The importance of risk in quality management

Whitepaper

bsi.

...making excellence a habit.™

Background and overview to the **ISO 9001:2015** revision

As an International Standard, ISO 9001 is subject to review on a regular basis. When considering the 2015 revision, the committee responsible decided that change was necessary in order to:

- Adapt to a changing world
- Enhance an organization's ability to satisfy its customers
- Provide greater focus on the customer
- Provide a consistent foundation for the future
- Reflect the increasingly complex environments in which organizations operate
- Ensure the new standard reflects the needs of all interested parties

The research that was carried out as part of the review process recognized that several other important changes were required since the last major change in 2000. These were:

- Providing a foundation for the integration with other management systems
- Introducing risk-based thinking, now prevalent in many organizations
- Aligning the QMS policy and objectives with the strategy of an organization
- Providing greater flexibility with documentation

To facilitate the integration of management system standards by users, a new common format has been developed by ISO to use in all management system standards. This is known as Annex SL or the High Level Structure and provides a standardized core text and structure for all ISO management system standards.

The structure of Annex SL and therefore all ISO management system standards in the future is:

Clause 1	Scope
Clause 2	Normative references
Clause 3	Terms and definitions
Clause 4	Context of the organization
Clause 5	Leadership
Clause 6	Planning
Clause 7	Support
Clause 8	Operation
Clause 9	Performance evaluation
Clause 10	Improvement

The fundamental objective of ISO 9001 however remains the same, which is to provide confidence in the organization's ability to consistently provide customers with conforming goods and services, and to enhance customer satisfaction.

Why is managing risk important in a quality management system?

Risk-based thinking is something we all do automatically and often sub-consciously to get the best result. The concept of risk has always been implicit in ISO 9001 – this revision makes it more explicit and builds it into the whole management system.

- Risk-based thinking ensures risk is considered from the beginning and throughout the process approach
- Risk-based thinking makes proactive action part of strategic planning
- Risk is often thought of only in the negative sense. Risk-based thinking can also help to identify opportunities. This can be considered to be the positive side of risk.

One of the key changes in the 2015 revision of ISO 9001 is to establish a systematic approach to risk, rather than treating it as a single component of a quality management system.

In previous editions of ISO 9001, a clause on preventive action was separated from the whole. Now risk is considered and included throughout the standard.

By taking a risk-based approach, an organization becomes proactive rather than purely reactive, preventing or reducing undesired effects and promoting continual improvement.

For all types of organizations, there is a need to understand the risks being taken when seeking to achieve objectives and attain the desired level of reward. Organizations need to understand the overall level of risk embedded within their processes and activities. The concept of "risk" in the context of ISO 9001 relates to the uncertainty of achieving the objectives of the system, which is to provide products and services that conform to customers' requirements. By understanding those risks and exploring ways in which the risks can be mitigated, the organization will also have an opportunity to drive change and improvement.

Also remember that as Annex SL is the framework for all ISO management system standards, "risk" will be a common theme across them all. In this context it may be worth considering taking an enterprise-wide approach to Risk Management to assist future integration.

How is risk being incorporated into the new **ISO 9001:2015** standard?

In the Introduction the concept of risk-based thinking is explained.

In **Clause 4** the organization is required to determine the risks which can affect its ability to meet the system objectives. It recognizes that the consequences of risk are not the same for all organizations. For some, the consequences of delivering a non-conforming product are minor; for others the consequence can be fatal. So risk-based thinking means considering risk quantitatively as well as qualitatively, depending on the business context.

In **Clause 5** top management is required to demonstrate leadership and commit to ensuring that risks and opportunities that can affect the conformity of a product or service are determined and addressed.

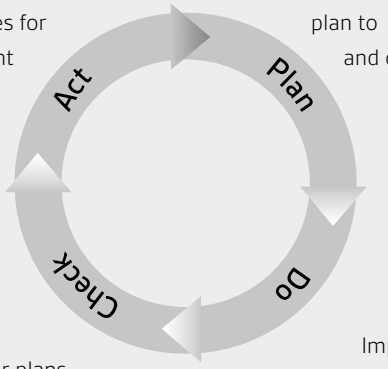
In **Clause 6** the organization is required to take action to identify risks and opportunities, and plan how to address the identified risks and opportunities.

Clause 8 looks at operational planning and control. The organization is required to plan, implement and control its processes to address the actions identified in Clause 6.

In **Clause 9** the organization is required to monitor, measure, analyze and evaluate the risks and opportunities.

In **Clause 10** the organization is required to improve by responding to changes in risk.

So in effect we have the PDCA (Plan, Do, Check, Act) cycle applied to risk.



Act

Implement changes to your approach and continually review opportunities for improvement

Plan

Gain leadership commitment. Identify and assess risks. Create plan to address risks and opportunities

Check

Monitor your plans through measurents, internal audit and reporting

Do

Implement your plan to mitigate risks., through communication, training and controls

What are the benefits?

The outputs from successful risk management include compliance, assurance and enhanced decision-making. These outputs will provide benefits by way of improvements in the efficiency of operations, effectiveness of tactics (change projects) and the efficacy of the strategy of the organization.

By considering risk throughout the organization, the likelihood of achieving the stated objectives is improved, output is more consistent and customers can be confident that they will receive the expected product or service.

Risk-based thinking therefore:

- Establishes a proactive culture of improvement
- Assures consistency of quality of goods or services
- Improves customer confidence and satisfaction
- Builds a strong knowledge base
- Proactively improves operational efficiency and governance
- Builds stakeholder confidence in the use of risk techniques
- Enables organizations to apply management system controls to analyze risk and minimize losses
- Improves management system performance and resilience
- Enables organizations to respond to change effectively and protect their business as they grow

What does this mean for organizations and how can they prepare?

For many organizations this will be business as usual. But if it's not, they'll need to start using a risk-driven approach in their organizational processes:

Identify the risks and opportunities – This will of course depend on the context of an organization and its appetite for taking risks.

Analyze and prioritize risks and opportunities. What is acceptable, what is unacceptable? What advantages or disadvantages are there to one process over another?

Plan actions to address the risks. How can risk be avoided or eliminated? How can risks be mitigated?

Implement the plan. Take the necessary actions.

Check the effectiveness of the actions. Does it work? Audit the approach, learn from experience, continually improve and also continue to consider innovative opportunities.

Reasons to consider **ISO 31000**

ISO 9001:2015 does not require a formal risk assessment or a specific single document. The information must be kept and available, and could be electronic, audio, video, written or any other type of media.

ISO 31000 (Risk management: Principles and guidelines) may be a useful reference for organizations looking for a more formal enterprise-wide risk process, but it's not obligatory.

Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty.

ISO 31000 provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment.

ISO 31000 gives a useful list on how to deal with risk:

- Avoiding risk by deciding not to start or continue with the activity that gives rise to the risk
- Accepting or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed decision

Using the right solution to manage risk

Companies are constantly looking for solutions that can improve business, enhance their operations, and optimize business performance. In today's market, success hinges on developing competitive advantage and profitability while demonstrating good corporate governance. Carefully calculating risk, going beyond the expected, and creating an environment for innovation are what generate the excellence needed to create that edge.

Experience teaches that the more successful businesses imbed best practice holistically across the entire organization, not just in one specific area. Instituting an enterprise-wide strategy breaks down long established silos separating departments and divisions, and, for many organizations, can represent a significant change in corporate culture.

Initiating such culture change can be a challenge. An effective and successful transition requires a bold, well-planned, demonstrable commitment to enhance systems and critical processes that drive long-term sustainable performance and create a gateway to excellence. Organizations must ensure that institutional knowledge is captured, analyzed, managed, and improved upon so that they can be best in class. Businesses need tools that drive continual business improvement, delivering real-time visibility and providing a consistent framework for automation. Purpose-built software provides your risk team with a complete view that is shared among auditors, managers, and executives in real-time so more effective collaboration can occur on issues that pose risk to the business.

Conclusion

- Risk-based thinking is not new
- Risk-based thinking is something you do already
- Risk-based thinking is continuous
- Risk-based thinking ensures greater knowledge and preparedness
- Risk-based thinking increases the probability of reaching objectives
- Risk-based thinking reduces the probability of poor results
- Risk-based thinking makes prevention a habit

Why BSI?

At BSI we create excellence by driving the success of our clients through standards. We enable others to perform better, manage risk and achieve sustainable growth.

For over a century our experts have been challenging mediocrity and complacency to help embed excellence into the way people and products work. We make excellence a habit.

Our products and services

We provide a unique combination of complementary products and services, managed through our three business streams: Knowledge, Assurance and Compliance.

Knowledge

BSI works with business experts, government bodies, trade associations and consumer groups to capture best practice and structure the knowledge all organizations need to succeed. The majority of the widely used and implemented international standards were originally shaped by BSI, for example ISO 9001 Quality Management and ISO/IEC 27001 for Information Security.

Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We help our clients understand how they are performing, thereby identifying areas of improvement from within.

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a standard so that it becomes an embedded habit. We train our clients to understand standards and how to implement them, as well as provide added value and differentiated management tools to facilitate the process of ongoing compliance.

To find out more visit: **bsigroup.com**

bsi.

bsigroup.com