Information Security STARTS HERE

An integrated approach to management systems

Adding an information security element

iso systems UK
Concept to Certification

Shifting to standardisation

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 organisational 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 organisations 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 organisations 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.

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'.

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.

Risk-based approach

Annex SL helps organisations to adopt a systematic, proactive approach to risk. This minimises 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 organisation
Clause 5	Leadership
Clause 6	Planning
Clause 7	Support
Clause 8	Operation
Clause 9	Performance evaluation
Clause 10	Improvement

The Annex SL High-Level Structure

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 organisation to add new Annex SL based management systems and combine them with existing ones.

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

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

Case Study

Project Client

Thanks to Annex SL, our client benefitted from commonalities between standards. This enabled the integration of the organisation'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 optimised certification process

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

When an organisation appoints a certification body, 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, organisations 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.

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 organisation – 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 organisation.

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 organisation'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 organisation'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 organisations to expand their integrated system to cover business continuity (ISO 22301) and, where relevant, IT service management (ISO 20000-1).

Building your integrated management system with ISO Systems UK

We understand that your organisation 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.

ISO Systems UK delivers a range of supporting services such as project support, ongoing maintenance, internal audit programmes, training services and dedicated eLearning portals relating to the world's leading standards and schemes from information security to environmental, quality and health & safety.

Find out more

Speak to us here at ISO Systems UK on **01325 788352** or email **services@isosystems.org.uk** to arrange a free consultation to discuss your organisation's requirements

We hope you found this publication useful and informative. Should you require further information or support you can contact us in a variety of ways:

Email us via services@isosystems.org
Call us on 01325 778352 / 07791 425011
Contact us via our website

Follow us on social media

Search: ISO SYSTEMS UK