk, taking into account threats, vulnerabilities and impacts
ISO 9000	– No direct reference, but stay tuned—2015 revision has extensive RM elements planned

It's a fairly straightforward method for conducting analysis and mitigating hazards. There are many ways to look at Risk, and each industry has developed different risk based tools to suit their specific business needs. Here's just a sample set of some risk tools:

- **Risk Matrix:** A useful (and colorful) matrix that takes typically two metrics—severity and probability, and ranks them in a grid to determine either a number or color.
- **Failure Modes and Effects Analysis (FMEA):** Is a design or process method that breaks down a product or process to its individual components and conducts a "what if" scenario to identify failure points and control these potential failures at the most base level. Once the product of process is rolled back up, the risks are identified and mitigated.
- **Decision Tree Analysis:** This is another method that outlines a "what if" scenario. By answering a series of questions of conditions, you can follow the tree through logical examples, and come to a decision on the overall risk.
- **Hazard Analysis and Critical Control Points (HACCP):** Commonly used in the food industry, HACCP breaks a process into steps and conducts a hazard analysis on each step; "what could go wrong, and how can we control it?" For each hazard, a control is implemented and a risk is mitigated.
- **Bowtie Risk Methodology:** This is a risk method designed to assess low-occurrence events, but when the occurrence is often very serious. Airlines use bow-tie very frequently, because the emphasis is not on the risk of an occurrence, it is more on the measurement of how effective the control is. What's attractive is that it is easy to read and translates well to all areas of the organization. *(See figure 2)*
- **Risk Register:** The Risk Register is like a library of historical risks and their outcomes. For every event with a risk associated with it, the risk register collects the data and is used to create visibility into the risk timeline of an organization. This helps to provide trending and analysis on future events based on the past risk of similar events.

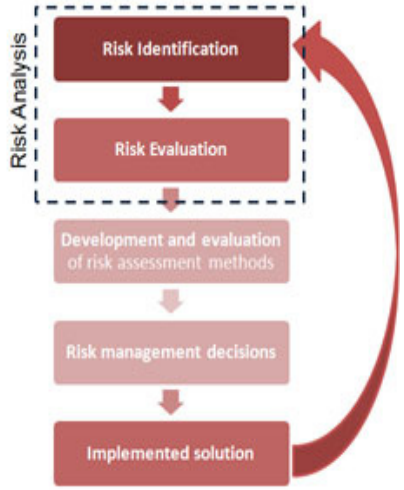
People ask, "Why risk"? Quality Management processes works just fine, and we report on Corrective Actions well enough. Well, reporting at the operational level works, but when you want to report across industries, it becomes necessary to normalize the data for making aggregate decisions. Risk is that universal language—some final thoughts:

- **Risk Management is not automatic; it requires people:** All these tools and technologies will only help you with Risk. The real Risk Management process happens with the people making the decision. Assemble a Risk Team, a cross-functional group that can sit and review the different risks, and weigh them using risk tools to come to a decision.
- **Risk is universal in terms of the enterprise focus:** Not all people speak Quality; not all people speak Safety; everyone speaks risk. When rolling data up to the enterprise level, normalizing operational processes in terms of risk help to create a universal language that decision makers can use to make better decisions.

Conclusion

And that's why Risk Management is continuing its charge through the Compliance industry—the tools outlined above and other tools (Fault Tree, HazOps, and so forth) are prime examples of how Compliance processes, whether Quality Management or others, are utilizing risk as a core benchmarking metric for decision-making in the enterprise.

Figure 1



Identify all relevant risks (e.g., hazard analysis)

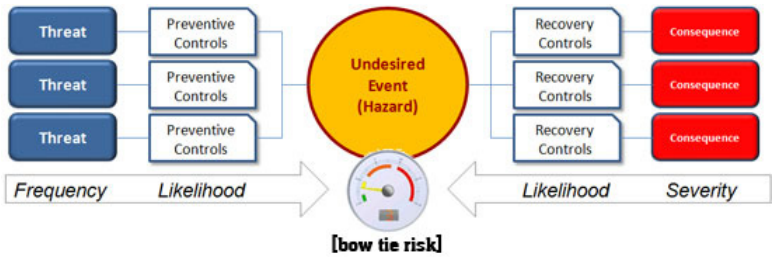
Quantify the risk (e.g., probability and severity)

Measure and monitor risk with objective, proven tools

Assessment: Accept (worth it), reduce (mitigate), compensate (insure), transfer (partner), avoid (stop)

Change management to introduce or improve controls

Figure 2



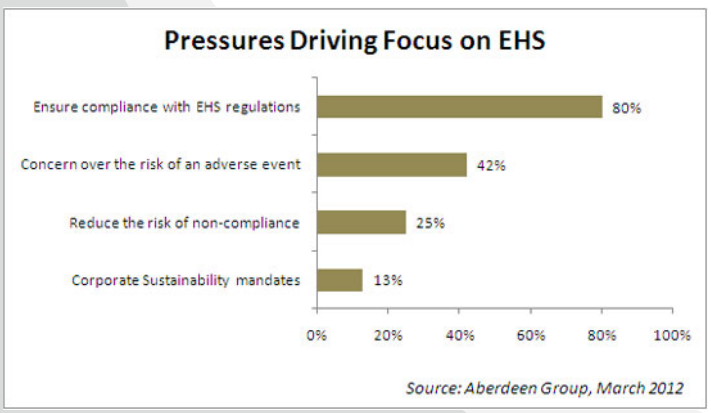
Does your EHS Software System Speak Risk? How Risk is Applied to EHS

Risk is fast becoming the strongest and most comprehensive way to benchmark compliance, make more informed decisions, and enhance visibility into areas of improvement within the organization.

For Quality Management and Compliance, this is a common trend, but what about EHS Management? Risk is equally as important in EHS processes, and can help drive better compliance to initiatives in tracking and improving safety within the organization. According to a recent report by Aberdeen Research, risk plays a large part in EHS Compliance:

These metrics show that risk is a growing factor in how organizations perceive their EHS compliance, and how they build their EHS processes. The question then becomes, "Where can we build Risk Assessment tools into common EHS processes?" Here are a few examples:

1. **Risk Coupled with Incident Management Filters Critical Events:** As safety professionals know, EHS systems most commonly have a way of tracking adverse safety events—"Incidents." Incidents can take many forms, whether Injuries or Illnesses; Fires or Explosions; Chemical spills or Hazardous Materials; the list goes on. As part of compliance, it's important to record incident data thoroughly and collect as much information as possible. This is partly good business practices, but also is a requirement of many regulatory reporting initiatives, such as those mandated by OSHA. Risk can be a critical factor in further identifying incident data. Using Risk Assessment, safety managers can filter incident data by risk factors such as severity or frequency. Risk matrices can help to make better decisions on how to handle incidents. More critical incidents rise to the top of the list, and have more importance than less critical events. This enables the safety team to address the more important issues within their Incident Management program.



2. **Risk Provides Consistent, Quantitative Benchmarking for Job Safety/Hazard Analysis:** Using Risk to ensure safety is not only beneficial as a reactive approach, but also in proactive planning. A good example is in Job Safety Analysis (JSA). JSA takes a job description, breaks the job to its individual steps and inputs the potential hazards of those steps. It then implements controls for these steps and seeks to improve the safety of a job at the most basic level. Risk is a prime way to assess the safety of job steps in a JSA. Leading JSA programs will look at the potential hazards and assign a risk level to those hazards. Then, by implementing a series of Personal Protective Equipment (PPE) and controls, they can seek to reduce the overall risk of that step. By reducing the risk within each step, you've automatic reduced the risk of that job as a whole. Risk is a great way to quantitatively measure and benchmark Job risks in a systematic way.

3. **Risk Can Provide a Quantitative Measure of Effectiveness in Corrective Action:** In much the same way risk can be used to filter the level of action to be taken on an incident, it can also be used to determine if a Corrective Action was truly effective. As part of the Corrective Action process, a root cause analysis

is designed to investigate the incident. The Corrective Action phase puts measures in place to correct the systemic issue, and Verification and effectiveness seeks to prove the corrective action worked. Risk in Corrective Action can be used as a way to benchmark effectiveness by measuring residual risk from a corrective action. By measuring the residual risk, organizations can analyze the corrective action to determine whether the action taken reduced the risk of recurrence to acceptable risk level. The Corrective Action may have been effective, but if it still poses a high degree of residual risk, then it wasn't effective. Risk is a good way to "double-check" a Corrective Action before it is completed.

4. **Risk Provides a Common Reporting Framework for the Enterprise:** Organizations are happy to be automating and streamlining their EHS processes, but if they cannot report on the data and affect change, then they've only completed half the journey. True Enterprise EHS systems provide valuable data, from the shop floor to the top floor. At the operational level, common EHS metrics are valuable, but at higher levels in the organization, it becomes meaningless jargon at some point. Executives speak Risk, plain and simple. They can effectively make decisions based on the top risks to the organization, and effect change based on this risk data. This is why ERM is such a valuable asset in an executive's toolbox. By translating EHS data into a common Risk element, EHS managers can effect change within their department by illustrating where the top risks are and drill-down from there. Risk reporting is becoming a universal method for interpreting data, and spans the enterprise.

Conclusion

For many organizations, Risk Management drives decision making. EHS Management Systems can benefit from implementing elements of Risk Management and Risk Assessment, to help streamline their operations, provide better decision-making capabilities, and to increase visibility to the enterprise.

Risk Assessment: Creating a Risk Matrix

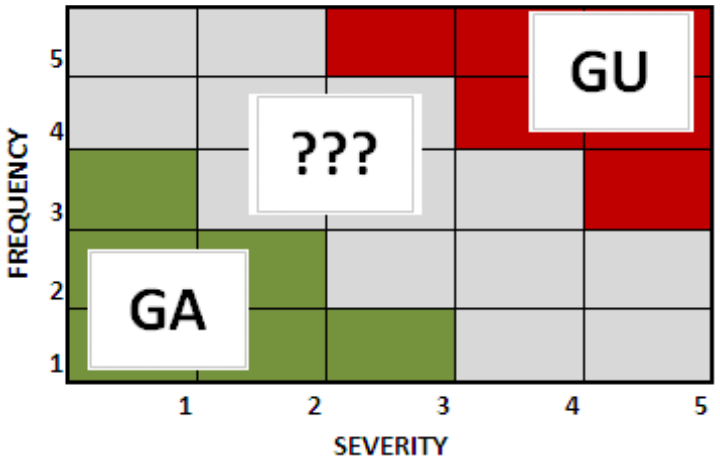
In this day and age, risk is the biggest buzzword in the compliance industry. We've talked about it, you can't go anywhere without hearing about it, and everyone's got a risk-based solution. I think the primary reason why we focus on Risk Assessment and Risk Management, is because in business, we need to quantify our actions. We can no longer rely purely on "gut instinct" to execute on events, whether Quality, Financial, Social, or similar areas. The world moves too fast, and one misstep can make or break your business. Risk provides the objective metric to help the decision-making process. But, you need to know how to use risk.

How do you define risk? It's not as easy as you may think. Companies spend plenty of time and money coming up with a scheme on how to calculate risk for their organization. Risk is defined as the "systematic application of policies, procedures, and practices to the tasks of analyzing, evaluating, and controlling risk." All this really means is that we put tools in place to help us look for risks, assess those risks, and then take action on the risk. The trick here is finding the risk, isn't it? How do we find the risk?

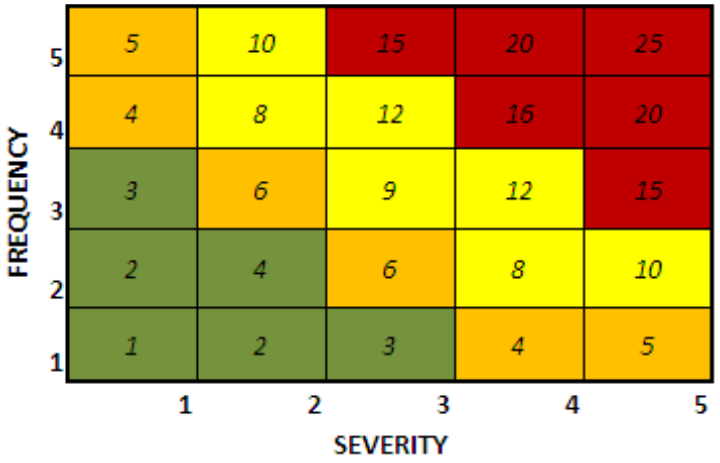
The components of risk usually manifest themselves in two forms: hazards or harms. Hazards represent the potential source of a harmful event (the cause). Harms are the resulting damages to products, persons, or the environment (the effect). Risk is essentially cause and effect on a defined scale. It's the scale in which most struggle.

Usually, when trying to quantify hazards and harms, most organizations look at two metrics: Severity and Frequency (or likelihood). Taking these metrics into account, we can develop a scale in which to measure hazards and their harms. This can be numeric (scale of 1-5), verbal (excellent to poor) or both. If you were to graph these scales, you would come up with a numerical matrix, one that highlights the risk "zones" by their multiplied number on the axis, much like this one below:

You can see that we have a Low-Risk or Generally Acceptable Risk zone, and a High-Risk or Generally Unacceptable Risk zone, but what about the middle? There's a gray area of subjectivity here. How do companies determine this gray area?



This is not always an easy answer. Some companies have to weigh the costs versus benefits on these risks, without creating a disproportionate cost to risk (Example: spending $1M to prevent a blister is disproportionate; spending $1M to prevent a fatality is proportionate). Companies will carefully vet these zone, and typically adopt a concept called ALARP (As Low as Reasonably Practicable). Simply put, this means that the risk is as low as we can possibly get it, or it's "Tolerable" or "Undesirable"—but it isn't critical or catastrophic. So then, with the ALARP in place, you have a risk matrix:



Now you can go off and start using it, right? Well...you need to "vet the matrix"—put it through real-world historical examples and see if the risk matrix comes up with the correct risk based on historical events. You may need to "tweak" the matrix based on the vetting

process. Hard mathematics will not properly assess the risk without a little real-world honing. Once you've fine-tuned the matrix, you can start utilizing it in your Compliance system.

Risk Assessments and risk matrices are wonderful tools to help guide decision-making in an organization, but they are not meant to be stand-alone tools. They help to provide a guide for Risk Assessment, using quantitative and repeatable metrics to ensure a consistent method of determining risk. Most best-in-class organizations will assemble a "risk team" to go over adverse events and determine the risk. It's up to the team to decide how an event will be handled, and what the true risk is. Risk matrices are the keys to unlocking quantitative risk-based processes, but the people are the drivers of the system.

The next question becomes, "How do I incorporate Risk into my Quality Management System?" More specifically, how can Risk ease the bottlenecks in an organization's Corrective Action process?

Too often, when adverse events enter an organization's Quality system, people are quick to open up a Corrective and Preventive Action (CAPA). No matter what the adverse event, its severity or impact, a CAPA is opened up. Having a CAPA system in place is an extremely valuable (and essential) part of a good QMS. However, if everything becomes a CAPA, then you create a bottleneck. Employees are so focused on working on their CAPAs, they forget to do anything else.

What you end up with is this—hundreds of CAPAs, without really knowing which CAPAs are critical to the business and which have less impact. It becomes the needle in the haystack conundrum—finding the critical adverse events can prove difficult if you don't have a way of finding them. I once asked a Quality Manager how he handles CAPAs—what his metric was. "We handle the most overdue first," was his reply, and he went on to say that if it isn't critical and is at the "bottom of the pile," then they don't get to it in time. That said, there is a better way.

1. **Not every event needs to be a CAPA:** Yes, it's true—if you can immediately correct an event, then correct it. Not every event needs to be opened up as a Corrective Action, only those that are systemic issues and pose a critical impact on the business.

2. **Use Risk to filter events:** So if not every event needs to be a CAPA, then how do we figure out the bad the from not-so-bad? You need a way to filter these events, and you need to do it in a repeatable, systematic method. Risk Assessment is a great way to do this. Risk matrices will help your team make the determination as to the criticality of an event. The higher the risk, the more likely we would like to take Corrective Action.

3. **Do a CAPA on your CAPA System:** Sometimes even a good CAPA process needs a little updating. Make sure to continually audit the CAPA process, and if the process is not efficient enough, then it may be time to do a CAPA to correct any potential bottlenecks or problems within. Like any good process, a little maintenance and "trimming" is always healthy.

4. **Use Risk to Ensure Effectiveness:** For an action to be truly corrective to the process, it must be effective, otherwise you're back to square one. Much like risk can be used to filter adverse events, risk can also be used to ensure effectiveness of a CAPA. Risk helps to ensure that not only is the CAPA effective, but it's within the risk limits of your organization's compliance standards.

Conclusion

CAPA is an effective and essential tool but, like many processes, can be blocked up if you are too reactive to events. In order to streamline your CAPA process, it is important to look at adverse events and filter them to properly determine how critical they are.

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