ISO 27001:2013 vs. ISO 9001:2008 Matrix

ISO/IEC 27001:2013		ISO 9001:2008		Explanation
0	Introduction	0	Introduction	
0.1 General 0.2 Compatibility with other management systems		0.1 General 0.4 Compatibility with other management systems		These clauses have the same requirements for both standards.
1	Scope	1	Scope	ISO 27001 does not allow exclusions of clauses, in contrast with ISO 9001, which allows exclusions from clause 7 of the standard.
2	Normative references	2	Normative references	This requirement is identical for both standards.
3	Terms and definitions	3	Terms and definitions	Both standards are referring to their own "Fundamentals and vocabulary" standards (ISO 9000 and ISO 27000).
4	Context of the organization			
4.1 Understanding the organization and its context				There are no similar clauses in ISO 9001.
4.2 Understanding the needs and expectations of interested parties		5.1.a Management commitment		You can use the same document to list statutory and regulatory requirements regarding your organization. See a sample document here: List of Legal, Regulatory, Contractual and Other Requirements
4.3 Determining the scope of the information security management system		4.2.2.a) Quality manual		The requirements are the same and can be met through the same document. See sample document here: ISMS Scope Document
4.4 Information security management system		4.1 General requirements		The requirements are the same; each system must be established, implemented, documented and continually improved.
5	Leadership	5	Management responsibility	

ISO/IEC 27001:2013	ISO 9001:2008	Explanation
5.1 Leadership and commitment	5.1 Management 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.
5.2 Policy	5.2 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 sample document here: Information Security policy
5.3 Organizational roles, responsibilities and authorities	5.5.1 Responsibility and authority	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 Quality management representative and Information security manager; the same auditor can perform QMS and ISMS audits.
6 Planning		
6.1.1 Actions to address risks and opportunities - general	8.5.3 Preventive action	Addressing risks can be considered as preventive action, but it can't be merged in the same document.
6.1.2 Information security risk assessment		There are no similar clauses in ISO 9001.
6.1.3 Information security risk treatment		There are no similar clauses in ISO 9001.
6.2 Information security objectives and planning to achieve them	5.1 Management commitment	Objectives and plans for their realization for both standards can be placed in one document.

ISO/IEC 27001:2013	ISO 9001:2008	Explanation
7 Support	6 Resource management	
7.1 Resources	6.1 Provision of resources 6.2 Human resources 6.3 Infrastructure 6.4 Work environment	Organization has to determine and provide necessary resources for process execution in order to meet requirements for both standards. You can use the same processes to fulfill the requirements, such as purchasing process.
7.2 Competence 7.3 Awareness	6.2.2 Competence, training and awareness	ISO 27001 divides competence and awareness and emphasizes awareness more than ISO 9001. However, you can use one training plan for both standards to reduce records. See sample document here: Training and Awareness Plan
7.4 Communication	5.5.3 Internal communication	The requirement is the same and can be met through the same processes. E.g., writing announcements on noticeboard, sending emails, regular staff meetings.
7.5 Documented information	4.2 Documentation requirements	You can apply the same procedure to meet the requirements of both standards and establish a documentation system. See sample document here: Procedure for Document and Record Control
8 Operation		
8.1 Operational planning and control	8.2.3 Monitoring and measurement of processes	The key performance indicators (KPIs) can be set for processes of both standards and described in the same document.
8.2 Information security risk assessment		There are no similar clauses in ISO 9001.
8.3 Information security risk treatment	8.5.3 Preventive action	Preventive actions, as a term, are not mentioned in ISO 27001, but risk treatment plan can be regarded as preventive action. Output of risk treatment process can be input into preventive actions.

ISO/IEC 27001:2013	ISO 9001:2008	Explanation
9 Performance evaluation		
9.1 Monitoring, measurement, analysis and evaluation	8 Measurement, analysis and improvement 8.1 General 8.2.3 Monitoring and measurement of processes 8.2.4 Monitoring and measurement of product	Organization must demonstrate effectiveness of the system through monitoring of parameters that the organization identified as important for process realization. These requirements can be met through the same document, e.g., Balanced Scorecard or Matrix of Key Performance Indicators.
9.2 Internal Audit	8.2.2 Internal audit	The same procedure for internal audit can be applied for both standards. See sample document here: Internal Audit Procedure
9.3 Management review	5.6 Management review	Although the requirement is the same, input elements of management review are different. The same document can be used for both standards, but it has to contain separate input elements for both standards. See sample document here: Management Review Minutes
10 Improvement	8.5 Improvement	
10.1 Nonconformity and corrective action	8.3 Control of nonconforming product 8.5.2 Corrective action	Two clauses from ISO 9001 are joined together in ISO 27001, but the requirements are the same and can be met through the same procedure. See sample document here: Procedure for Corrective Action
10.2 Continual improvement	8.5.1 Continual improvement	Like in every management system, the emphasis is on continual improvement, which is conducted through a joint procedure for corrective actions.