



## **RISK MANAGEMENT IN ISO 9000 SERIES STANDARDS**

***Evgeny Avanesov***

Working Party on Regulatory Cooperation and Standardization Policies  
ECONOMIC COMMISSION FOR EUROPE

Groupe de travail des politiques de coopération en matière de réglementation et de  
normalisation  
COMMISSION ÉCONOMIQUE POUR L'EUROPE

Рабочая группа по политике в области стандартизации и сотрудничества по вопросам  
нормативного регулирования  
ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ

*The papers carry the names of the authors and should be cited accordingly. The findings, interpretations, and conclusions expressed in this paper are entirely those of the authors. They do not necessarily represent the views of the United Nations, or those of the governments they represent.*

© The Authors.

*All rights reserved. No part of this paper may be reproduced without the permission of the authors.*

# RISK MANAGEMENT IN ISO 9000 SERIES STANDARDS

*Evgeny Avanesov*

D.B.A., Member of

Russian delegation in

ISO/TC 176, ISO/TC 207

## Introduction

The international community has developed a number of documents in some way related to the standardization of approaches to risk management. The International Organization for Standardization (ISO), together with the International Electrotechnical Commission (IEC) are the lead organizations in the development of international standards. Some national standardization bodies and non-governmental organizations also have contributed to the development and use of standardized approaches to risk management.

### **The most important national and international standards for the risk management**

<b>Producer</b>	<b>Name</b>
<b>ISO/IEC</b>	ISO/FDIS 31000:2009 Risk management -- Principles and guidelines
	ISO/IEC Guide 73:2002 Risk Management — Vocabulary — Guidelines for use in standards
	ISO/IEC Guide 51:1999 Safety aspects — Guidelines for their inclusion in standards
	ISO 14971:2000 Medical devices — Application of risk management to medical devices
	ISO 17776:2000 Petroleum and natural gas industries — Offshore production installation — Guidelines on tools and techniques for hazard identification and risk assessment
<b>CSA</b>	CSA Q 850:1997 Risk Management Guidelines for Decision Makers

<b>JSA</b>	JIS Q 2001:2001 Guidelines for development and implementation of risk management system
<b>AS/NZS</b>	AS/NZS 4360:2004 Risk management
<b>BSI</b>	PAS 56:2003 Guide to Business Continuity
	BS 31100:2008 Code of practice for risk management
	BS 6079-3 Project Management - Part3: Guide to the management of business related project risk
	PD6668 Managing Risk for Corporate Governance
<b>ÖN</b>	ONR 49000 Risk management for organizations and systems — Terms and principles
	ONR 49001 Risk management for organizations and systems — Elements of the risk management systems
	ONR 49002-1 Risk management for organizations and systems — Part 1: Guidelines for risk management
	ONR 49002-2 Risk management for organizations and systems — Part 2: Guidelines for the integration of risk management into the general management system
	ONR 49003 Risk management for organizations and systems
	ONORM S 2300 Risk, security and crisis management — Concepts
	ONORM S 2310 Risk, security and crisis management — Selection and verification criteria for persons appointed for crisis management

There is also a document issued by the Institute of Risk Management (IRM), Association of Insurance and Risk Managers (AIRMIC) - A Risk Management Standard (2002).

This is an incomplete list, and I apologize if some of the other papers on this topic are not pointed out.

A little bit of focus on two documents:

The efforts of ISO and IEC has led to appearance of ISO/IEC Guide 73:2002 Risk management - Vocabulary-guidelines for use in standards. This paper aims to provide members of ISO and IEC, government and non-governmental organizations involved in standardization at the international, regional and national levels, a set of basic definitions and terminology relating to risk management. The need for a particular guidance document on the use of ideology and technology of risk management within the framework of standards has been recognized some time ago, based on the fact that many of the technical committees and working groups, ISO or IEC address the issue of risk management in different manner. And, Guide 73, finally, provides a general framework for incorporating risk management in international standards.

However, despite the availability of terminology document ISO/IEC Guide 73:2002, a synthesis ISO standard that ensures a consistent approach to risk management, is still lacking. This can lead to confusion among users of documents relating to the interpretation and practical application. The global economic situation, the practice of the business community in this area pushed ISO to expedite finalization of the international standard for risk management. I say about the forthcoming ISO 31000:2009 Risk management -- Principles and guidelines.

As can be seen from the Draft, the new standard will provide vision, guidance, and generic iterative process of risk management in organizations of any size. The standard is designed to be a document higher level, to ensure support for existing standards. Therefore, ISO 31000:2009 is not specific to any industry or sector. ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences. Although ISO 31000:2009 provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. An important thing that ISO 31000:2009 is not intended for the purpose of certification.

But what about the risk management theme in other generic management system standards?

### **The reflection of the risk management standards for management systems**

I think that is not necessary to talk specifically about the importance of the ISO 9000 series for the business community. This is the most popular product of the ISO using by more than one million companies worldwide.

Using the process approach, which is proposed by standard ISO 9001:2008, for its activities, organizations are striving to meet the needs and expectations of both internal and external customers. Quality management is no

longer the exclusive preserve of manufacturing companies, process approach has proven as an invaluable tool for service organizations, local authorities, health organizations, finance and transport. An additional benefit of working with ISO 9001: 2008 is the fact that the standard requires to improve the processes operating in the organization.

Traditionally, the Quality management system (QMS) is developed as follows. The basis for the development of QMS is some purpose of organization or its mission. How it can be formed - is not specified in the standard. Then they establish a Quality Policy of organization, which is deployed to objectives. All system is built on this framework to for the aim of fulfilling objectives. Risk management has no place in this scheme.

However, the risk approach method is an integral part of other generic management systems standards: Environmental Management Standard ISO 14001 and the Occupational Health & Safety Assessment Standard OHSAS 18001. Organizations should identify and assess each of the risks they've been faced. Infrequent risks with minor effects are shall be only controlled. Significant risks with severe consequences should be managed in such a way as to either completely eliminate them or reduce the frequency of their occurrence and severity of consequences.

Organizations that have successfully applied the ISO 14001 standards, conducting ongoing analysis of the environmental management system, an integral part of which is the consideration of significant environmental aspects associated with air emissions, discharges into water, waste disposal, ground pollution, use of raw materials and natural resources and other environmental problems . The style of thinking and behavior of such organizations usually meets the expectations of stakeholders: risk management and prevention of losses related to the environment.

Organizations that successfully use OHSAS 18001, identify hazards and carry out an assessment of the risks associated with routine activities, as well as the risk of presence of sub-contractors and visitors on the site. The key stakeholders are the people inside the organization, which creates a culture of risk management.

It is a pity that risk management approach has not yet become one of the cornerstones of ISO 9001.

The objective of business is to integrate this good practice and to apply it more broadly, including quality management. In fact, along with the application process approach, it is obvious to use the same risk assessment process applied to the objects such as market trends, strategic directions of business development expertise, operational activities, consumer satisfaction with

products and services. As a result of these two approaches, the organization may pay more attention to the needs and expectations of its customers and other stakeholders. They also are in a better position in terms of environmental management and concern for the health and safety in the workplace.

### **The ISO 9000 standards and risk management.**

The new version of ISO 9001 was issued at the end of 2008. For the first time the introduction explicitly emphasizes, that the development of a quality management system must take into account the environment in which the organization operates, changes in that environment, as well as risks associated with this environment.

Then it states that ISO 9001 does not contain requirements in relation to other types of management, in particular to environmental management, management of health and safety, financial management or risk management.

Indeed, in the ISO 9001 you will not find a specific reference to risk management (i.e. identification, analysis, evaluation, action on the reduction or deletion, etc.).

However, the analysis of ISO 9001 demonstrates that it indirectly refers to some situations of risk management.

### **Examples of the requirements of ISO 9001:2008, indirectly associated with the risk management**

<b>ISO 9001:2008 clauses</b>	<b>Comments</b>
<b>5.6. Management review</b>	Review should include an assessment of improvement opportunities and needs for changes in the quality management organization. One of the conditions of this review is to analyze changes that could affect the quality management system
<b>6.2 Human Resources</b>	By meeting the requirements to ensure the necessary competence, you can manage the risks associated with human resources.
<b>6.3 Infrastructure</b>	The provision and maintenance of infrastructure (i.e. buildings, equipment, information environment) needed to achieve conformity to product

	requirements, would manage the risks associated with the control of infrastructure
<b>7.2.2 Review of requirements related to the product</b>	The requirement to review contract prior to its signing, including determining the organization's ability to fulfill certain requirements, significantly reduces the risk of default on contractual obligations in the future
<b>7.3.7 Control of design and development changes</b>	It is necessary to evaluate the effect of the changes on constituent parts and product already delivered.
<b>7.4 Purchasing</b>	Definition of criteria for evaluating vendors and their systematic evaluation reduces risks of the vulnerability of organizations associated with the activity of suppliers and partners
<b>7.5. Production and service provision</b>	Provision of controlled conditions for production (i.e., availability of necessary information, instructions, equipment, measurement and testing, etc.) significantly reduces the risk of release of nonconforming products.
<b>8.2.1 Customer satisfaction</b>	Monitoring information relating to customer perception as to whether the organization has met their requirements is an important element for the identification of risks associated customer dissatisfaction, and hence the risk to the reputation / image of the organization and, consequently, declining market share
<b>8.2.2 Internal audit</b>	Internal audits help to identify operational risks
<b>8.5.3 Preventive action</b>	The organization shall determine actions to eliminate causes of potential non- conformances in order to prevent their occurrence, i.e. to conduct risk assessment.

There are far too many examples.

Risk management is more strongly suggested by the ISO 9004. Fully updated version of the standard under the working title « Managing for the sustained success of an organization — A quality management approach» is expected to be published in October - November 2009. The paper, which proposes ways to improve business performance, feels free to emphasize the need for risk management for the development and sustainability of the business in organization.

## Examples of the ISO/DIS 9004:2009 related to risk management

ISO/DIS 9004 clause	Content
<b>4.5 Sustained success</b>	An organization's environment will be always changing and uncertain; therefore, in order to achieve sustained success, it will be necessary for its management to constantly monitor and regularly analyze the organization's environment to identify potential risks
<b>5.2 Strategy and policy formulation</b>	The formulation of an organization's strategy should be based on analyses of demands, products, risks and opportunities
<b>5.3 Strategy and policy planning</b>	To give effect to its strategy and policies an organization seeking sustained success should establish and maintain processes that evaluate strategic risks
<b>6.1 Resource management.</b>  <b>General</b>	To ensure the availability of the resources for the future activities, the organization's management should identify and evaluate the risks of their potential scarcity
<b>6.4.2 Suppliers and partners – selection, evaluation and improvement of their capabilities</b>	In selecting and evaluating partners, and continually improving their capabilities, the organization's management should consider issues such as the risks connected with relationships with partners
<b>6.5 Infrastructure</b>	The organization's management should identify and assess the risks associated with its infrastructure and take action to mitigate the risks
<b>6.7 Knowledge, information and technology</b>	The organization's management should establish processes for assessing the evaluation of risks related to changes of technology
<b>6.8 Natural resources</b>	The organization's management should consider the risks and opportunities related to the availability and use of natural resources (such as water, oil, minerals and raw materials) in the short term, as well as in the long term
<b>7.2 Process planning</b>	In the organization's planning processes, consideration should be given to possible financial and other risks
<b>8.1 Monitoring, measurement, analysis</b>	To achieve sustained success in an ever changing and uncertain environment it is necessary for the

<b>and review. General</b>	organization's management to monitor and regularly analyze the organization's environment to identify potential risks
<b>8.3.1 Measurement. General</b>	The methods used for collecting information and data regarding key performance indicators should be practicable and appropriate to the organization (e.g. risk assessments and risk controls)
<b>8.3.2 Key performance indicators</b>	Specific information relating to risks, and opportunities should be considered when selecting the KPIs
<b>8.3.3 Internal audit</b>	Internal auditing can be an effective process for identifying problems, risks and nonconformities that are subsequently addressed through root cause analysis and the development and implementation of preventive and corrective action plans
<b>8.4 Analyzing</b>	The organization's management should analyze the organization's environment, identify risks and opportunities, and establish plans to manage them
<b>9.3 Innovation</b>	The organization's management should assess the risks accompanying the innovation activities and prepare preventive actions to avoid or minimize the risks, including contingency plans where necessary

## **Conclusion**

The 26 meeting of ISO/TC 176, which is known to be responsible for maintaining and updating the ISO 9000 series standards, took place in Tokyo on February this year. Particular attention of gathered professionals was attracted to a new group with the title «The concepts and ideas for the future revision of ISO 9001». The group has the following task: the brainstorming to identify common concepts and ideas that could form the basis for future activities ISO/TC 176 on the revision of ISO 9001. In the future, these ideas, together with the views of other stakeholders, such as: business, standardization, accreditation, certification bodies, and other technical committees of ISO, should be the basis for the design specification for the revision of ISO 9001. The first of the proposed concept has been designated as an opportunity and the need to integrate risk management into the standard ISO 9001. It was stated that there is a need to address the issue of a separate allocation of subjects at risk, and decide to which objects should be considered: production, organization, quality management system compliance with business continuity, supply chain management, resources and infrastructure.

Firstly, survey of standard users will be carried out. Then, we will see the routine standards development process adopted in the ISO. But before 2015 a new ISO 9001 is unlikely to be released.

Of course, all discussions about the future of ISO 9001 are very preliminary, but it is clear that the formal inclusion of risk management in this important document will meet the realities of nowadays and help organizations to:

- identify and analyze the risks associated with the market (customers, competitors, regulatory documents, suppliers);
- consider the risks inherent in QMS;
- legitimize the importance of implementing quality management system;
- facilitate communication with top management, operating risks and potential consequences of their occurrence for the organization;
- Improve decision-making process on priorities and activities;
- designate and utilize the resources needed for the QMS and the processes of production / service delivery;
- effectively manage the organizational processes (risks associated with processes to improve their coordination and tracking;
- improve operational activities;
- increase the confidence of the stakeholders, particularly customers and shareholders;
- better manage suppliers (solvency and ability to perform the contract, outsourcing);
- make the link with the financial sector
- involvement of personnel;
- improve compatibility with ISO 14001 and OHSAS 18001;
- become more flexible to implement improvements and innovations.

## **Literature**

1. ISO 9001:2008 **Quality management systems —Requirements**
2. ISO/FDIS 9004:2009 **Managing for the sustained success of an organization — A**

**quality management approach**

3. ISO/TC 176/SC 2/N 867 **Report of the ISO/TC 176/SC 2 /TG “Concepts and Ideas for a Future Revision of ISO 9001”**

4. ISO/TC 176/SC 2/N 852 **Paper from France, concerning the Future Revision of ISO 9001 and Risk Management**