An integrated approach to management systems

Adding an information security element

Shifting to standardization

Today's marketplaces require companies to consider a wide range of components that define success. Management systems and processes that have been effectively implemented can underpin all drivers of organizational effectiveness. They also help to introduce a continual improvement mindset that sits at the heart of any good business.

Since ISO 9001 – the international standard that defines the requirements of a quality management system – was introduced, over one million organizations have achieved certification. It is now one of the most significant pieces of business literature ever written.

Following the success of ISO 9001, many additional standards have since been published, and more organizations began to implement multiple management systems – each requiring separate third-party certification. As a result, it became clear that a lack of consistency in the structure and content of different ISO standards made it very difficult to take a more integrated approach. As a solution, ISO introduced Annex SL.

The role of Annex SL

Annex SL is the framework that all new and revised ISO management system standards follow.

To ensure that standards are consistent and compatible with one another, Annex SL includes four key themes:

High-level structure

This is the foundation of Annex SL and features ten clauses from scope to planning and improvement. It dramatically reduces duplication of effort, with management systems following the same set of basic requirements.

Identical core text

As a minimum, management system standards will have at least 84 generic requirements, plus any additional discipline-specific requirements.

This helps ensure that materials relating to standards are clear, repeatable and easily digested by those working across multiple areas.

Common terms and definitions

There are 22 terms and definitions which must be addressed in all standards. For example, 'interested party' is the term preferred to 'stakeholder' and 'leadership' replaces 'management responsibility'.

Risk-based approach

Annex SL helps organizations to adopt a systematic, proactive approach to risk. This minimizes the occurrence and impact of undesired events and promotes continual improvement.

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

Ease of implementation

The compatibility that Annex SL introduces makes it easier to integrate the requirements of multiple standards into a single system. As a result, it's now much more straightforward for an organization to add new Annex SL based management systems and combine them with existing ones.

This is a more practical approach that minimizes duplication and creates a system where the many parts push towards the same set of strategic goals. Annex SL also provides organizations with a best practice framework to manage other processes that haven't been chosen for certification.

Through integration, organizations can use their resources more efficiently and take a standardized approach to documentation. They can also improve their management of crucial operations and processes.

Case Study

Terex Trucks

Terex Trucks was one of the first organizations to transition to ISO 9001:2015.

Thanks to Annex SL, Terex Trucks benefited from commonalities between standards. This enabled the integration of the organization's quality (QMS) and environmental management systems (EMS).

"There is a lot of commonality between the two standards [ISO 9001 and ISO 14001], and with both now following the structure introduced by Annex SL, we were able to learn from the work we completed on our QMS to integrate our EMS at the same time.

Our performance statistics confirm that we have successfully delivered on our aims for the QMS and EMS, and we will continue to build on this in the future through the deployment of our management system."

An optimized certification process

The advantages of integration are not limited to the implementation of management systems.

When an organization appoints a certification body, such as LRQA, integrated audits drive a more efficient approach. For example, the high-level structure may only need to be reviewed once, which could reduce the number of site visits required.

Through integration, organizations also build long term relationships with certification bodies and auditors.

With exposure to multiple systems, auditors develop an intimate, holistic knowledge of the business and its goals, as well as its modus operandi. This enables the delivery of more profound insights that carry a higher impact.

Digital Assurance

When working with LRQA, organizations can, in many cases, choose to have their audits delivered remotely using safe and secure technology. This option provides the same high-quality service with several added benefits, including flexibility, fast delivery and access to global expertise.

Companies can also opt for a blended approach that optimizes the overall process using remote audits while utilizing on-site options to help build strong personal relationships.

All LRQA clients that choose a remote audit benefit from the flexibility and convenience it delivers. However, it also shows organizations how mainstream technology can be leveraged to perform an effective audit that is not limited by geographical boundaries. This helps some businesses identify how they can use similar technology and platforms for their own internal oversight and audit programs.

Including ISO 27001 in your integrated management system

ISO 27001 is the international standard that outlines the requirements for an information security management system (ISMS).

For any organization – regardless of size or sector - ISO 27001 provides a solid foundation for a comprehensive information and cyber security strategy. It outlines a best practice framework to mitigate risks and safeguard business-critical information through identification, analysis and actionable controls.

Including ISO 27001 in a wider integrated management system is an ideal way to ensure that as a strategic focus area, best practice information security is embedded within the organization.

Integrating ISO 27001 with ISO 9001

Thanks to Annex SL, it's become increasingly popular to integrate ISO 27001 and ISO 9001. Both standards share a similar structure and focus on internal and external issues – albeit from different, discipline specific angles.

Integrating the requirements of both standards into a single system ensures that the organization's processes are aligned. Similarities between the standards also provide an opportunity to speed up implementation and use resources more efficiently.

For each standard, specific requirements differ. However, as an example, the following common areas can be addressed using the same processes and systems; leading to different outcomes:

- Interested parties
- Responsibilities
- Document management system
- Internal audit & management review
- Systems for nonconformities and corrective actions

Extending your system to manage specific information security risks

Depending on an organization's risk profile, other standards and guidelines allow an opportunity to expand the system to address more specific threats.

ISO 27001 is part of the ISO 27000 series of standards. Within the ISO 27000 family, several other standards and guidelines exist, which are extensions to ISO 27001.

These additional standards and guidelines outline controls relating to areas like privacy & data protection (ISO 27701, ISO 27018) and cloud security (ISO 27017). Compliance with additional standards such as these further strengthens the information security element of an integrated system. It ensures that a more robust and extensive approach to risk management is in operation.

It's also common for organizations to expand their integrated system to cover business continuity (ISO 22301) and, where relevant, IT service management (ISO 20000-1).

Case Study

OCTO Telematics

OCTO Telematics (OCTO) is a leading provider of telematics services and advanced data analytics for the insurance sector.

OCTO implemented a comprehensive, integrated management system that was audited and certified by LRQA. It helps the organization keep pace with the constantly evolving information security threat landscape – proactively mitigating risks before they occur.

"The high-level structure of Annex SL, with its identical basic text, common terms and definitions, facilitated the integration of our management systems."

"Through integration, OCTO were able to minimize conflict between individual systems. It also reduced duplication of processes, administration work and general bureaucracy. This ensured a much stronger focus on the needs of the whole business rather than one particular area."

"A certified ISMS is a gateway to securing business with important customers. However, it's also enabled OCTO to take an organic approach to system security – through extending the ISMS to properly manage the threats and opportunities that relate to our business."

Attilio De Bernardo

Chief Information Security Officer
OCTO Telematics

Building your integrated management system with LRQA

We understand that your organization has unique requirements. Whether you're a small or medium-sized business looking to take the first steps towards an integrated management system or a large enterprise looking for additional levels of assurance - our team of experts will work closely with you to understand your specific needs.

LRQA delivers a range of accredited audit, certification and training services relating to the world's leading standards and schemes from information security to quality and health & safety.

Get in touch

For more information, visit **lrqa.com/us**

YOUR FUTURE. OUR FOCUS.

About LRQA:

By bringing together unrivaled expertise in certification, brand assurance, food safety, cybersecurity, inspection and training, we've become a leading global assurance provider.

We're proud of our heritage, but it's who we are today that really matters, because that's what shapes how we partner with our clients tomorrow. By combining strong values, decades of experience in risk management and mitigation and a keen focus on the future, we're here to support our clients as they build safer, more secure, more sustainable businesses.

From independent auditing, certification and training; to technical advisory services; to real-time assurance technology; to data-driven supply chain transformation, our innovative end-to-end solutions help our clients negotiate a rapidly changing risk landscape – making sure they're shaping their own future, rather than letting it shape them.

Get in touch

Visit **www.lrqa.com/us** for more information
866-971-LRQA
info-usa@lrqa.com

1330 Enclave Parkway, Suite 200
Houston, TX 77077
United States