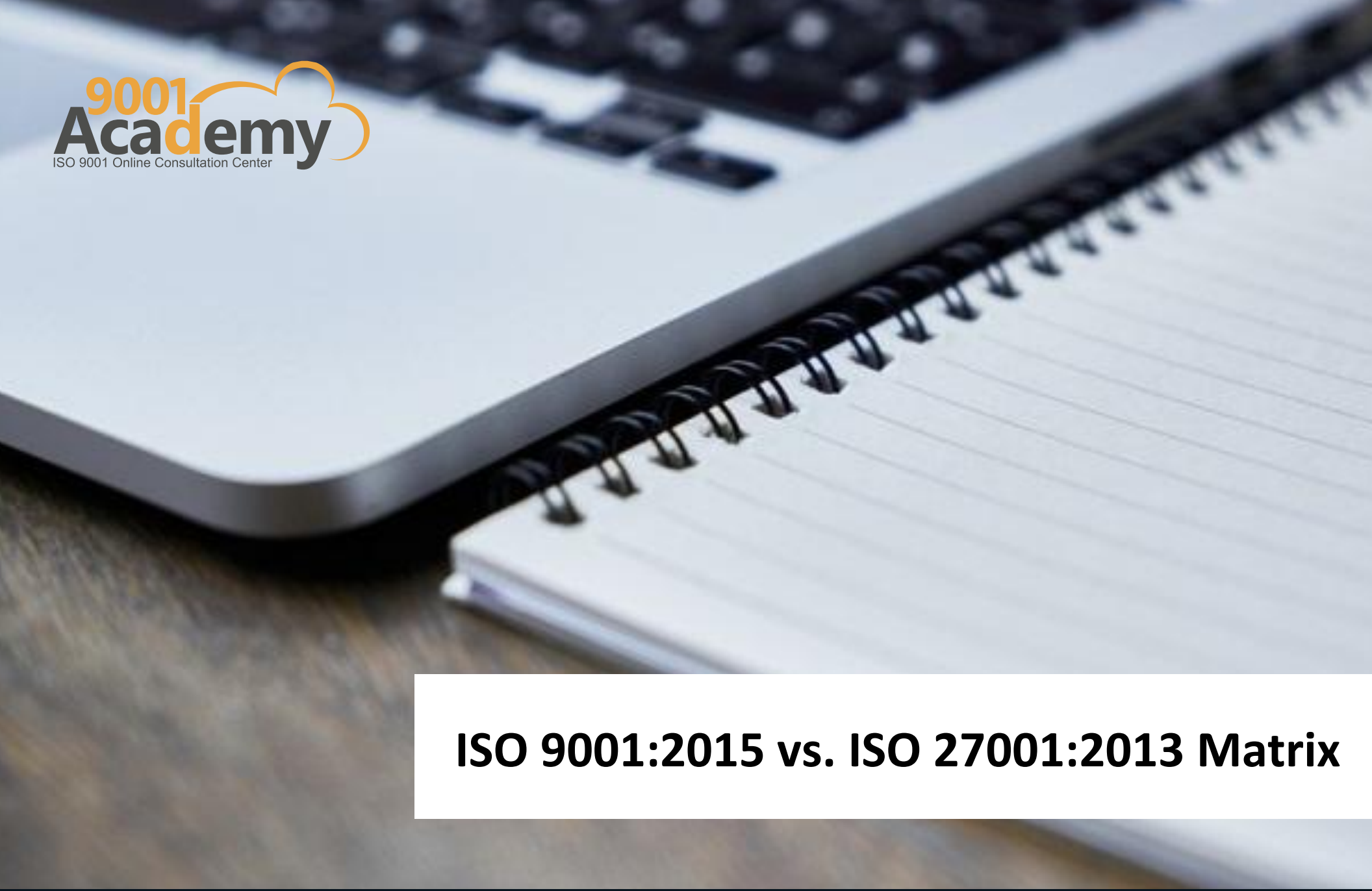

9001 Academy
ISO 9001 Online Consultation Center

ISO 9001:2015 vs. ISO 27001:2013 Matrix

Advisera
Making certification simple.

ISO 9001:2015	ISO 27001:2013	Explanation
Introduction	**Introduction**	
0.1 General	0.1 General	In both standards, this clause explains what the standard is, as well as the benefits and purpose of the standards. Of course, the standards have different scopes, with ISO 9001 focusing on quality, while ISO 27001 focuses on information security.
0.2 Quality management principles		There are no similar clauses in ISO 27001.
0.3 Process approach		There are no similar clauses in ISO 27001.
0.4 Relationships with other management system standards	0.2 Compatibility with other management system standards	Both standards are aligned with Annex SL and apply a high-level structure, making for easy incorporation into a single, integrated management system. For more information, see: How to integrate ISO 9001 and ISO 27001.
1 Scope	**1 Scope**	There are no big similarities regarding this clause, other than the fact that both clauses define the purpose of the standard and to what type of organization it can be applied.
2 Normative references	**2 Normative references**	This requirement is identical for both standards.
3 Terms and definitions	**3 Terms and definitions**	Both standards have this clause, but ISO 9001 refers to ISO 9000, while ISO 27001 refers to ISO 27000, as documents that contain information and definitions concerning the terminology being used in the standards.
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	The standard requires the organization to determine internal and external issues related to the ability of the management system to achieve the intended results. ISO 9001 is referring to quality and ISO 27001 is referring to information security. For more information, see: How to identify the context of the organization in ISO 9001:2015.

ISO 9001:2015	ISO 27001:2013	Explanation
4.2. Understanding the needs and expectations of interested parties	4.2. Understanding the needs and expectations of interested parties	Requirements of both standards are the same; they both require relevant interested parties to be identified, as well as their needs and expectations. For more information, see: Understanding needs & expectations of interested parties in ISO 9001:2015, How to identify ISMS requirements of interested parties in ISO 27001, and How to identify interested parties according to ISO 27001 and ISO 22301.
4.3 Determining the scope of the quality management system	4.3 Determining the scope of the information security management system	Both standards require the scope of the management system to be defined. 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. For more information, see: How to define the scope of the QMS according to ISO 9001:2015 and How to define the ISMS scope.
4.4. Quality management system and its processes	4.4. Information security management system	The requirements are 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	The requirements are the same, and the management has to treat both standards in the same way regarding implementing the policies, provision of resources, continual improvement, assigning roles and responsibilities, etc. For more information, see: How to comply with new leadership requirements in ISO 9001:2015.
5.1.1 General		
5.1.2 Customer focus		There is no similar clause in ISO 27001.
5.2 Policy	5.2 Policy	

ISO 9001:2015	ISO 27001:2013	Explanation
5.2.1 Developing the quality policy		The requirements are almost the same and in theory, they could be met through a single document. However, it is better if the policies are written as separate documents, in which case they must be compatible with each other. See a sample Quality Policy. For more information, see: How to Write a Good Quality Policy and What should you write in your Information Security Policy according to ISO 27001?
5.2.2 Communicating the quality policy		
5.3 Organizational roles, responsibilities and authorities	5.3 Organizational roles, responsibilities and authorities	The requirements are the same, so roles, responsibilities, and authorities for both standards can be communicated in the same way. For example, the same person can be the quality management representative and the information security manager; the same auditor can perform both QMS and ISMS audits.
6 Planning	**6 Planning**	
6.1 Actions to address risks and opportunities	6.1 Actions to address risks and opportunities	Both standards require the identification and addressing of risks and opportunities arising from the context of the organization regarding quality and information security. For more information, see: How to address risks and opportunities in ISO 9001, ISO 27001 risk assessment & treatment – 6 basic steps and How to organize initial risk assessment according to ISO 27001 and ISO 22301. For ISO 9001:2015, see a sample document here: Procedure for Addressing Risks and Opportunities. For ISO 27001:2013, see a sample document here: Risk Assessment and Risk Treatment Methodology. You can also check out this book on risk management: ISO 27001 Risk Management in Plain English.

ISO 9001:2015	ISO 27001:2013	Explanation
6.2 Quality objectives and plans to achieve them	6.2 Information security objectives and planning to achieve them	Objectives and plans for their realization for both standards can be placed in one document. For more information, see: How to Write Good Quality Objectives. See sample document here: Quality Objectives.
6.3 Planning of changes		There is no similar clause in ISO 27001.
7 Support	**7 Support**	
7.1 Resources	7.1 Resources	The organization has to determine and provide the necessary resources for process execution in order to meet the requirements for both standards. You can use the same processes to fulfill the requirements, such as the purchasing process.
7.1.1 General		
7.1.2 People		There is no similar clause in ISO 27001.
7.1.3 Infrastructure		There is no similar clause in ISO 27001.
7.1.4 Environment for the operation of processes		There is no similar clause in ISO 27001.
7.1.5 Monitoring and measuring resources		There is no similar clause in ISO 27001.
7.1.6 Organizational knowledge		There is no similar clause in ISO 27001.
7.2 Competence	7.2 Competence	Requirements regarding competence are the same for both standards; the organization needs to identify and provide training for the necessary competences of employees and to keep records on the employees' competences. For more information, see the following courses: ISO 9001:2015 Foundations Course and ISO 27001:2013 Foundations Course.

ISO 9001:2015	ISO 27001:2013	Explanation
7.3 Awareness	7.3 Awareness	Both standards require employees to be aware of the relevant policies and procedures, as well as their role within the management system and how they impact the performance of the organization regarding quality and information security. For more information, see: How to ensure competence and awareness in ISO 9001:2015, How to perform training & awareness for ISO 27001 and ISO 22301 and 8 Security Practices to Use in Your Employee Training and Awareness Program. For ISO 9001:2015, see a sample document here: Procedure for Competence, Training and Awareness. For ISO 27001:2013, see a sample document here: Training and Awareness Plan.
7.4. Communication	7.4. Communication	The requirement is the same and can be met through the same processes. E.g., writing announcements on a noticeboard, sending emails, regular staff meetings.
7.5 Documented information	7.5 Documented information	Requirements of both standards are the same regarding control of the documented information. You can apply the same procedure to meet the requirements of both standards and establish the documentation system. For more information, see: New approach to document and record control in ISO 9001:2015. For ISO 9001:2015, see a sample document here: Procedure for Document and Record Control. For ISO 27001:2013, see a sample document here: Procedure for Document and Record Control.

ISO 9001:2015	ISO 27001:2013	Explanation
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; in ISO 9001 the focus is on defining and controlling processes, and in ISO 27001 the focus is on establishing information security controls.
8.2 Requirements for products and services		There is no similar clause in ISO 27001.
8.3 Design and development of products and services	A.6.1.5 Information security in project management	This control can be part of the procedure for design and development. See a sample document here: Procedure for Design and Development.
8.4 Control of externally provided processes, products and services	A.15 Supplier relationships	Contracts made with suppliers should include information security clauses, and information security can be one of the criteria for the evaluation of suppliers. For more information on the purchasing process, see: Purchasing in QMS – The Process & the Information Needed to Make it Work. For more information on the process for supplier security, see: 6-step process for handling supplier security according to ISO 27001 and Which security clauses to use for supplier agreements? For ISO 9001:2015, see a sample document here: Procedure for Purchasing and Evaluation of Suppliers. For ISO 27001:2013, see a sample document here: Supplier Security Policy and Security Clauses for Suppliers and Partners.
8.5 Production and service provision	A.12 Operations security	Information security should be included in IT processes that support the production and service provision. The Quality Plan can refer to information security policies. See a sample document here: Quality Plan.
8.6 Release of products and services		There is no similar clause in ISO 27001.

ISO 9001:2015	ISO 27001:2013	Explanation
8.7 Control of nonconforming outputs		There is 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 organization must demonstrate the effectiveness of the system through monitoring of parameters that the organization identified as being important for process realization. These requirements can be met through the same document. For more information, see: Analysis of measuring and monitoring requirements in ISO 9001:2015 and How to perform monitoring and measurement in ISO 27001. See a sample document here: Matrix of Key Performance Indicators. Clause 9.1 in ISO 9001 also includes monitoring customer satisfaction. Measuring customer satisfaction should include the level of fulfillment of contractual and other requirements, which is a common requirement for both standards. See a sample document here: Procedure for Measuring Customer Satisfaction.
9.2 Internal Audit	9.2 Internal Audit	The same procedure for internal audit can be applied for both standards. For more information, see our courses: ISO 9001:2015 Internal Auditor Course, ISO 27001:2013 Internal Auditor Course and book ISO Internal Audit: A Plain English Guide. See a sample document here: Procedure for Internal Audit.
9.3 Management review	9.3 Management review	Although the requirement is the same, input elements of the management review are different. The same document can be used for both standards, but it has to contain separate input elements for each standard. See a sample document here: Procedure for Management Review.

ISO 9001:2015	ISO 27001:2013	Explanation
10 Improvement	**10 Improvement**	
10.1 General		There is no similar clause in ISO 27001.
10.2 Nonconformity and corrective action	10.1 Nonconformity and corrective action	The requirements of both standards are similar regarding nonconformities and corrective actions, and they can be met by the same process. For ISO 9001:2015, see a sample document here: Procedure for the Management of Nonconformities and Corrective Actions. For ISO 27001:2013, see a sample document here: Procedure for Corrective Action.
10.3 Continual improvement	10.2 Continual improvement	Like in every management system, the emphasis is on continual improvement, which is conducted through a joint procedure for corrective actions.
Annex A (informative) Clarification of new structure, terminology and concepts		There are no similar annexes in ISO 27001.
Annex B (informative) Other International Standards on quality management and quality management systems developed by ISO/TC 176		There are no similar annexes in ISO 27001.

You can download a preview of the ISO 9001:2015 Documentation Toolkit and ISO 27001:2013 Documentation Toolkit. This will allow you to see a sample of the policies and procedures required to implement the standards.

9001 Academy
ISO 9001 Online Consultation Center

Advisera Expert Solutions Ltd
for electronic business and business consulting
Zavizanska 12, 10000 Zagreb
Croatia, European Union

Email: support@advisera.com
U.S. (international): +1 (646) 759 9933
United Kingdom (international): +44 1502 449001
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485
Australia: +61 3 4000 0020

EXPLORE **ADVISERA**

9001 Academy · 9100 Academy · 13485 Academy · 14001 Academy · 16949 Academy · 18001 Academy

20000 Academy · 27001 Academy · EUGDPR Academy · Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple