International Organization for Standardization

International Accreditation Forum

Date: 13 January 2016

Auditing Practices Group Guidance on:

Risk Based Thinking

Risk has been always implicit and addressed in ISO 9001. Many of its requirements, are aimed to prevent risks, therefore risk and ISO 9001 is not a new combination. Previous editions of ISO 9001 included a clause on preventive action, which aimed to prevent the occurrence of nonconformities.

ISO 9001 specifies requirements for the organization to understand its context and determine risks as a basis for planning. Risk based thinking considers both risks and opportunities.

The Introduction and Annex A of ISO 9001:2015 provide an explanation on risk based thinking, including clarification on risk and opportunity concepts. More comprehensive information can be found in Risk based thinking paper at www.iso.org/tc176/sc02/public.

An audit of risk-based thinking in an organization cannot be performed as a stand-alone activity. It should be implicit during the entire audit of a QMS, including when interviewing top management. An auditor should act in accordance with the following steps and collect objective evidence as follows:

- What inputs are used by the organization for risk and opportunity determination? These inputs should include the following:
  - ✓ analysis of external and internal issues
  - ✓ the strategic direction of the organization.
  - ✓ interested parties, related to its QMS, and their requirements, also related to the QMS.
  - ✓ the scope of QMS of the organization.
  - ✓ the processes of the organization.

- The auditor should note that the organization has to determine the extent of documented information needed to provide objective evidence of the application of risk based thinking. There is no specific requirement in ISO 9001:2015 on how to document the results of determinations of risks and opportunities.

- An organization's needs for, and the extent and type of, documented information will vary greatly due to the context of the organization, its size, culture, nature of products and services, applicable statutory and regulatory requirements, or customer requirements regarding the risks on products, etc.

- How can an organization determine its risks and opportunities, while considering the above? Objective evidence could be in various forms, for example:
  - ✓ Meeting minutes
  - ✓ SWOT analysis
  - ✓ Reports on customer feedback.
  - ✓ Brain-storming activities
  - ✓ Competitor analysis.
  - ✓ Planning, analysis and evaluation activities related to several processes, e.g. strategic planning, design and development, marketing, production and service provision, corrective actions, …
  - ✓ Management review
  - ✓ Risk determination or evaluation records, if determined applicable or needed by the organization,
  - ✓ etc.

- How can an organization address its determined risks and opportunities? The actions needed to be taken can be in different forms, for example:
  - ✓ The revision of old, or the setting of new, objectives.
  - ✓ Action plans.
  - ✓ On the job training
  - ✓ Work instructions
  - ✓ Improvement targets and projects, etc.

- Does the organization evaluate the effectiveness of above mentioned actions? The auditor should confirm if internal audits and performance evaluation activities take into account the effective application of risk based thinking.

For further information on the ISO 9001 Auditing Practices Group, please refer to the paper:
Introduction to the ISO 9001 Auditing Practices Group

Feedback from users will be used by the *ISO 9001 Auditing Practices Group* to determine whether additional guidance documents should be developed, or if these current ones should be revised.

Comments on the papers or presentations can be sent to the following email address: charles.corrie@bsigoup.com.

The other ISO 9001 Auditing Practices Group papers and presentations may be downloaded from the web sites:

www.iaf.nu

www.iso.org/tc176/ISO9001AuditingPracticesGroup

Disclaimer

This paper has not been subject to an endorsement process by the International Organization for Standardization (ISO), ISO Technical Committee 176, or the International Accreditation Forum (IAF).

The information contained within it is available for educational and communication purposes. The *ISO 9001 Auditing Practices Group* does not take responsibility for any errors, omissions or other liabilities that may arise from the provision or subsequent use of such information.