



Applying ISO management system standards to enterprise risk management

ISO management system standards can be important tools in a company-wide risk management programme. The first step is to understand what is meant by a generic risk management system. Next, the organization needs to look at how a standards-based system can be implemented.



by Valentin Nikonov

Valentin Nikonov is a project management professional recognized by the International Project Management Association and a certified ISO 9001:2000 auditor. As a senior specialist with the Growth Trajectory consultancy, located in Yekaterinburg, Russia, he is responsible for projects to implement integrated management systems, including risk management systems. Mr. Nikonov also participates in the activities of working party WP.6 of the United Nations Economic Commission for Europe. The focus of WP.6 is Regulatory Cooperation and Standardization Policies examining quality-related issues, including the development and implementation of integrated management systems.

e-mail valentin@traectoria.ru

Web www.traectoria.ru



For decades, ISO management system standards have proved invaluable to organizations around the globe aiming for improvement in a variety of areas: quality (ISO 9001:2000), information security (ISO/IEC 27001:2005), environment (ISO 14001:2004) and others.

These areas are quite specific and so are the standards. At the same time, there is an important unifier: they all can “work” for common goals – helping organizations of any type to systematically manage risks. That, in turn, is a condition for business stability, profitability and safety.

Managing different types of risk

All organizations work under a certain level of uncertainty, including market risks, credit risks, operational risks and legal risks.

These risks influence organizational performance and often hamper development, and in many cases impact business partners and consumers. Professionalism in dealing with uncertainty reduces threats to organizational stability, improves general economic health, and increases personal safety and quality of life. Successfully dealing with uncertainty requires continuous and efficient risk management.

With proper risk management methodology and tools, organizations of all kinds enhance their governance systems to become more predictable, stable and safe.

Another important consideration is that a company's risks can expose its partners and customers. This means that risk management systems are necessary not only for organizational profitability and security, but also for maintaining stable international trade.

Enterprise risk management

Risk management is a very broad methodology that can be applied to commercial businesses, delivery of public services, the non-governmental sector and even personal decisions. In any accident – from the Chernobyl catastrophe to a trivial car accident or a product that fails to meet quality requirements – there is always something that leads to the undesirable event. This may be simple human error (failure to follow safety guidelines), lack of training (an incompetent driver) or insufficient busi-

ness processes (poor quality control).

Although we must acknowledge that there are many risks that we cannot influence, there are still plenty of things that can be managed and changed. In simple terms, risk management provides techniques that help organizations prevent bad things from happening. In order to make this a consistent process, organizations need to systematically manage risks with an efficient enterprise risk management system, which can be based on existing ISO standards on management systems.

The two main objectives of an enterprise risk management system are to:

- help make the organization profitable; and to
- make the organization and all parties affected by its work safe and secure.

Profitability is directly related to the quality of services and goods, and to market demand for these products. Security results from implementation of protective measures. However, security measures can often hamper the business. To maintain profitability, organizations need to be as efficient as possible – to “drive as fast as possible”. But to make the business more secure, organizations need to carefully consider each action – to “drive slower”.

An enterprise risk management system can serve as a tool for combining business efficiency and security on the basis of continual management of risks.



There are many definitions of risk, but for our purposes these can be defined by four factors:

- **Event** – the threat that something may (or may not) happen to affect any of the interested parties.
- **Vulnerability** – factors that allow the threat to become realized.
- **Probability** – a measure of uncertainty of the threat to be realised.
- **Impact** – a measure of the consequences, usually in financial terms.

Nonconformities, mistakes, errors or deviations from requirements are examples of risks that can be managed and prevented.

ISO standards for risk management

ISO management system standards provide valuable tools for handling various kinds of organizational risks – quality, information security, occupational health and safety, environment, project management and more. An enterprise risk management programme can be built by integrating these

SPECIAL REPORT

systems into a single company-wide structure.

Every organization is subject to a wide range of risks, including:

- **HR risks** – a key person may leave the company; inadequate training may cause service provision to fail, etc.
- **Supplier and partner risks** – purchased products may not meet quality requirements; delivery may be late, etc.
- **Information security risks** – critical servers may fail; software bugs may compromise products or operations; confidential information may be stolen, etc.

- **Service provision process risks** – failures in the service provision processes: human error, technical mistakes, etc.
- **Legal risks** – new regulatory requirements may substantially change business conditions.
- There are also **ecological risks** and **occupational health and safety risks**.

To systematically manage these risks, a continuous risk management process should be implemented within the organization.

petence may want to change jobs.

Quantification. Next the risk should be quantified and analyzed so that serious risks requiring special attention can be determined. Assuming that the threatened loss of critical competence described above is judged a serious risk, four options are available:

**Risk management
is necessary for
organizational profitability
and security and stable
international trade**

knowledge and reduce dependence on that individual, or motivate the employee to stay in his or her position.

- **Transfer the risk** – outsource the at-risk process to ensure business continuity. The organization may outsource the process in which the employee is involved.
- **Avoid the risk** – cease activities that might lead to risks. Change the business strategy so that the organization is not dependent on the employee's competence.

Implementation. After the strategy is chosen, it needs



- **Financial risks** – changes on securities markets.
- **Marketing and product design risks** – a product may no longer be required on the market; competitors may introduce higher quality products; newly designed products may encounter production problems; supplier prices may change, etc.

Risk management and ISO 9001

Risk management is a continuous process encompassing the following steps:

Risk identification. Knowing the risks is the first step towards managing them. For example, an organization can identify the risk that a key worker possessing unique com-

- **Accept the risk** – knowingly acknowledge its existence but take no immediate action. Decide to handle the problems caused by the departing employee when the situation arises.
- **Mitigate the risk** – reduce the probability of the event or reduce its impact. The organization may try to document the employee's

to be implemented. The most common course is risk mitigation; the organization implements actions as described by a mitigation strategy.

Project analysis. The organization analyzes progress in implementation of the risk management strategy, ensuring that planned measures are completed.



Residual risk evaluation. After everything is complete, residual risks need to be evaluated and business continuity must be planned. Mitigation does not provide a 100 % guarantee that the risk will not occur; the organization needs a plan of action in the event the employee leaves.

If we treat ISO 9001:2000 as the core standard for the management system – meaning that all activities are managed within the quality management system and that quality is broadly understood – we see that all the processes from Section 8 of the standard are necessary for risk management, including internal audits, corrective and preventive actions, customer feedback, strategic planning and management review, and nonconforming product management.



ISO 9001:2000 process	Risk management process step
<i>Internal audits (8.2.2)</i>	All types of operational risk identification and analysis
<i>Customer satisfaction (8.2.1)</i>	Identification of customer-related and reputational risks (may also be considered operational risks)
<i>Strategic planning and management review</i> (strategic planning process is not literally described in ISO 9001, however it can be derived from clauses 5.3, 5.4 and 5.6)	Strategic risk identification, operational risk analysis (through review of corrective and preventive actions)
<i>Control of nonconforming product (8.3)</i>	Identification and management of risks that occurred, influencing product quality.
<i>Corrective and preventive actions (8.5.2, 8.5.3)</i>	The process of identification, quantification, analysis and mitigation of operational risks.

Table 1 – ISO 9001 processes related to risk management.

If the organization arrives at the conclusion that a nonconformity can be called a realized risk which requires mitigation, and a potential nonconformity is called a risk, the corrective and preventive actions process (clauses 8.5.2 and 8.5.3) is suitable for identification, quantification and management of risks.

Corrective and preventive actions may be implemented in such a way that their registration and analysis serve as a tool for risk processing. A sure way for an organization to manage the many risks it faces is to process them through such a process. The steps required by ISO 9001 cover all aspects of the risk management process.

Addressed risks

In addition to the risk management process, ISO 9001 gives organizations advice on how to deal with specific nonconformities, or risks.

Competence management is one of the most important mitigation strategies for *Human Resources risks*, described in clause 6.2 **Human Resources**. To manage *infrastructure risks*, the organization should conform to the requirements of clause 6.3 **Infrastructure**. The *suppliers and partners risk* mitigation strategy is described in clause 7.4 **Purchasing**. Development of supplier evaluation criteria and the supplier systematic evaluation makes an organization less vulnerable to these external risks.



Marketing and new product design risks are addressed in clauses 7.2 **Customer-related processes** and 7.3 **Design and development**. These recommendations can substantially reduce marketing- and client-related risks. If the requirements of clause 7.5 **Production and service** provision are met, risks associated with the *processes of service provision* will also be reduced.

At the same time, there are many risks that are not covered by the ISO 9001 standard,

operational risk. The approaches described in ISO/IEC 27001 imply development of the risk management process for dealing with information security risks. The only differences between ISO 9001 and ISO/IEC 27001 in this regard are to

- determine the information security risks we need to know the informational assets, and
- how to manage them (this is required for development of an information security management system).

ment system to address specific elements of operational risk – information security risks.

The same may be said of ISO 14001 and other ISO management system standards. They can all be a part of an enterprise risk management system addressing specific threats, while ISO 9001 should be a basis for this system since it contains the fundamental risk management process.

Conclusion

In general, ISO management system standards contain tools for managing operational risks as in the cases discussed above. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Operational risks are the most common risks for any organization. In the most well-known classification of risks (used in Basel II Capital Accord) we find three major classes: market, credit and operational risks.

While market and credit risks are very important in banking and finance, operational risks are equally important to every organization. These risks are addressed in ISO standards.

With ISO management system standards, businesses receive concepts and techniques for managing all types of organizational risks:

- ISO 9001 provides tools and a framework for managing operational risks.
- ISO 14001, OHSAS 18001 (occupational health and

security management – not an ISO standard), ISO/IEC 27001 and other standards provide special tools for addressing specific risks: environmental, occupational health and safety, information security, etc.

- An enterprise risk management system can be based on these standards.

The implementation of an enterprise risk management system will help organizations all over the world to effectively manage risks, providing profitability and security for their organizations, assuring the safety of stakeholders and sustainable growth of the world economy.

Development of a widely recognized standard and guides for an enterprise risk management system could help organizations to effectively implement the techniques described above.

This standard could be based on existing management system standards, making it easier for organizations that have already implemented ISO standards to embed risk management concepts into their processes for achieving both profitability and security.



but they are addressed in other standards for management systems. For example, *IT* risk mitigation strategies may be found in the ISO/IEC 20000 (IT service management) and ISO/IEC 27001 (information security management) standards, while *environmental* risks are addressed in the ISO 14000 standards.

The ISO/IEC 27001 standard includes strategies and tools for *information security* risk management, which constitutes an important element of

ISO 9001 corrective and preventive actions may serve as a tools for risk processing

The standard includes hints on how to mitigate information security risks (listed in Annex A).

ISO/IEC 27001 can be treated as an important part of an organization's risk manage-