27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

ISO 27001:2013 vs. ISO 22301:2012 Matrix

Advisera
Making certification simple.

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
0	Introduction	0	Introduction	
0.1	General	0.1	General	Information about the high-level structure of the standards, the process approach adopted for managing the systems, and the possibility of integrating them with each other or with other ISO management systems. For more information on this topic, see this article: How to implement integrated management systems.
0.2	Compatibility with other management system standards	0.2	The Plan-Do-Check-Act (PDCA) model	
		0.3	Components of PDCA in this International Standard	
1	Scope	1	Scope	Statements about the generality of the standards (fit for all kinds of organizations, independent of size, type, and nature). ISO 27001 does not allow exclusions of clauses from sections 4 to 10 (it only allows exclusions of controls from Annex A), in contrast with ISO 22301, which states that the extent of application of its requirements depends on each organization's operating environment and complexity.
2	Normative references	2	Normative references	ISO 22301 does not have normative references. ISO 27001 refers only to its documented vocabulary (ISO 27000).
3	Terms and definitions	3	Terms and definitions	Both standards list their own “Fundamentals and vocabulary” (ISO 27000 for ISO 27001, and ISO 22301 includes its own definitions of the main terms).
4	Context of the organization	4	Context of the organization	

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
4.1	Understanding the organization and its context	4.1	Understanding the organization and its context	These clauses require the organization to determine all internal and external issues that may be relevant to its business purposes and to the achievement of the objectives of their respective Information Security Management System (ISMS) / Business Continuity Management System (BCMS). In the case of BCMS, this also includes all elements that affect, or may be affected by, potential disruptive incidents (e.g., activities, function, service, products, etc.).
4.2	Understanding the needs and expectations of interested parties	4.2	Understanding the needs and expectations of interested parties	The standards require the organization to assess who the interest parties are in terms of its respective ISMS / BCMS, what their needs and expectations may be, which legal and regulatory requirements, as well as contractual obligations, are applicable, and consequently, if any of these should become compliance obligations. Legal and regulatory requirements must be documented, kept updated, and communicated to all interested parties. For both ISMS and BCMS, one document can be used to define the process of identification of interested parties, as well as statutory, regulatory, contractual, and other requirements related to information and business processes to be protected, and responsibilities for their fulfillment. See a sample document here: Procedure for Identification of Requirements. For both ISMS and BCMS, one document can be used to list requirements regarding information and business process to be protected. See a sample document here: List of Legal, Regulatory, Contractual and Other Requirements.
		4.2.1	General	

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
		4.2.2	Legal and regulatory requirements	For more information on this topic, see these articles: How to identify interested parties according to ISO 27001 and ISO 22301 and How to identify ISMS requirements of interested parties in ISO 27001.
4.3	Determining the scope of the information security management system	4.3	Determining the scope of the business continuity management system	The scope and boundaries and applicability of the ISMS / BCMS must be examined and defined considering the internal and external issues, interested parties, their needs and expectations, as well as legal and regulatory compliance obligations. Specifically for an ISMS, the existing interfaces and dependencies between the organization's activities and those performed by other organizations must be identified. Additional required considerations for the BCMS scope are: products, services, and organizational size, nature, and complexity. The scope and justified exclusions must be kept as "documented information." One document can be used to define scope for both standards. See a sample document here: ISMS Scope Document. For more information on this topic, see these articles: How to define the ISMS scope and Problems with defining the scope in ISO 27001.
		4.3.1	General	
		4.3.2	Scope of the BCMS	

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
4.4	Information Security Management System	4.4	Business Continuity Management System	The ISMS / BCMS should be established and operated and, by using interacting processes, be controlled and continuously improved.
5	Leadership	5	Leadership	
5.1	Leadership and commitment	5.1	Leadership and commitment	Both clauses require top management and line managers with relevant roles in the organization to demonstrate genuine effort to engage people to support their respective management system. These clauses provide many actions top management must commit to, in order to enhance the organization's levels of leadership, involvement, and cooperation in the operation of the ISMS / BCMS. For more information on this topic, please see the article: Roles and responsibilities of top management in ISO 27001 and ISO 22301.
		5.2	Management commitment	
5.2	Policy	5.3	Policy	Top management has the responsibility to establish policies, which are aligned with the organization's purposes and provide a framework for setting information security / business continuity objectives, including a commitment to fulfill applicable requirements and the continual improvement of the ISMS / BCMS and their results. Both policies must be maintained as documented information, be communicated within the organization, be available to all interested parties, and be reviewed, periodically or when significant changes occur in the organizational context. The requirements are practically the same, and in theory, they could be met through a single document. However, since they have different purposes, it is better if the policies are written as separate documents. In any case, they must be

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
				compatible with each other. See sample documents here: Information Security Policy and Business Continuity Policy. For more information on this topic, please see these articles: The purpose of business continuity policy according to ISO 22301 and What should you write in your Information Security Policy according to ISO 27001?
5.3	Organizational roles, responsibilities and authorities	5.4	Organizational roles, responsibilities and authorities	Both standards state that it is the responsibility of top management to ensure that roles, responsibilities, and authorities are delegated and communicated effectively. The responsibility must also be assigned to ensure that the ISMS / BCMS meets the terms of its respective standard, and that the ISMS / BCMS performance can be accurately reported to top management. For example, a manager, or managers, must be indicated to oversee Business continuity / Information security management activities; the same auditor can perform BCMS and ISMS audits, etc. For more information on this topic, please see these articles: What is the job of Chief Information Security Officer (CISO) in ISO 27001? and The challenging role of the ISO 22301 BCM Manager.
6	Planning	6	Planning	
6.1	Actions to address risks and opportunities	6.1	Actions to address risks and opportunities	Many similarities can be found between these requirements, as you can see below.
6.1.1	General			These clauses seek to cover the “preventive action” stated in previous versions of both standards (ISO 27001:2005 and BS-25999-2). The organization must plan actions to handle risks and opportunities relevant to the context of the organization (section 4.1) and the needs and expectations of interested parties (section 4.2), as a way to ensure that the ISMS / BCMS can

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
				achieve its intended outcomes and results, prevent or mitigate undesired consequences, and continually improve. These actions must consider their integration with ISMS / BCMS activities, as well as how effectiveness should be evaluated.
6.1.2	Information security risk assessment	8.2.3	Risk assessment	Since they are much more detailed, the ISO 27001 clauses about information security risk assessment and treatment planning can help cover the planning part required for the ISO 22301 clause regarding business continuity risk assessment. See sample document here: Risk Assessment and Risk Treatment Methodology. For more information on this topic, please see these articles: Can ISO 27001 risk assessment be used for ISO 22301? and ISO 27001 risk assessment & treatment – 6 basic steps.
6.1.3	Information security risk treatment			
6.2	Information security objectives and planning to achieve them	6.2	Business continuity objectives and planning to achieve them	Information security / Business continuity objectives should be established and communicated at appropriate levels, functions, and intervals, having considered their alignment with the information security / business continuity policy, minimum levels of delivery of products and services, the possibility of measurement, the applicable requirements, and results from business impact analysis, risk assessment, and risk treatment. The objectives must be updated when deemed necessary. They must be thought of in terms of what needs to be done, when it needs to be done by, what resources are required to achieve them, who is responsible for the objectives, and how results are to be evaluated, to ensure that objectives are being achieved and can be updated when circumstances require. These must be kept as documented information.

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
				For more information on this topic, please see these articles: ISO 27001 control objectives –Why are they important? and Setting the business continuity objectives in ISO 22301.
7	Support	7	Support	
7.1	Resources	7.1	Resources	Both standards state almost the same thing – that resources required by the ISMS / BCMS to achieve the stated objectives and show continual improvement must be defined and made available by the organization. For more information on this topic, please see this article: How to demonstrate resource provision in ISO 27001.
7.2	Competence	7.2	Competence	Requirements here are practically the same. The competence of people given responsibility for the ISMS / BCMS who work under the organization's control must meet the terms of the standards, to ensure that they are capable and confident and that their performance does not negatively affect the ISMS / BCMS. Competence can be demonstrated by experience, training, and/or education regarding the assumed tasks. When the competence is not enough, training must be identified and delivered, as well as measured to make sure the required level of competence was achieved. Evidence of competence on both standards must be kept as documented information. You can use one training plan for both standards to reduce records. See sample document here: Training and Awareness Plan.

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
				For more help with information security and business continuity training, please see the article How to perform training & awareness for ISO 27001 and ISO 22301.
7.3	Awareness	7.3	Awareness	Awareness is closely related to competence in the standard. People who work under the organization's control must be made aware of the information security / business continuity policy and its contents, what their personal performance means to the ISMS / BCMS and its objectives, and what the implications of nonconformities may be to the management systems. Additionally for the BCMS, people must be made aware of which roles they must perform during disruptive incidents. See also: 8 Security Practices to Use in Your Employee Training and Awareness Program.
7.4	Communication	7.4	Communication	Internal and external communication deemed relevant to the ISMS / BCMS must be determined, as well as the processes by which they must be effected, considering what needs to be communicated, by whom, when it should be done, and who needs to receive the communication. These requirements are the same and can be met through the same processes: e.g., writing announcements on noticeboard, sending emails, regular staff meetings, etc. Differences regarding ISO 22301 are that communication processes for internal and external communication need to be recorded as documented information, and they should consider interested parties and communication resources in disruptive events scenarios.

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
				For more help with this topic, see also: How to create a Communication Plan according to ISO 27001 and Enabling communication during disruptive incidents according to ISO 22301.
7.5	Documented information	7.5	Documented information	Both standards use the concept of "documented information," and require the management of documents and records (creation, updating, and control) – both those required by the standards and those viewed as critical by the organization to the ISMS /BCMS and its daily operation. You can apply the same procedure to meet the requirements of both standards and establish the documentation system. See sample document here: Procedure for Document and Record Control. For more help with this topic, see also: • List of mandatory documents required by ISO 27001 (2013 revision); • Mandatory documents required by ISO 22301; • Document management in ISO 27001 & BS 25999 – 2; and • Records management in ISO 27001 and ISO 22301.
7.5.1	General	7.5.1	General	
7.5.2	Creating and updating	7.5.2	Creating and updating	
7.5.3	Control of documented information	7.5.3	Control of documented information	
8	Operation	8	Operation	
8.1	Operational planning and control	8.1	Operational planning and control	General statements here are the same regarding risks and opportunities, and fulfillment of standard requirements: • processes, both internal and those outsourced deemed relevant, must be identified, planned, implemented, and controlled; • documented information deemed necessary to provide confidence that the processes are being performed and achieving their results as planned must be retained; • changes must be planned and controlled; and • impacts of unexpected changes must be evaluated, and proper actions considered.

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
		8.2	Business impact analysis and risk assessment	This ISO 22301 clause has only a partial relationship with ISO 27001, as explained below.
		8.2.1	General	These ISO 22301 clauses have no similarity with ISO 27001, but its application in ISMS planning can help optimize the allocation of resources, by defining which processes, and consequently which information, are more critical for the organization. To learn more about this topic, please see these articles Risk assessment vs. business impact analysis and How to implement business impact analysis (BIA) according to ISO 22301.
		8.2.2	Business impact analysis	
8.2	Information security risk assessment	8.2.3	Risk assessment	These ISO 27001 clauses about performing information security risk assessment and treatment can help identify: • information security risks that can impact business continuity, as well as risks that can disrupt security controls in a disaster scenario; and • actions, resources, responsibilities, and deadlines needed to prevent and handle disruptive events that are information-related. See sample documents here: Risk Assessment Table, Risk Treatment Table, and Risk Treatment Plan. For more help with this topic, see also: • ISO 27001 risk assessment: How to match assets, threats and vulnerabilities How to assess consequences and likelihood in ISO 27001 risk analysis
8.3	Information security risk treatment			

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
		8.3	Business continuity strategy	These ISO 22301 clauses have no similarity with ISO 27001, but its application in ISMS planning can help the continuity of both information systems and information security functions in case of a disruptive event, by defining which strategies, resources, and activities should be performed, as well as by means of exercising and testing, ensuring they are fit for purpose and will work when needed. See sample documents here: Business Continuity Strategy and Business Continuity Plan. For more help with this topic, see also: • Can business continuity strategy save your money? • Activation procedures for business continuity plan • Incidents in ISO 22301 vs. ISO 27001 vs. ISO 20000 vs. ISO 28003 • Business continuity plan: How to structure it according to ISO 22301 • How to perform business continuity exercising and testing according to ISO 22301
		8.3.1	Determination and selection	
		8.3.2	Establishing resource requirements	
		8.3.3	Protection and mitigation	
		8.4	Establish and implement business continuity procedures	
		8.4.1	General	
		8.4.2	Incident response structure	
		8.4.3	Warning and communication	
		8.4.4	Business continuity plans	
		8.4.5	Recovery	
		8.5	Exercising and testing	

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
9	Performance evaluation	9	Performance evaluation	
9.1	Monitoring, measurement, analysis and evaluation	9.1	Monitoring, measurement, analysis and evaluation	The requirements here are practically the same, only adjusted to cover the specific purpose of each standard: • establishment and evaluation of performance metrics regarding the effectiveness and efficiency of information security / business continuity processes, procedures, and functions; and • establishment and evaluation of performance metrics regarding ISMS / BCMS compliance with the standards, preventive actions in response to adverse trends, and the degree to which the information security / business continuity policies, objectives, and goals are being achieved.
		9.1.1	General	The methods established should take into consideration what needs to be monitored and measured, how to ensure the accuracy of results, and at what frequency to perform the monitoring, measurement, analysis, and evaluation of ISMS / BCMS data and results. Performance results must be properly retained as evidence of compliance and as a source to facilitate subsequent corrective actions.
		9.1.2	Evaluation of business continuity procedures	Although this clause is not similar to ISO 27001, its content is nothing more than a specification of clause 9.1.1, used to emphasize the importance of business continuity plans performance evaluation for ISO 22301, either by testing them, reviewing them after a disruptive event, or after significant changes in the business context.

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
9.2	Internal audit	9.2	Internal audit	The requirements here are the same. Internal audits should be performed at planned intervals, considering the processes' relevance and results of previous audits, to ensure effective implementation and maintenance, as well as compliance with the standard's requirements and any requirements defined by the organization itself. Criteria and scope for each audit must be defined. Auditors should be independent and have no conflict of interest over the audit subject. Auditors also must report the audit results to relevant management, and ensure that non-conformities are subject to the responsible managers, who in turn must ensure that any corrective measures needed are implemented in a timely manner. Finally, the auditor must also verify the effectiveness of corrective actions taken. The same procedure for internal audit can be applied for both standards. See sample document here: Internal Audit Procedure. To learn more about this topic, please see these articles: How to make an Internal Audit checklist for ISO 27001 / ISO 22301 and How to prepare for an ISO 27001 internal audit.
9.3	Management review	9.3	Management review	Although the requirement is the same, input elements for the management review are different, considering the purposes of each standard. Management review must be performed at planned intervals, at a strategic and top management level, covering the required aspects all at once or by parts, in a way that is most suitable to business needs.

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
				The status of actions defined in previous reviews, significant internal and external factors that may impact the management system, information security / business continuity performance, and opportunities for improvement should be reviewed by top management, so relevant adjustments and improvement opportunities can be implemented. The same document can be used, but it has to contain separate input elements for both standards. See sample document here: Management Review Minutes. For more details on this topic, please see the article: Why is management review important for ISO 27001 and ISO 22301?
10	Improvement	10	Improvement	
10.1	Nonconformity and corrective action	10.1	Nonconformity and corrective action	The requirements here are the same for both clauses: • Outputs from management reviews, internal audits, and compliance and performance evaluation should all be used to form the basis for nonconformities and corrective actions. • Responses to mitigate a nonconformity and/or corrective action must be proportional to its impact and the need to eliminate the root cause. • The effectiveness of actions taken must be evaluated and documented. • Continual improvement must be used to achieve and maintain the suitability, adequacy, and effectiveness of the management system regarding fulfillment of the organizations' objectives. Continual improvement can make use, with few adjustments, of the same procedure to handle non-conformity and corrective action. See sample document here: Procedure for Corrective Action. For more details on this topic, please see these articles:
10.2	Continual improvement	10.2	Continual improvement	

ISO/IEC 27001:2013		ISO 22301:2012		Explanation
				• Practical use of corrective actions for ISO 27001 and ISO 22301 • Achieving continual improvement through the use of maturity models • The blessing of continuous improvement in ISO 22301
	Annexes			
Annex A	Reference control objectives and controls			Even though ISO 22301 lists no controls, upon results of the BIA and business continuity risk assessment, practically all controls described in ISO 27001 Annex A may be applicable to ISO 22301 business continuity plans. ISO 27001 Annex A has a specific section to ensure the continuity of information security management during adverse situations, as well as the availability of information systems (controls from section A.17). For more detail on this subject, please take a look at these articles: • Overview of ISO 27001:2013 Annex A • How to structure the documents for ISO 27001 Annex A controls • How to use ISO 22301 for the implementation of business continuity in ISO 27001

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

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

Email: support@advisera.com
Phone: +1 (646) 759 9933
Toll-Free (U.S. and Canada): 1-888-553-2256
Toll-Free (United Kingdom): 0800 808 5485

EXPLORE **ADVISERA**

27001 Academy · 9001 Academy · 9100 Academy · 14001 Academy · 16949 Academy · 18001 Academy · 20000 Academy

Conformio · eTraining · AdviseraBooks

Advisera
Making certification simple.