Risk management and management system standards

A management system provides best practice guidance on the way in which an organisation manages a specific function of its business, to achieve its objectives. These objectives can relate to several different topics, including product or service quality, environmental performance, occupational health and safety and many more.

Each of these is the subject of a specific ISO standard: for instance, quality management (ISO 9001), environmental management (ISO 14001) and occupational safety (ISO 45001). They all share a common structure and are known generically as Management System Standards (MSS).

MSS are the result of consensus among international experts. They can be implemented by any organisation, large or small, and are designed to be applicable across all economic sectors and diverse geographical and cultural backgrounds.

One of the fundamental principles of MSS is that all the standards can be used to create an overall integrated business management system. Those who already use an MSS in one part of their business, and are considering implementing additional ones in another area, will find that the process has been made as intuitive as possible. That is because of the High-Level Structure (HLS). The concept of the HLS is that management standards are structured in the same way, regardless of the area of application. This generic structure also prescribes identical core text, common terms, and core definitions.

The High-Level Structure (HLS)

The structure of the common HLS (known as Annex SL) for all ISO management system standards is:

Clause 1 Scope
Clause 2 Normative references
Clause 3 Terms and definitions
Clause 4 Context of the organisation
Clause 5 Leadership
Clause 6 Planning
Clause 7 Support
Clause 8 Operation
Clause 9 Performance evaluation
Clause 10 Improvement

Guidance on ISO 31000 for users of MSS

All MSS refer to risk management or risk-based thinking, which are effectively the same thing. This allows the international risk management standard, ISO 31000:2018, to then be used to structure risk management within each MSS.

ISO 31000:2018 offers guidance to all types of organisation, regardless of type and size, and is written for people who create and protect value in organisations by managing risks, making decisions, setting purpose and strategy, achieving objectives, and improving performance.

ISO 31000 provides a common approach to managing any type of risk faced by an organisation. The purpose of the risk management framework is to assist the organisation in integrating risk management into significant activities and functions, including management systems.

Using ISO 31000 can help organisations increase the likelihood of achieving its objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment.

So how can risk management be incorporated into an MSS?

A new document, ISO IWA 31:2020, sets out how ISO 31000 can be applied within management systems.

In **Clause 4** of the HLS, the organisation is required to determine the risks which can affect its ability to meet the system objectives. It recognises that the consequences of risk are not the same for all. For some, the consequences of delivering a non-conforming product are minor; for others, the consequence can be fatal. The requirements relating to communication in MSS are supplemented with suggestions in ISO 31000.

In **Clause 5**, top management is required to demonstrate leadership and commit to ensuring that risks and opportunities that can affect the conformity of a product or service are determined and addressed. This is supported by both the principles and framework for risk management in ISO 31000.

In **Clause 6**, the organisation is required to take action to identify risks and opportunities, and plan how to address them. The ISO 31000 process sets out how this may be implemented.

Clause 8 covers operational planning and control. The organisation is required to plan, implement, and control its processes to address the actions identified in Clause 6. Again, this is supported by guidance in ISO 31000.

In **Clause 9,** the organisation is required to monitor, measure, analyse and evaluate risks and opportunities: this also forms a core part of the risk management process in ISO 31000.

Finally, in **Clause 10** the organisation is required to commit to continuous improvement by responding to changes in risk, as per ISO 31000.

ISO IWA 31 cross references in detail the principles, process, and framework of ISO 31000 against each of the ten clauses of the HLS in turn.

Benefits of integrating risk management into MSS

There are many benefits from integrating risk management into MSS.

These include:

- Appling risk management systemically to all aspects of the organisation, from management and its governing body, to operations at every level.
- Promoting a risk-aware culture in decision-making, to take advantage of opportunities and prevent undesirable results.
- Ensuring everyone has responsibility for managing risk, within their respective areas of competence and assigned limits of authority and accountability.
- Meeting increasing expectation from clients for ethical behaviour, recognising that this applies to all aspects of processes.
- Controlling legal risks, and thus meeting both regulatory and compliance obligations.
- Saving costs and reducing possible operational confusion by combining previously separate processes and operating manuals.
- Meeting supplier and customer expectations and thus protecting both brands and reputation.

An example – integrated risk and quality management

While risk and quality management are often thought of as separate and different, they complement each other a great deal. Both disciplines rely on similar analysis techniques to determine which actions drive more efficient business practices. Risk management can therefore be seen to be an integral part of a quality management system.

As an example of how risk and quality management complement one another, consider the challenges of managing a large supplier base. Meeting multiple compliance directives requires a complex set of processes, in turn requiring a thorough quality management system. An integrated risk and quality management system allows a firm to more easily anticipate and meet the demands of those processes.

Given the increasingly competitive nature of manufacturing today, risk management is relevant at every level of a quality management system. Bringing the systems together, not only gives a firm competitive advantage over the long term but may also protect its reputation. Failure to address risk costs money and reduces customer satisfaction. Why not therefore improve customer satisfaction by delivering a high-quality product where risk is already being managed? In other words, preventing or eliminating negative risk, such as product failure, is a core component of quality and leads to true customer satisfaction.