a white paper from

NSF-ISR

Risk-Based Thinking

ISO 9001:2015 – Not as Difficult as You May Think

With the introduction of ISO 9001:2015, **risk-based thinking** has become a "new" compliance requirement. However, this significant change to the previous version of the standard is actually *not so new at all*. The 2008 version of ISO 9001 required organizations to gather and analyze data from their processes to continually improve upon them, and to implement actions to prevent recurrence of nonconformities. Taken a step further, data analysis was also required to prevent the occurrence of potential nonconformities from happening in the first place.

Many organizations may be struggling with the concept of risk-based thinking and which approach, or approaches, are best. They may also be struggling with what risks auditors will be looking for them to address. One simple approach may be for top management to stop and consider the things that keep them awake at night, and the things that are most sensitive in terms of the overall operation of the company. Let's consider a few of them:

- Cost of materials
- Cost of labor
- Cost of operating equipment (e.g. maintenance, depreciation, etc.)
- Cost of utilities
- Cost of poor quality (e.g. scrap)

There are many more to consider, but the overall theme is that all of them have a cost associated to them. Additionally, if left untreated, all of them can have a negative impact on the Quality Management System (QMS).

An organization's top management should take credit for the fact that they may have been using risk-based thinking for years, albeit not included within their QMS. Now, the standard is requiring organizations to formalize the process of identifying the risks associated with operating the business and the QMS while:

I. Showing the actions taken to mitigate the risks to avoid costs
II. Minimizing the impact of risks
III. Ultimately improving the QMS and the organization

The approaches to demonstrating risk-based thinking in the QMS will likely be as unique and varied as the organizations seeking registration to ISO 9001:2015, however, there are some fundamental elements of the process that should be common:

- Identification of the risks
- Analysis of the risks and their impact on the QMS (or organization itself)
- Qualifying or quantifying risks in order to prioritize
- Determination of actions to mitigate risks
- Implementation of actions to mitigate risks
- Analysis of the results of actions taken

For example, many organizations rely on internet access to properly operate their business. Poor internet service (i.e., unstable connections, low bandwidth, etc.) may present a risk to organizations relying on the interchange of information via on-line systems, applications and emails, especially where use of customer on-line systems are mandated. Here, we can safely assume in our example that this may be a high priority risk.

The good news is that an organization's top management, or the staff that they have deemed responsible for the selection of an internet service provider (ISP), has probably done an informal analysis of the risk prior to making the selection of the ISP. In order to mitigate the risk, organizations will likely review the offerings of several ISPs (where available) before making a choice, and consider different aspects of the ISP's services (cost, bandwidth, user ratings, etc.). The actual review and selection process could be considered actions to mitigate the potential risk, and monitoring the performance of the ISP over time could be consider an analysis of the action taken (i.e. satisfaction with the ISP as it related to operation of the business).

Taking the above example a little further, some organizations may be so reliant on internet access that outages would essentially shut them down. This may be identified as a new risk, or treated as its own separate issue. Mitigating this risk should be analyzed, prioritized, and actions taken in accordance with the priority.

In some cases it may be necessary to have redundant systems, or another service in standby mode should the selected ISP lose connectivity.

To complete the example of risks associated with internet access, organizations are encouraged to consider all facets of the risks they have identified. What are other risks that present themselves related to internet service?

- Employee usage on their own devices (mobile phones, tablets, etc.)
- Misuse of the organization's internet (Social media, streaming, etc.)
- Downloading and use of pirated software (for business or personal use)
- Other use or misuse that would reduce the internet service ability to support the QMS and business processes
- Other use or misuse that could damage the company's reputation

In conclusion, there are many risks to an organization's QMS that are considered and dealt with every day by Top Management. ISO 9001:2015 now requires that the identification, review, mitigation and analysis be formalized in order to demonstrate compliance with the various clauses in the Standard that refer to risks. Organizations' Top Management is encouraged to take a leadership role in making the entire organization sensitive to risk, communicating them, and reducing or eliminating the potential impact these risks have on the overall organization, and the successful operation of the QMS.