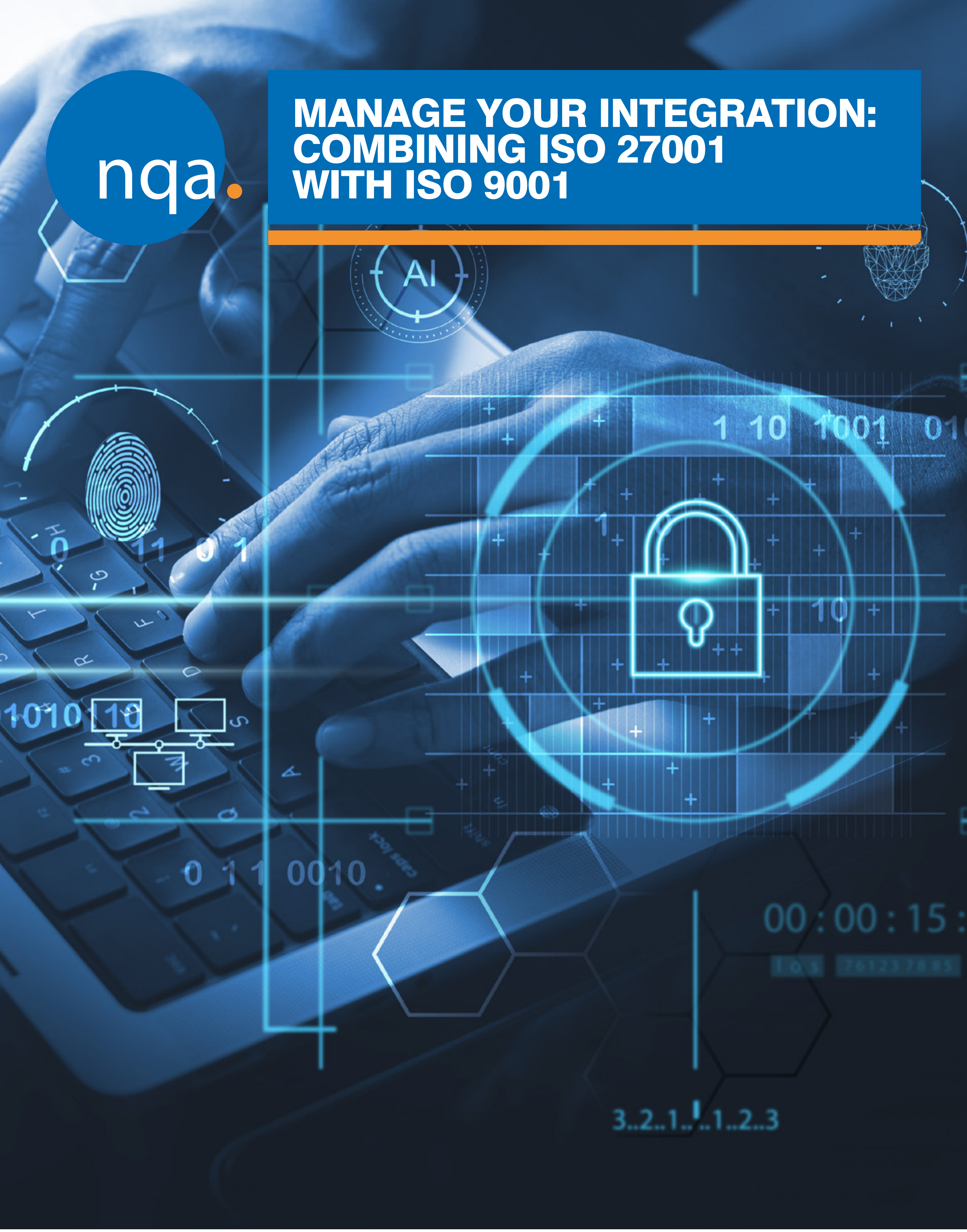
nqa.

MANAGE YOUR INTEGRATION: COMBINING ISO 27001 WITH ISO 9001



53,000 CERTIFICATES GLOBALLY

100% TRANSPARENT FEES

1000+ EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP 10 YEARS

OVER 100 OPERATING COUNTRIES

CARBON NEUTRAL

INTRODUCTION

ISO 27001:2022 (Information Security Management) is one of the fastest growing standards right now. ISO 27001:2022, the Information Security Management Standard, is one of the most popular certified ISO standards globally, due to the constant evolution of threats in the digital landscape, and an increased focus on data being considered a cherished business asset.

Similarly to ISO 27001, ISO 9001:2015 is the internationally recognised standard for quality management. It is the most widely used QMS standard in the world, with over 1.1 million certificates issued to organisations 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 a second management system if you already have one is to combine them into an Integrated Management System (IMS). This way both systems meet the requirements of the standards and you won't be duplicating lots of work.

HOW TO START:

If you're already meeting the requirements of one standard, the chances are that you may not be far away from achieving the same requirement under a different standard.

This guide maps out out the various different clauses within both ISO 9001:2015 and ISO 27001:2022 to help you understand how implementing another standard on top of existing processes and procedures can be achieved successfully.

THE SIMILARITIES

- **Context of the organisation**
  Both standards require organisations to identify the internal and external issues relevant to the company. ISO 9001 focuses on quality and ISO 27001 focuses on cyber security and data privacy.

- **Interested parties**
  Organisations must determine the interested parties plus their needs and expectations relating to quality and/or information security. This can be achieved in the same process with a combined list.

- **Responsibility and authority**
  Both standards require the roles and responsibilities to be defined. Although these roles may be different, the same process for identifying and defining these roles can be used.

- **Competence, awareness, communication and documented information**
  These requirements are similar for many standards and not just ISO 9001 and ISO 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 organisation can be completed together or separately.

- **Nonconformity and corrective action**
  Both systems require a process for handling nonconformities and corrective action. These can be the same, with no reason to separate them.

THE DIFFERENCE

ISO 27001:2022 differs from ISO 9001:2015 in that it specifically requires information security risk assessment and treatment. Your organisation must implement a methodology that allows you to identify information security risks.

The information security risk treatment process requires an organisation to apply one or several of the controls listed within Annex A and to publish a Statement of Applicability (SoA), to mitigate risk.

MAPPING

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

GAP GUIDE AND GUIDANCE

4 Context of the organisation

ISO 9001:2015	ISO 27001:2022	GUIDANCE
4.1. Understanding the organisation and its context	**4.1. Understanding the organisation and its context**	Both standards require organisations 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 organisations 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 dependencies between all 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

5.1 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.
5.2 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.
5.3 Organisational roles, responsibilities and authorities	**5.3 Organisational 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.

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 organisation in terms of quality and information security. The only difference with ISO 27001 is that the standard provides a list of control measures that 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 plans to achieve them**	Both standards stipulate a need to establish objectives and their plans for realisation. These can be separate documents or placed together.

GAP GUIDE AND GUIDANCE

ISO 9001:2015	ISO 27001:2022	GUIDANCE
7 Support		
7.1 Resources	**7.1 Resources**	The standards require the organisation 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.
7.2 Competence	**7.2 Competence**	Both standards require the organisation 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 organisation's performance with regards to quality and information security.
7.4 Communication	**7.4 Communication**	Both standards require the same level of communication support, which can be met with the same method.
7.5 Documented information	**7.5 Documented information**	The requirement is the same and the same processes can be applied.
8 Performance evaluation		
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 processes, whereas ISO 27001 focuses on establishing information security controls.'
8.3 Design and development of products and services	**A.5.8 Information security in project management**	A.5.8 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.5.19 Information security in supplier relationships**	Although they have different clause numbers, the two standards share similar requirements. Contracts entered into with suppliers should include a consideration of information security clauses.
8.5 Production and service provision	**Throughout Annex A**	No specific control can be directly mapped to this clause. ISO 27001 has numerous controls, including A.5.37, which directly relate to production and service provision.

GAP GUIDE AND GUIDANCE

9 Performance evaluation

ISO 9001:2015	ISO 27001:2022	GUIDANCE
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, but the input elements that separate the standards have to be included.

10 Improvement

ISO 9001:2015	ISO 27001:2022	GUIDANCE
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	**10.1 Continual improvement**	As with every management system, an emphasis is placed on continual improvement that can be conducted via a joint procedure for corrective action.

If you already have a robust quality management system in place under ISO 9001, there are huge benefits in implementing an information security management system.

Not only does it help demonstrate compliance with the latest GDPR rules, but ISO 27001 provides the perfect framework for organisations to show that 'Secure by Design' is embedded throughout their business, products and services.