ISO 27001 & ISO 22301 Premium Documentation Toolkit

https://advisera.com/27001academy/iso-27001-22301-premium-documentation-toolkit/

Note: The documentation should preferably be implemented in the order in which it is listed here. The order of implementation of documentation related to Annex A is defined in the Risk Treatment Plan.

No.	*Document code*	*Document name*	*Relevant clauses in the standard*	*Mandatory according to ISO 27001*	*Mandatory according to ISO 22301*
	01	**Document Management**			
1	01	Procedure for Document and Record Control	ISO 27001 7.5; A.5.33 ISO 22301 7.5		
	02	**Preparations for the Project**			
2	02	Project Plan			
	03	**Identification of Requirements**			
3	03	Procedure for Identification of Requirements	ISO 27001 4.2; A.5.31 ISO 22301 4.2		
4	03.1	Appendix 1 – List of Legal, Regulatory, Contractual and Other Requirements	ISO 27001 4.2; A.5.29; A.5.31 ISO 22301 4.2	✓*	✓
	04	**ISMS Scope**			
5	04	ISMS Scope Document	ISO 27001 4.3	✓	
	05	**General Policies**			
6	05	Information Security Policy	ISO 27001 5.2; 5.3**; 6.2; 7.4; A.6.3	✓	

No.	*Document code*	*Document name*	*Relevant clauses in the standard*	*Mandatory according to ISO 27001*	*Mandatory according to ISO 22301*
	06	**Risk Assessment and Risk Treatment**			
7	06	Risk Assessment and Risk Treatment Methodology	ISO 27001 6.1.2; 6.1.3; 8.2; 8.3 ISO 22301 8.2.1; 8.2.3	✓	
8	06.1	Appendix 1 – Risk Assessment Table	ISO 27001 6.1.2; 8.2 ISO 22301 8.2.3	✓	
9	06.2	Appendix 2 – Risk Treatment Table	ISO 27001 6.1.3; 8.3 ISO 22301 8.2.3	✓	
10	06.3	Appendix 3 – Risk Assessment and Treatment Report	ISO 27001 8.2; 8.3 ISO 22301 8.2.3	✓	
	07	**Applicability of Controls**			
11	07	Statement of Applicability	ISO 27001 6.1.3 d)	✓	
	08	**Implementation Plan**			
12	08	Risk Treatment Plan	ISO 27001 6.1.3; 6.2; 7.1; 8.3; 9.1	✓	
	09	**ISO 27001 Annex A – Security Controls**			

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
13	09.01	IT Security Policy	ISO 27001 A.5.9; A.5.10; A.5.11; A.5.14; A.5.17; A.5.32; A.6.7; A.7.7; A.7.9; A.7.10; A.8.1; A.8.7; A.8.10; A.8.12; A.8.13; A.8.19; A.8.23	✓*	
14	09.02	Clear Desk and Clear Screen Policy (Note: This can be implemented as part of the IT Security Policy.)	ISO 27001 A.7.7; A.8.1		
15	09.03	Mobile Device, Teleworking and Work from Home Policy (Note: This can be implemented as part of the IT Security Policy.)	ISO 27001 A.6.7; A.7.9; A.8.1		
16	09.04	Bring Your Own Device (BYOD) Policy	ISO 27001 A.5.14; A.6.7; A.8.1		
17	09.05	Procedures for Working in Secure Areas	ISO 27001 A.7.4; A.7.6		
18	09.06	Information Classification Policy	ISO 27001 A.5.9; A.5.10; A.5.12; A.5.13; A.5.14; A.7.10; A.8.3; A.8.5; A.8.11	✓*	
19	09.07	Inventory of Assets	ISO 27001 A.5.9		

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
20	09.08	Security Procedures for IT Department	ISO 27001 A.5.7; A.5.14; A.5.37; A.7.10; A.7.14; A.8.4; A.8.6; A.8.7; A.8.8; A.8.9; A.8.10; A.8.12; A.8.13; A.8.15; A.8.16; A.8.17; A.8.18; A.8.20; A.8.21; A.8.22; A.8.23; A.8.31; A.8.32	✔*	
21	09.09	Change Management Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO 27001 A.8.32		
22	09.10	Backup Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO 27001 A.8.13		
23	09.11	Information Transfer Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO 27001 A.5.14		
24	09.12	Disposal and Destruction Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO 27001 A.7.10; A.7.14; A.8.10		
25	09.13	Policy on the Use of Encryption	ISO 27001 A.5.31; A.8.24		

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
26	09.14	Access Control Policy	ISO 27001 A.5.15; A.5.16; A.5.17; A.5.18; A.8.2; A.8.3; A.8.4; A.8.5; A.8.11		
27	09.15	Password Policy (Note: This can be implemented as part of the Access Control Policy.)	ISO 27001 A.5.16; A.5.17; A.5.18		
28	09.16	Secure Development Policy	ISO 27001 A.5.33; A.8.11; A.8.25; A.8.26; A.8.27; A.8.28; A.8.29; A.8.30; A.8.31; A.8.32; A.8.33	✓*	
29	09.17	Appendix 1 – Specification of Information System Requirements	ISO 27001 A.8.26		
30	09.18	Supplier Security Policy	ISO 27001 A.5.7; A.5.11; A.5.19; A.5.20; A.5.21; A.5.22; A.5.23; A.6.1; A.6.2; A.6.3; A.8.30		
31	09.19	Security Clauses for Suppliers and Partners	ISO 27001 A.5.20; A.5.21; A.6.2; A.8.30		
32	09.20	Incident Management Procedure	ISO 27001 7.4; A.5.7; A.5.24; A.5.25; A.5.26; A.5.27; A.5.28; A.6.4; A.6.8	✓*	
33	09.21	Appendix 1 – Incident Log	ISO 27001 A.5.27		

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
34	09.22	Confidentiality Statement	ISO 27001 A.5.20; A.6.2; A.6.5; A.6.6	✓*	
35	09.23	Statement of Acceptance of ISMS Documents	ISO 27001 A.6.2		
	10	**ISO 22301 Core Business Continuity Documents**			
36	10.01	Business Continuity Policy	ISO 22301 4.1; 4.3; 5.2; 5.3; 6.2; 6.3; 9.1.1 ISO 27001 A.5.29		✓
37	10.02	Business Impact Analysis Methodology	ISO 22301 8.2.1, 8.2.2 ISO 27001 A.5.29		
38	10.03	Appendix 1 –Business Impact Analysis Questionnaire	ISO 22301 8.2.1, 8.2.2 ISO 27001 A.5.29		
39	10.04	Business Continuity Strategy	ISO 22301 8.3, 8.4.2 ISO 27001 A.5.5; A.5.29		
40	10.05	Appendix 1 – Recovery Time Objectives for Activities	ISO 22301 8.2.2 ISO 27001 A.5.29		
41	10.06	Appendix 2 – Examples of Disruptive Incident Scenarios	ISO 22301 8.5 ISO 27001 A.5.29		
42	10.07	Appendix 3 – Preparation Plan for Business Continuity	ISO 22301 6.2		

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
43	10.08	Appendix 4 – Activity Recovery Strategy	ISO 22301 8.3 ISO 27001 A.5.29		
44	10.09	Business Continuity Plan	ISO 22301 8.4 ISO 27001 A.5.29		✓
45	10.10	Appendix 1 – Incident Response Plan	ISO 22301 8.4.3, 8.4.4 ISO 27001 A.5.5; A.5.26; A.5.29		✓
46	10.11	Appendix 2 – Incident Log	ISO 22301 8.4.3		✓
47	10.12	Appendix 3 – List of Business Continuity Sites	ISO 22301 8.4.4 ISO 27001 A.5.29		✓
48	10.13	Appendix 4 – Transportation Plan	ISO 22301 8.3.2 ISO 27001 A.5.29		
49	10.14	Appendix 5 – Key Contacts	ISO 22301 8.4.3 ISO 27001 A.5.29		✓
50	10.15	Appendix 6 – Disaster Recovery Plan	ISO 22301 8.4.5 ISO 27001 7.4; A.5.29; A.5.30; A.8.14	✓*	✓
51	10.16	Appendix 7 – Activity Recovery Plan	ISO 22301 8.4.5 ISO 27001 A.5.29		✓
52	10.17	Exercising and Testing Plan	ISO 22301 8.5 ISO 27001 A.5.29		
53	10.18	Appendix 1 – Exercising and Testing Report	ISO 22301 8.5 ISO 27001 A.5.29		

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
54	10.19	BCMS Maintenance and Review Plan	ISO 22301 8.6 ISO 27001 A.5.29		
55	10.20	Post Incident Review Form	ISO 22301 8.6 ISO 27001 A.5.27; A.5.29		
	11	**Training & Awareness**			
56	11	Training and Awareness Plan	ISO 27001 7.2; 7.3; 7.4; A.6.3 ISO 22301 7.2; 7.3	✓	✓
	12	**Internal Audit**			
57	12	Internal Audit Procedure	ISO 27001 9.2; A.5.30; A.5.35; A.8.34 ISO 22301 9.2		
58	12.1	Appendix 1 – Annual Internal Audit Program	ISO 27001 9.2 ISO 22301 9.2	✓	✓
59	12.2	Appendix 2 – Internal Audit Report	ISO 27001 9.2 ISO 22301 9.2	✓	✓
60	12.3	Appendix 3 – Internal Audit Checklist	ISO 27001 9.2 ISO 22301 9.2		
	13	**Management Review**			
61	13.1	Measurement Report	ISO 27001 6.2; 9.1 ISO 22301 9.1; 9.3		
62	13.2	Management Review Minutes	ISO 27001 9.3 ISO 22301 9.3	✓	✓

No.	*Document code*	*Document name*	*Relevant clauses in the standard*	*Mandatory according to ISO 27001*	*Mandatory according to ISO 22301*
	14	**Corrective Actions**			
63	14	Procedure for Corrective Action	ISO 27001 10.1; A.5.27 ISO 22301 10.1		
64	14.1	Appendix 1 – Corrective Action Form	ISO 27001 10.1; 10.2 ISO 22301 10.1	✓	✓

*The listed documents are mandatory only if the corresponding controls are identified as applicable in the Statement of Applicability.

**General roles and responsibilities are described in the Information Security Policy, whereas detailed roles and responsibilities are specified in each document of this toolkit.