MANAGE YOUR INTEGRATION

ISO 9001 TO ISO 27001 GAP GUIDE

ISO 27001:2013 the Information Security Management Standard is one of the fastest growing standards right now; partly due to the ever evolving digital landscape and the recent introduction of the new General Data Protection Regulations (GDPR).

Similarly to ISO 9001, ISO 27001 is the internationally recognized standard for information security management. It is the most widely used ISMS standard in the world, with over 35k certificates issued to organizations in 178 countries.

What do these standards have in common? And if you have one management system can you have the other?

The best way to implement another management system if you already have one is to implement an Integrated Management System (IMS). This way both systems meet the requirements of the standard and you won't be duplicating lots of work.

How do you start though? Firstly look at the easy bits - what's common. If you are already fulfilling one standard requirement, chances are you may not be far away from achieving the same requirement under a different standard.

Within this brief you will see that we have mapped out the various different clauses within both ISO 9001:2015 and ISO 27001:2013 to help you understand how implementing another standard on top of existing processes and procedures can be achieved successfully.

First a brief overview of the main clauses and the similarities.

- **Context of the organization**
  Both standards require organizations to identify the internal and external issues relevant to the company albeit from a different viewpoint. ISO 9001 focuses on Quality and ISO 27001 focuses on Information Security
- **Interested parties**
  Organizations must determine the interested parties plus their needs and expectations relating to quality or information security. This can be achieved in the same process with a combined list created
- **Responsibility and authority**
  Both standards require the roles and responsibilities for the QMS and ISMS to be defined. Although these roles may be different the same process for the identification and definition of these roles can be the same
- **Competence, awareness, communication and documented information**
  These requirements are similar for many standards and not just ISO 9001 & 27001. They can be addressed in the same way and in many cases at the same time
- **Internal audits and management review**
  Although the audit criteria and management review input and outputs will differ, the process is exactly the same and depending on the size or complexity of the organization can be done together or separately
- **Nonconformity and corrective action**
  Both systems require a process for handling nonconformities and corrective action. This can be the same with no reason to keep them separate

THE DIFFERENCE

ISO 27001:2013 differs from ISO 9001:2015 in that it adds Information Security Risk Assessment and risk treatment into the ISMS. For an Information Security Risk Assessment, the organization must develop a methodology for the identification of information security risks. This is a separate process than that of addressing risk and opportunities with 9001.

The Information Security Risk Treatment process requires an organization to apply one or several of the information security controls listed within Annex A in an attempt to mitigate risk.

MAPPING

The following table shows the various clauses in the standards and their similarities:

ISO 9001:2015	ISO 27001:2013	GUIDANCE
4 Context of the Organization	**4 Context of the Organization**	
4.1. Understanding the organization and its context	**4.1. Understanding the organization and its context**	Both standards require organizations to determine internal and external issues related to the suitability of the management system achieving its intended outcome.
4.2. Understanding the needs and expectations of interested parties	**4.2. Understanding the needs and expectations of interested parties**	Both standards require organizations to identify relevant interested parties as well as their needs and expectations.
4.3 Determining the scope of the quality management system	**4.3 Determining the scope of the information security management system**	The scope of the management system must be defined for both standards. The difference is that ISO 9001 requires products and services to be considered, and ISO 27001 requires consideration of interfaces and dependencies between the processes when defining the scope.
4.4. Quality management system and its processes	**4.4. Information security management system**	The requirements are exactly the same, each system must be established, implemented, documented, and continually improved.
5 Leadership	**5 Leadership**	
5.1 Leadership and commitment	**5.1 Leadership and commitment**	Both standards require management to implement policies, make provisions for resources, Continual Improvement assigning roles and responsibilities etc.
5.1.1 General		No similar clause in ISO 27001.
5.1.2 Customer focus		No similar clause in ISO 27001.
5.2 Policy	**5.2 Policy**	The requirements are very similar and could be met in a single document. Some policies are written as separate documents. If separate the policies should be compatible with each other.
5.2.1 Establishing the quality policy		No similar clause in ISO 27001.
5.2.2 Communicating the quality policy		No similar clause in ISO 27001.
5.3 Organizational roles, responsibilities and authorities	**5.3 Organizational roles, responsibilities and authorities**	The requirements from the standard are the same in that roles, responsibilities and authorities can be communicated in the same way. This means, for example, the Quality Manager can also be the Information Security Manager and, based on competency could perform the internal audits on both systems.

ISO 9001:2015	ISO 27001:2013	GUIDANCE
6 Planning	**6 Planning**	
6.1 Actions to address risks and opportunities	**6.1 Actions to address risks and opportunities**	Both standards specifically require the identification of risks and opportunities arising from the context of the organization in terms of quality and information security. The only difference with ISO 27001 is that the standard provides a list of control measures which can be used to mitigate these risks in the form of Annex A.
6.2 Quality objectives and plans to achieve them	**6.2 Information security objectives and planning to achieve them**	Both standards stipulate a need to establish objectives and their plans for realisation. These can be separate documents or placed together.
6.3 Planning of changes		No similar clause in ISO 27001.
7 Support	**7 Support**	
7.1 Resources	**7.1 Resources**	The standards require the organization to determine and provide the necessary resources for process execution. This means the same processes can be used, such as; a purchasing process to fulfil requirements.
7.1.1 General		No similar clause in ISO 27001.
7.1.2 People		No similar clause in ISO 27001.
7.1.3 Infrastructure		No similar clause in ISO 27001.
7.1.4 Environment for the operation of processes		No similar clause in ISO 27001.
7.1.5 Monitoring and measuring resources		No similar clause in ISO 27001.
7.1.5.2 Measurement Traceability		No similar clause in ISO 27001.
7.1.6 Organizational knowledge		No similar clause in ISO 27001.
7.2 Competence	**7.2 Competence**	Both standards require the organization to identify and provide training for the necessary competencies of employees and also to keep records regarding those competencies.
7.3 Awareness	**7.3 Awareness**	A requirement of both standards is that employees are aware of the relevant policies and procedures. This also includes awareness of the role they play within the management system and how they impact the organizations performance with regards to quality and information security.
7.4 Communication	**7.4 Communication**	Both standards require the same thing and can be met via the same methods or processes.
7.5 Documented information	**7.5 Documented information**	The requirement is the same and the same processes/ procedures can be applied.

ISO 9001:2015	ISO 27001:2013	GUIDANCE
8 Operation	**8 Operation**	
8.1 Operational planning and control	**8.1 Operational planning and control**	Although the clause names are the same they have different scopes between the standards. ISO 9001 – focuses on defining and controlling process ISO 27001 – focuses on establishing information security controls.
8.2 Requirements for products and services		No similar clause in ISO 27001.
8.3 Design and development of products and services	**A.6.1.5 Information security in project management**	A.6.1.5 is a control measure from ISO 27001 Annex A and can be part of the procedure for design and development.
8.4 Control of externally provided processes, products and services	**A.15 Supplier relationships**	Although different clause numbers – very similar requirements. Contracts entered into with suppliers should include a consideration of information security clauses. Indeed, information security can be used as criteria for the evaluation of suppliers.
8.5 Production and service provision	**A.12 Operations security**	Any IT processes that support the production and service provision should have the information security requirements taken into account.
8.6 Release of products and services		No similar clause in ISO 27001.
8.7 Control of nonconforming outputs		No similar clause in ISO 27001.
9 Performance evaluation	**9 Performance evaluation**	
9.1 Monitoring, measurement, analysis and evaluation	**9.1 Monitoring, measurement, analysis and evaluation**	The effectiveness of the management system must be monitored using the parameters that the organization has identified as being important for the process realization. ISO 9001 also monitors customer satisfaction (9.1.2).
9.2 Internal Audit	**9.2 Internal Audit**	The same procedure can be applied to both standards regarding internal audits.
9.3 Management review	**9.3 Management review**	The clause and requirements are the same however both standards have different input elements. The same documentation can be used however the separate input elements must be contained.
10 Improvement	**10 Improvement**	
10.1 General		No similar clause in ISO 27001.
10.2 Nonconformity and corrective action	**10.1 Nonconformity and corrective action**	The same process can used to meet the similar requirements of both standards.
10.3 Continual improvement	**10.2 Continual improvement**	As with every management system an emphasis is placed on continual improvement which can be conducted via a joint procedure for corrective action.

If you already have a robust Quality management system in place under ISO 9001:2015, the benefits of implementing an Information Security Management System as well are countless. Not only does it help to demonstrate compliance to the new GDPR but it also highlights to your customers, employees and stakeholders that you take information security and data security seriously. You may already be doing more than you think.

nqa.

www.nqa.com