How to Manage Risk In a Global Economy

Management tools and ISO standards support key processes

by Sandford Liebesman

The global economy has provided organizations many opportunities that didn’t exist just 10 years ago. But the flattening of the Earth via the internet and extensive outsourcing to countries such as China and Mexico have also presented organizations with many risks. The designers of the guidance commonly used for Sarbanes-Oxley Act (SOX) financial and accounting compliance recognized the importance of risk by including risk assessment as one element of the system of internal control.

An assessment process that can be used to manage risk consists of the following:

- Defining the organization’s objectives.
- Specifying the risk categories.
- Identifying risks to the objectives.
- Specifying the methods of managing risk.

Types of risk

Four types of risk worry organizations:

1. **Strategic risk** is concerned with the inability to achieve high level goals. For strategic risk assessment, management should consider technology changes, creditors’ demands, competitors’ actions, economic conditions, political conditions and customer needs. These considerations should be included in the quality management system planning process described in ISO 9001, clause 5.4.2.

2. **Organizational risk** is based on an organization’s structure and is affected by external and internal factors.

   External factors include technology developments, competition legislation and the global environment. Examples of internal risks are physical security, information system processing, lost shipping and receiving records, personnel competence and changes in management responsibilities.

3. **Compliance risk** affects the ability to meet legal and regulatory requirements. The focus is on financial, environmental, health and safety, and security factors. Management is concerned because of the threat of fines, shutdowns or criminal
prosecutions. There is also a concern with conformance to quality and environmental standards and specifications.

Environmental compliance risks include liquid spills, gaseous emissions and solid waste creation. ISO 14001, the environmental management system standard, requires monitoring and measurement of environmental risks, identification of significant environmental aspects and evaluation of compliance to the standard.

The U.S. Environmental Protection Agency (EPA) has recognized the value of ISO 14001 by establishing a national environmental performance track that provides incentives for participation. The incentives include allowing specific facilities to have lower priority for routine EPA inspections and the right to use EPA’s performance track logo.

4. **Operational risk** concentrates on factors that could prevent the efficient use of resources. These include an ineffective management system, poor customer satisfaction, supply chain problems, a weak revenue recognition process, poor information security management, the effect of natural disasters and logistical risks.

**Types of operational risk**

Factors that affect the capabilities of a management system include management strategies, practices and tools; data processing and call center capabilities; contract administration; and design and development effectiveness. Compliance with ISO 9001 can be used to manage these factors.

There are areas of operational risk that can be managed using ISO 9001: customer satisfaction, supply chain, revenue recognition, information security, logistics and natural disasters.

Customer satisfaction risk is affected by customer communication, delivery problems, product quality, design problems, repair problems and the accuracy of customer feedback. ISO 9001 requires the organization to gather and analyze customer satisfaction data.

Supply chain risk can be caused by poor communication with suppliers. Procurement managers must be concerned with factors such as managing outsourced products and services, risks associated with having a sole supplier, delivery problems, quality of received products, inventory management, and design and documentation problems. Again, ISO 9001 is an effective mitigation tool.

Revenue recognition risk is affected by problems with accounts payable and accounts receivable, revenues recorded before delivery, quotation to cash errors, spreadsheet errors and out-of-date or incomplete pricing information.

Quality managers can play an important role in controlling the effectiveness of the revenue recognition process. An overlap between quality and financial management systems includes product realization (ISO 9001, clause 7), costs, sales, invoices, payments, inventory management and delivery.

In many organizations, revenue recognition problems have a major effect on the organization’s earnings. Corrections could require a restatement of earnings, which might trigger a falling stock price.
Information security risks include viruses, unsecured files, inaccurate financial records, poor change control, information retrieval errors, overuse of spreadsheets, use of contractors and consultants, introduction of new technology (including hardware, software and network), industrial espionage and fraud. 

The new ISO/IEC 27001 is designed to provide management of information security. Its suitable uses include:

- Formulating security requirements and objectives.
- Ensuring that security risks are managed cost effectively.
- Complying with laws and regulations.
- Defining new information security management processes.
- Determining (by internal and external auditors) the degree of compliance with the policies, directives and standards.

Logistics risks include transportation of raw materials and completed products, products damaged during shipping, delays that cause understocking of materials and homeland security.

Threats to U.S. security are a major concern. The search for concealed weapons of mass destruction will slow shipping and receiving processes. New tools will have to be developed to screen and trace materials economically without supply line disruption. Software is also at risk due to the creation and dissemination of viruses by those who want to hurt the general economy.

Natural disasters in the past few years have included major hurricanes, flood, fires, earthquakes, contamination and epidemics. Business continuity requires safekeeping of enterprise information in protected storage.

Organizations should plan for disaster recovery and business continuity with a process that ensures the following:

- All documents are retained and available to investigating agencies.
- Potential material events are covered.
- Audit documents are safe for the seven-year period required for compliance with SOX.
- There is a business continuity plan.

**Risk management methodology**

Risk analysis methodology starts with the organization determining its risk appetite and risk tolerance so all personnel can understand the organization’s philosophy. Tools are then used to determine the risk levels and manage the risks.

Risk appetite is the amount of risk an entity is willing to accept. It is the measure of the risk-reward trade-off in the business.

On the other hand, risk tolerance relates to the entity’s specific objectives. It is the amount of variation an entity is willing to accept relative to these objectives. Risk appetite defines the boundary of acceptable risk for many categories, while risk tolerance defines the variation in objectives that affect specific risks.
Risk appetite sets the high level risks for organization. For example, an organization might say new product development should not exceed 25% of the projected overall profit. Perhaps one of the objectives is that the budget for R&D for a product is $1 million, and the risk tolerance for budgets is 15%. If spending on a particular new product is going to exceed $1.15 million, action would be taken to reduce the spending on R&D. It is the responsibility of top management and the board of directors to align risk appetite and risk tolerance with the organization’s strategy.

**Organizational controls**

One key tool for managing risk is the organization’s set of controls. These are especially important for compliance with SOX. Auditors test the controls as a key part of the compliance process. The financial controls are at two levels—entity and activity. The quality controls are also at these two levels and appear as “shall” statements in ISO 9001 and ISO 14001.

“Shall” statements are often accompanied by requirements to submit a quality record. These records are often used to identify impending risks. Examples of entity level controls are HR policies, codes of conduct, communication strategy, accounting practices, management’s risk assessment process, organizational responsibilities and contract review. Contract review requirements are related to quality requirements in ISO 9001, clause 7.2.2.

Activity level controls include reconciliation of general ledger to a subsidiary ledger, automated data validation and edit checks, and review and approval of paper based information prior to input.

Quality controls at the activity level include control of nonconforming product (ISO 9001, clause 8.3), design and development validation (ISO 9001, clause 7.3.6), preventive action (ISO 9001, clause 8.5.3) and identification of significant environmental aspects (ISO 14001, clause 4.3.1).

Risk management consists of activities to identify and analyze risks that might prevent achievement of objectives. Effective risk management requires definition and compatibility of the organization’s objectives, identification of risks to achieving objectives, judgment of which risks are critical and use of risk management tools to mitigate risks.

**Risk management tools**

A key tool is the risk level matrix (see Table 1, p. 58). For each identified risk, the consequences and likelihood of occurrence of the risk are estimated and input into a risk level matrix.
Once the level of concern is determined for each risk, preventive actions can be implemented for the extreme and high risks. Organizations can use the ISO 9001 preventive action process to accomplish this. Other risk management tools include:

- Objectives, risk, controls and alignment (ORCA).\(^2\)
- ISO 9001’s improvement process.
- Failure mode effects analysis (FMEA).
- Risk control matrix.

ORCA requires organizations to articulate objectives, identify and assess risks across the entire spectrum, build in balanced controls to manage risks and ensure alignment of objectives, risks and controls across the entire enterprise.

The ISO 9001 improvement process consists of using the ISO 9001 improvement loop: quality policy, quality management system planning, quality objectives, audit results, analysis of data, corrective and preventive actions, and management review. Data analysis identifies opportunities for corrective and preventive actions.

FMEA\(^3\) examines potential failures in products or processes and helps select remedial actions that reduce risks. It starts with a description of the parts of a system. Next, the consequences of each part failure are determined.

A risk level matrix can be used to evaluate the level of concerns for each failure. The ability of controls to detect failures is also determined. Actions that could eliminate or reduce the occurrence or improve the detectability of risks are identified.

Finally, the FMEA method is used to track changes that were incorporated to avoid potential failures.

A risk control matrix\(^4\) can be used to track risks and associated controls. It consists of the following information in tabular form:

- Process.
- Risk.
- Control objective.
- Controls.
- Control owner.
Getting started

Risk management must start with a definition of an organization’s objectives. These should be measurable, as required by ISO 9001.
Risks are obstacles that impede progress toward achieving these objectives. An organization needs to determine its risk appetite and tolerance so employees will have a consistent risk philosophy.
An organization can determine risk levels by combining the likelihood of an event and its consequences in a risk level matrix. The result is used to determine the appropriate management activities. In a SOX compliant process, risk based controls are tested to identify evidence of potential SOX deficiencies.

REFERENCES


SANDFORD LIEBESMAN is president of Sandford Quality Consulting LLC, Morristown, NJ, following more than 30 years of experience in quality at Bell Laboratories, Lucent Technologies and Bellcore (Telcordia). He is an author of the books TL 9000, Release 3.0: A Guide to Measuring Excellence in Telecommunications, second edition, and Using ISO 9000 to Improve Business Processes. Liebesman, a fellow of ASQ, is a member of ISO technical committee 176 and the ANSI Z-1 committee on quality assurance and a RABQSA International certified ISO 9000 and TL 9000 lead auditor.