

## 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. The documentation for business continuity management (No. 8. A.17 in the package) is implemented in the order in which it is listed here.

Please note that some documents in this Toolkit are not mandatory – depending on the size and complexity of your company, you can choose whether to implement them or not.

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
	<b>00</b>	<b>Document Management</b>			
1	00	Procedure for Document and Record Control	ISO/IEC 27001 7.5 ISO 22301 7.5		
	<b>01</b>	<b>Preparations for the Project</b>			
2	01	Project Plan			
	<b>02</b>	<b>Identification of Requirements</b>			
3	02	Procedure for Identification of Requirements	ISO/IEC 27001 4.2, A.18.1.1 ISO 22301 4.2		
4	02.1	Appendix 1 – List of Legal, Regulatory, Contractual and Other Requirements	ISO/IEC 27001 4.2, A.18.1.1 ISO 22301 4.2	✓*	✓
	<b>03</b>	<b>ISMS Scope</b>			
5	03	ISMS Scope Document	ISO/IEC 27001 4.3	✓	
	<b>04</b>	<b>General Policies</b>			
6	04	Information Security Policy	ISO/IEC 27001 5.2, 5.3	✓	
	<b>05</b>	<b>Risk Assessment and Risk Treatment</b>			

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
7	05	Risk Assessment and Risk Treatment Methodology	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, 8.3 ISO 22301 8.2.1, 8.2.3	✓	✓
8	05.1	Appendix 1 – Risk Assessment Table	ISO/IEC 27001 6.1.2, 8.2 ISO 22301 8.2.3	✓	
9	05.2	Appendix 2 – Risk Treatment Table	ISO/IEC 27001 6.1.3, 8.3 ISO 22301 8.3.3	✓	
10	05.3	Appendix 3 – Risk Assessment and Treatment Report	ISO/IEC 27001 8.2, 8.3	✓	
	<b>06</b>	<b>Applicability of Controls</b>			
11	06	Statement of Applicability	ISO/IEC 27001 6.1.3 d)	✓	
	<b>07</b>	<b>Implementation Plan</b>			
12	07	Risk Treatment Plan	ISO/IEC 27001 6.1.3, 6.2, 8.3	✓	
	<b>08</b>	<b>Annex A – Security Controls**</b>			
	<b>A.6</b>	<b>Organization of Information Security</b>			
13	A.6.1	Bring Your Own Device (BYOD) Policy	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1		
14	A.6.2	Mobile Device and Teleworking Policy	ISO/IEC 27001 A.6.2 A.11.2.6		
	<b>A.7</b>	<b>Human Resource Security</b>			

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
15	A.7.1	Confidentiality Statement	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2	✓ *	
16	A.7.2	Statement of Acceptance of ISMS Documents	ISO/IEC 27001 A.7.1.2	✓ *	
	<b>A.8</b>	<b>Asset Management</b>			
17	A.8.1	Inventory of Assets	ISO/IEC 27001 A.8.1.1, A.8.1.2	✓ *	
18	A.8.2	IT Security Policy	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2	✓ *	
19	A.8.3	Information Classification Policy	ISO/IEC 27001 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3		
	<b>A.9</b>	<b>Access Control</b>			
20	A.9.1	Access Control Policy	ISO/IEC 27001 A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3	✓ *	

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
21	A.9.2	Password Policy (Note: it may be implemented as part of Access Control Policy)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3		
	<b>A.10</b>	<b>Cryptography</b>			
22	A.10	Policy on the Use of Encryption	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5		
	<b>A.11</b>	<b>Physical and Environmental Security</b>			
23	A.11.1	Clear Desk and Clear Screen Policy (Note: it may be implemented as part of IT Security Policy)	ISO/IEC 27001 A.11.2.8, A.11.2.9		
24	A.11.2	Disposal and Destruction Policy (Note: it may be implemented as part of Security Procedures for IT Department)	ISO/IEC 27001 A.8.3.2, A.11.2.7		
25	A.11.3	Procedures for Working in Secure Areas	ISO/IEC 27001 A.11.1.5		
	<b>A.12</b>	<b>Operations Security</b>			
26	A.12.1	Security Procedures for IT Department	ISO/IEC 27001 A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4	✔ *	

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
27	A.12.2	Change Management Policy (Note: it may be implemented as part of Security Procedures for IT Department)	ISO/IEC 27001 A.12.1.2, A.14.2.4		
28	A.12.3	Backup Policy (Note: it may be implemented as part of Security Procedures for IT Department)	ISO/IEC 27001 A.12.3.1		
	<b>A.13</b>	<b>Communications Security</b>			
29	A.13	Information Transfer Policy (Note: it may be implemented as part of Security Procedures for IT Department)	ISO/IEC 27001 A.13.2.1, A.13.2.2		
	<b>A.14</b>	<b>System Acquisition Development and Maintenance</b>			
30	A.14	Secure Development Policy	ISO/IEC A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1	✔ *	
31	A.14.1	Appendix 1 – Specification of Information System Requirements	ISO/IEC 27001 A.14.1.1	✔ *	
	<b>A.15</b>	<b>Supplier Relationships</b>			

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
32	A.15.1	Supplier Security Policy	ISO/IEC 27001 A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2		
33	A.15.2	Security Clauses for Suppliers and Partners	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3	✓ *	
	<b>A.16</b>	<b>Information Security Incident Management</b>			
34	A.16	Incident Management Procedure	ISO/IEC 27001 A.7.2.3, A.16.1.1, A.6.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7	✓ *	
35	A.16.1	Appendix 1 – Incident Log	ISO/IEC 27001 A.16.1.6		
	<b>A.17</b>	<b>Business Continuity</b>			
36	A.17.1	Business Continuity Policy	ISO 22301 4.1, 4.3, 5.3, 6.2, 9.1.1 ISO/IEC 27001 A.17.1.1		✓
37	A.17.2	Business Impact Analysis Methodology	ISO 22301 8.2.1, 8.2.2 ISO/IEC 27001 A.17.1.1		✓
38	A.17.2.1	Appendix 1 – Business Impact Analysis Questionnaire	ISO 22301 8.2.1, 8.2.2 ISO/IEC 27001 A.17.1.1		✓

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
39	A.17.3	Business Continuity Strategy	ISO 22301 8.3, 8.4.2 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓
40	A.17.3.1	Appendix 1 – List of Activities	ISO 22301 8.2.2 ISO/IEC 27001 A.17.1.1		✓
41	A.17.3.2	Appendix 2 – Recovery Priorities for Activities	ISO 22301 8.2.2 ISO/IEC 27001 A.17.1.1		✓
42	A.17.3.3	Appendix 3 – Recovery Time Objectives for Activities	ISO 22301 8.2.2 ISO/IEC 27001 A.17.1.1		✓
43	A.17.3.4	Appendix 4 – Examples of Disruptive Incident Scenarios	ISO 22301 8.5 ISO/IEC 27001 A.17.1.1		✓
44	A.17.3.5	Appendix 5 – Preparation Plan for Business Continuity	ISO 22301 6.2		✓
45	A.17.3.6	Appendix 6 – Activity Recovery Strategy	ISO 22301 8.3 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓
46	A.17.4	Business Continuity Plan	ISO 22301 8.4 ISO/IEC 27001 A.17.1.2		✓
47	A.17.4.1	Appendix 1 – Incident Response Plan	ISO 22301 8.4.3, 8.4.4 ISO/IEC 27001 A.17.1.2		✓
48	A.17.4.2	Appendix 2 – Incident Log	ISO 22301 8.4.3 ISO/IEC 27001 A.17.1.3		✓

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
49	A.17.4.3	Appendix 3 – List of Business Continuity Sites	ISO 22301 8.4.4 ISO/IEC 27001 A.17.1.2		✓
50	A.17.4.4	Appendix 4 – Transportation Plan	ISO 22301 8.3.2 ISO/IEC 27001 A.17.1.2		✓
51	A.17.4.5	Appendix 5 – Key Contacts	ISO 22301 8.4.3 ISO/IEC 27001 A.17.1.2		✓
52	A.17.4.6	Appendix 6 – Disaster Recovery Plan	ISO 22301 8.4.5 ISO/IEC 27001 A.17.1.2	✓*	✓
53	A.17.4.7	Appendix 7 – Activity Recovery Plan	ISO 22301 8.4.5 ISO/IEC 27001 A.17.1.2		✓
54	A.17.5.1	Exercising and Testing Plan	ISO 22301 8.5 ISO/IEC 27001 A.17.1.3		
55	A.17.5.2	Appendix 1 – Exercising and Testing Report	ISO 22301 8.5 ISO/IEC 27001 A.17.1.3		✓
56	A.17.5.3	BCMS Maintenance and Review Plan	ISO 22301 9.1.2 ISO/IEC 27001 A.17.1.3		
57	A.17.5.4	Post Incident Review Form	ISO 22301 9.1.2 ISO/IEC 27001 A.17.1.3, A.16.1.6		✓
	<b>09</b>	<b>Training &amp; Awareness</b>			
58	09	Training and Awareness Plan	ISO 22301 7.2, 7.3 ISO/IEC 27001 7.2, 7.3	✓	✓



No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 22301
	<b>10</b>	<b>Internal Audit</b>			
59	10	Internal Audit Procedure	ISO/IEC 27001 clause 9.2 ISO 22301 9.2		
60	10.1	Appendix 1 – Annual Internal Audit Program	ISO/IEC 27001 clause 9.2 ISO 22301 9.2	✓	✓
61	10.2	Appendix 2 – Internal Audit Report	ISO/IEC 27001 clause 9.2 ISO 22301 9.2	✓	✓
62	10.3	Appendix 3 – Internal Audit Checklist	ISO/IEC 27001 clause 9.2 ISO 22301 clause 9.2		
	<b>11</b>	<b>Management Review</b>			
63	11.1	Measurement Report	ISO/IEC 27001 clauses 6.2, 9.1 ISO 22301 clauses 6.2, 9.1	✓	
64	11.2	Management Review Minutes	ISO/IEC 27001 clause 9.3 ISO 22301 9.3	✓	✓
	<b>12</b>	<b>Corrective Actions</b>			
65	12	Procedure for Corrective Action	ISO/IEC 27001 clause 10.1 ISO 22301 10.1		
66	12.1	Appendix 1 – Corrective Action Form	ISO/IEC 27001 clause 10.1 ISO 22301 10.1	✓	✓

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



\*\*Folder "Annex A" does not include a separate folder for ISO 27001 section "A.18 – Compliance" because the documentation that covers controls from this section can be found in these folders:

- 02 – Procedure for Identification of Requirements
- 08, A.8 – Asset Management
- 08, A.10 – Cryptography