

Milan Majernik – Jana Pankova Jurikova \*

---

## THEORETICAL-METHODOLOGICAL ASPECTS OF INTEGRATED RISK MANAGEMENT STANDARDIZATION

*The authors are submitting a system model for integrated risk management. Results and conclusions of the paper are based on analysis of development, current status and progressive trends in standardization and risk management aspects of quality, safety, environment etc. Originality of the solution lies “in an enclosure” of quality management systems, safety management system and environmental management system according to standards, under the ISO standard ISO 31000 in the Slovak version of the upcoming STN. Solution is based on the philosophy of a single audit of compliance for the accreditation of certification bodies – they will certify risk management system. First audit can be realized for the certification system and the second for implementation system. The prepared standard ISO 31000 would be certification’s standard.*

### 1. Introduction

Enterprising at European and worldwide globalized markets is now inconceivable without acceptance of ISO standards and EU regulations for environmental management, management aspects of quality, safety, social responsibility, but also others.

An increasing number of socially required and maintained management systems and the associated burden on their certification, respectively registration (especially auditing) is forcing organizations (businesses, CO, AO) to seek new approaches to assess their compliance with worldwide standards.

Many organizations (companies) are now separate implementation of management systems (quality, environment, safety, etc.) enormously burdened (rising costs, an excessive burden on employees and specific documentation and necessary training, the requirements of communication with stakeholders, internal and external audits, etc.). The question arises inevitably, how many separately implemented enterprise management systems is company still able to sustain. Separately maintained and developed if there are constantly emerging new requirements and specific ISO standards (e.g. 16949, 22000, 26000, etc.).

One way to solve these problems is the integration of management systems. But the problem is that for conformity in the IMS (while the internal, certificated, supervised, recertificated auditing) there is no standard among ISO standards covering requirements for sub-systems.

It turns out that such a solution could be based on approach to risk management application (a prepared group of standards

ISO 31000). Slovak Office of standards, metrology and testing (SOSMT) is preparing a basic version to ISO 31000 “Risk Management – Principles and Guidance” at present. This standard is not intended for certification such as the ISO 9000, 14000, 27000 and so on. This fact is in custody on the reported problems with auditing positive.

If you manage to modify the ISO 31000 into a Deming cycle of continuous improvement of risk management (quality, environmental, safety, social, project, investment ...) by including the requirements of sub-systems of course, their integrated auditing will be real.

The inspiration for such scientific routing solution is also the fact that within Slovak national accreditation services (SNAS) is now the Technical Committee of “Accreditation risk management” constituted and SOSTM prepares issue of the ISO 31000 “Risk Management”.

### 2. Integrated Enterprise Risk Management System

With the ever increasing demands on the current market and technical development it is very challenging to maintain, respectively manage quality of product at a level as the company requires. This management requires relatively high effort to adapt to new changes and understand that quality of product means the achievement of a lot of criteria in many areas, either environmental protection, health protection of workers or other criteria. [5] Management of various aspects represents the core of the current management system, which can be implemented within the organization by using appropriate standards (Fig. 1).

---

\* Milan Majernik, Jana Pankova Jurikova  
University of Central Europe in Skalica, Slovakia, E-mail: janajurikova@yahoo.com

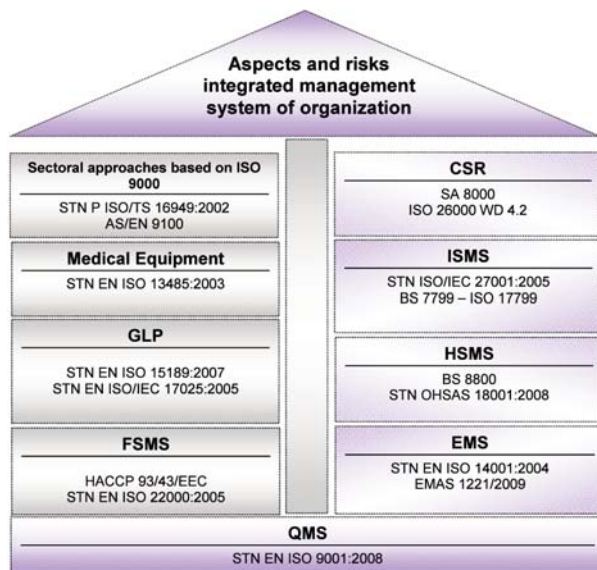


Fig. 1 Management systems in the organization

At present, generally the effort applies to put these related systems to a common basis - the modern management processes. Neither certified QMS nor certified EMS lead to high productivity and competitiveness if they are treated as isolated systems. The current trend is thus clearly intended to “comprehensive business integration”, where the other business subsystems access to the most frequently constructed systems without which it is impossible to ensure the competitiveness of the organization.

In terms of method and procedure it is significant to focus on the Deming cycle of continuous improvement. It also appears that the change in behavior (improvement) is impossible without changes in thinking and attitudes of all stakeholders in the management system.

The problematic area of integration of management systems (and the fact that there are still many new appearing) remains an area of “authorization” (accreditation, certification) and related audits in compliance with relevant standards (ISO 9000, 14000, 27000, OHSAS 18000...).

In this context there is no doubt that further development should be directed not only to implementation of integrated management systems (IMS), but also to integrated (single) auditing for various types of audits (pre-certificated, certificated, inspected, supervised, internal).

### 3. Authorization of an integrated risk management

The processes of accreditation and certification are an inherent part of implementation, maintenance and authorization management systems.

Methodical guidelines developed by SNAS for accreditation of management systems have undergone fairly significant changes

and do not always have such a form that could be used only one methodical guideline for accreditation of certifying an integrated system of risk management.

SNAS accredited bodies certifying quality management systems, quality assurance systems in accordance with NATO requirements, quality management systems for welding, systems of sustainable forest management, quality management systems for medical devices, environmental management systems, management systems and safety health, safety management systems and information management systems, food safety, on the basis of methodical guideline for accreditation of certification bodies certifying management systems. This methodical guideline is not usable for integrated risk management system too.

New, original idea is that SNAS will proceed based on only one methodical guideline during the accreditation process. This guideline will become usable in the accreditation process of bodies certifying risk management system. (Fig. 2). The basis of the risk management becomes risk register. It would solve significant aspects of organization.

Deeper analysis of processes shows the authorization process for consistency with respect to demonstrating compliance with relevant ISO standards (9000, 14000, 27000, 18000) to the sequence of steps and time limits and frequency of audits. The problem can be in terms of audits of separate implementation of individual management systems (Surveillance, control, internal and re-certificated). The advantage of risk management system from this point of view is the single audit of management partial aspects in accordance with relevant standards, broader audit team CO.

All of the requirements for risk management system certification, that the organization must ensure, are defined in the prepared standard ISO 31000 “Risk Management - Principles and Guidance”

### 4. Risk management systems in the enterprise

Risk management has a very important role in many business areas. It is now understood as a systemic and comprehensive tool to manage all processes of risk assessment. The base is to document policy as a management liability. It must correspond to strategic areas, goals and business character of organization. [13]

Risk management is a term that implies a logical and systematic method for determining the context, identification, analysis, evaluation, treatment, monitoring and communicating risks associated with any activity, function or process. It also deals with the identification of opportunities, as well as reduction of loss.

The basic requirements of risk management are: [11]

- definition of risk management policies (define, document commitment and goal setting - focusing on the character of the business),

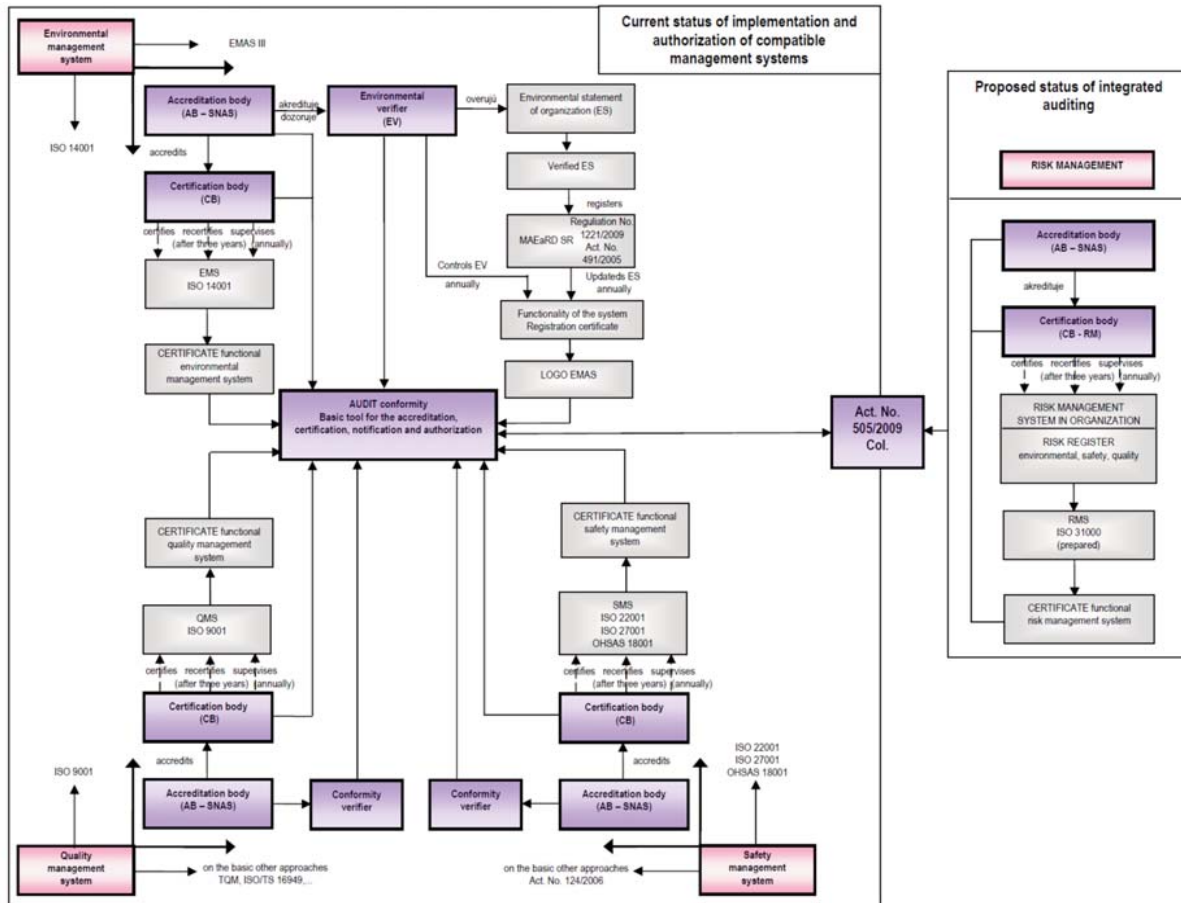


Fig. 2 Relationships in the process of accreditation, certification and authorization of management systems

- planning and provision of resources (developing, implementing and maintaining a system of risk management in accordance with this standard, the assessment of performance management and review of the organization as a basis for improvement),
- responsibility and authority,
- resources,
- program implementation,
- management review.

As currently prepared standard is not intended to encourage risk management, we must take into account the changing needs of a particular organization, its particular goals, structure, operations, processes, functions and products. It is assumed that the standard can be used in the harmonization of risk management practices within existing standards.

The goal of risk management is, therefore, the reduction of various kinds of risks relating to the matter at a socially acceptable level. It can be the amount of risk whose source may be the environment, technology, human, organization and others. Risk management will solve integrated risk assessment process and also the integrated process of accreditation and certification in the future.

**4.1. Framework of STN ISO 31000**

**4 Framework for managing risk**

- 4.1 General
- 4.2 Mandate and commitment
- 4.3 Design of framework for managing risk
  - 4.3.1 Understanding the organization and its context
  - 4.3.2 Risk management policy
  - 4.3.3 Accountability
  - 4.3.4 Integration into organizational processes
  - 4.3.5 Resources
  - 4.3.6 Establishing internal communication and reporting mechanisms
  - 4.3.7 Establishing external communication and reporting mechanisms
- 4.4 Implementing risk management
  - 4.4.1 Implementing the framework for managing risk
  - 4.4.2 Implementing the risk management process
- 4.5 Monitoring and review of the framework
- 4.6 Continual improvement of the framework
- 5 Process for managing risk**
  - 5.1 General
  - 5.2 Communication and consultation

- 5.3 Establishing the context
  - 5.3.1 General
  - 5.3.2 Establishing the external context
  - 5.3.3 Establishing the internal context
  - 5.3.4 Establishing the context of the risk management process
  - 5.3.5 Developing risk criteria
- 5.4 Risk assessment
  - 5.4.1 General
  - 5.4.2 Risk identification
  - 5.4.3 Risk analysis
  - 5.4.4 Risk evaluation
- 5.5 Risk treatment
  - 5.5.1 General
  - 5.5.2 Selection of risk treatment options
  - 5.5.3 Preparing and implementing risk treatment plans
- 5.6 Monitoring and review
- 5.7 Recording and improvement the risk management process

**4.2. Transformation of the key elements of risk management system according to ISO 31000 to the Deming cycle**

Common methodical tool of implementation, maintenance and assessment of management systems of partial aspects (quality, environment, security, information security, etc.) and integrated management system is the Deming cycle of continuous improvement (PDCA - plan - do - check - improve).

The prepared standard can be used as a substitute for ISO standards for partial aspects, if the structure and processes for risk management are united with these standards.

There are key elements of risk management system assigned (Fig. 3) according to the forthcoming ISO 31000 in each stage of Deming cycle of continuous improvement.

**5. Conclusion**

Standardization of various aspects of management processes also places increased demands on the auditing process for accreditation (CO, environmental verifiers), certification of management systems (quality, environment, security) and the mandatory internal audits within the implemented management system.

IMS accreditation process must be based not only on the experience and knowledge of practice, but must rely primarily on the results of scientific research studies, the results of forecasting the development (a process of accreditation and environmental management) and the European and global progress in these areas.

Properly analyzed the structure of the upcoming structure of process standardization of risk management of organization in general, ISO 31000, refers to the fact that from the structure's point of view and also the process of implementation there are no significant differences from the standards for the management of partial aspects (Quality - ISO 9000, Environment - ISO 14000, Safety - OHSAS 18000, etc.). It seems that the organization could use (and many even did) the implemented standards, address the issue of risk management. A fundamental question then is whether the forthcoming standard will not just be another "duplicate" in the IMS standards organization, also causing the indicated problems with auditing.

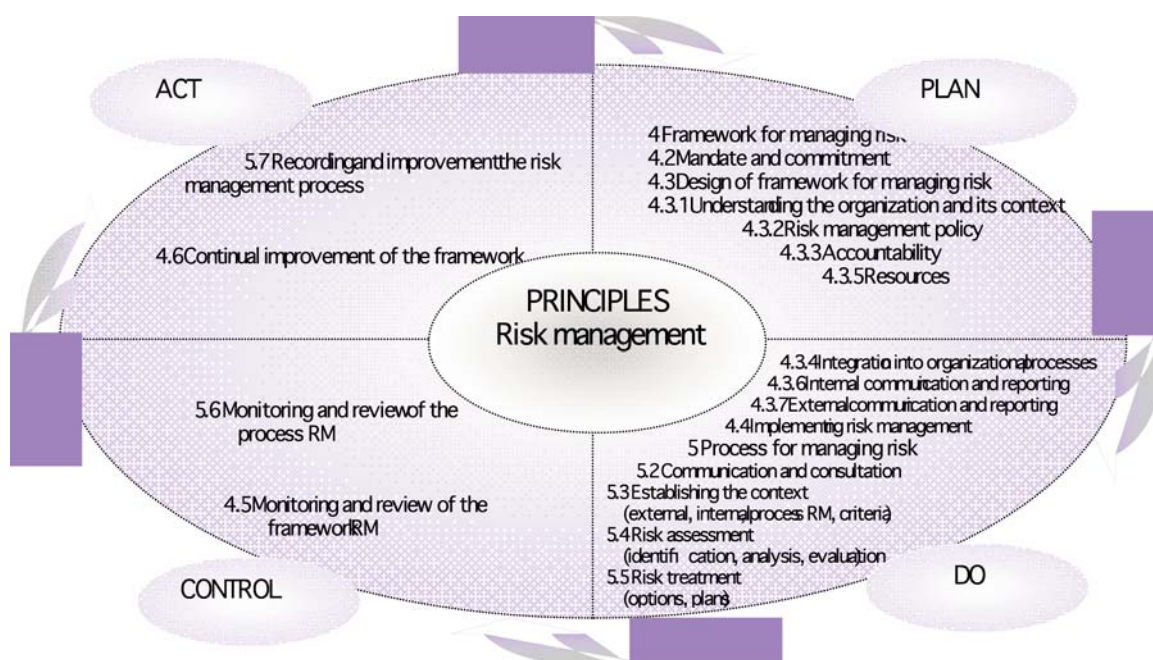


Fig. 3 The key elements of risk management system according to ISO 31000 in the Deming cycle of continuous improvement

Transformation of the structures of the forthcoming standard for Deming cycle of continuous improvement and adjustment separately proposed PDCA management process, risks and structures of risk management (particularly in the – Check audit) creates a space for its use as an “umbrella” standard management of partial aspects.

### References:

- [1] BRENTON, P., SHEEHY, J., VANCAUTEREN, M.: Technical Barriers to Trade in the European Union: Importance for Accession Countries, *CEPS Working Document*, No. 144. April 2000.
- [2] HOHNL, W., MICHEL RUIZ, J.: *Accreditation and Certification*, Module M31. [on-line] Available on the Internet: <<http://www.kam.sjf.stuba.sk/katedra/publikacie/leonardo/ucebnica/31s.pdf>>.
- [3] HRUBEC, J., VIRCIKOVA, E.: *Integrated Management System*, Slovak University of Agriculture in Nitra, 2009, p. 543, ISBN 978-80-552-0231-0.
- [4] ISO/IEC 31010:2009 Risk management – Risk Assessment Techniques, Int’l Organization for Standardization, 2009.
- [5] MAJERNIK, M., KOLLAR, V., PANKOVA JURIKOVA, J.: *Accreditation and Certification in Environment*, Skalica : University of Central Europe, 2009., p. 122, ISBN 978-80-89391-07.
- [6] NENADAL, J. et al.: *Integrated Management System. A Practical Guide for Quality Managers, Environmentalists and Safety Technicians*, Praha: Verlag Dashofer, publishing house, l.l.c, 2008, p. 2698.
- [7] OSTERTAGOVA, E., BOSAK, M.: *Mathematical Model for Evaluation of the Engineering Projects Environmental Quality*, Proc. of 6. Int’l Conference Environmental Management, Trnava, 2006, p. 170–175, 2006. ISBN 80-89281-02-08.
- [8] PANKOVA JURIKOVA, J.: *The Methodology for Accreditation of Environmental Management in an Integrated Management System*, Dissertation thesis, Kosice : Technical University of Kosice, Faculty of Mechanical Engineering, 2010, p. 167.
- [9] STRHAN, R.: *Certification as a Tool of Economic Policy*, In: Proc. of Int’l conference Business Enterprise in Terms of Theory and Practice of the Knowledge Economy, Bratislava: Publishing EKONOM, 2006. ISBN 80-225-2227-9, pp. 684–688.
- [10] STN EN ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing, Bratislava : SUTN, 2003.
- [11] Slovak Office of Standards, Metrology and Testing: Prepared STN ISO 31000:2009 Risk Management – Principles and Guidelines on Implementation, Bratislava, 2010.
- [12] VEBER, J. et al.: *Management of Quality, Environment and Safety: Legislation, Systems, Methods, Practice*, Praha : Management Press, 2006, p. 350, ISBN 80-7261-146-1.
- [13] WHITING, J.: *What is New in ISO 31000 Risk Management – Principles and Guidelines on Implementation*, Nashville : TapRoot, 2009.