ISO 27001 & ISO 27017 & ISO 27018 Cloud Documentation Toolkit

https://advisera.com/27001academy/iso-27001-iso-27017-iso-27018-cloud-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.

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

No.	*Doc. code*	*Document name*	*Relevant clauses in the standard*	*Mandatory according to ISO 27001*	*Mandatory according to ISO 27017**	*Mandatory according to ISO 27018**
	01	**Document Management**				
1	01	Procedure for Document and Record Control	ISO 27001 7.5; A.5.33 ISO 27018 A.10.2			✓
	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 27017 18.1.1 ISO 27018 A.10.2; A.12.1		✓	✓
4	03.1	Appendix 1 – List of Legal, Regulatory, Contractual and Other Requirements	ISO 27001 4.2; A.5.29; A.5.31 ISO 27017 18.1.1 ISO 27018 A.12.1	✓**	✓	✓

No.	Doc. code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
	04	**ISMS Scope**				
5	04	ISMS Scope Document	ISO 27001 4.3	✓		
	05	**General Policies**				
6	05.1	Information Security Policy	ISO 27001 5.2; 5.3***; 6.2; 7.4; A.6.3 ISO 27017 5.1.1 ISO 27018 5.1.1; A.10.2	✓	✓	✓
7	05.2	Cloud Security Policy	ISO 27001 A.5.37; A.8.6; A.8.15; A.8.17; A.8.22; A.8.32 ISO 27017 6.1.1; 9.4.4; 12.1.3; 12.4.1; 12.4.4; 13.1.3; 18.1.2; CLD.6.3.1; CLD.9.5.1; CLD.9.5.2; CLD.12.1.5; CLD.12.4.5; CLD.13.1.4 ISO 27018 12.4.1; A.10.2		✓	✓

No.	*Doc. code*	*Document name*	*Relevant clauses in the standard*	*Mandatory according to ISO 27001*	*Mandatory according to ISO 27017**	*Mandatory according to ISO 27018**
8	05.3	Policy for Data Privacy in the Cloud	ISO 27001 A.5.1; A.5.34; A.6.2; A.6.8; A.8.15; A.8.33 ISO 27017 5.1.1; 12.4.1; 16.1.2 ISO 27018 5.1.1; 11.2.7; 12.4.1; 12.4.2; 12.4.3; 16.1.2; A.2.1; A.3.1; A.3.2; A.6.1; A.6.2; A.8.1; A.10.1; A.10.2; A.11.1; A.11.2		✓	✓
	06	**Risk Assessment and Risk Treatment**				
9	06	Risk Assessment and Risk Treatment Methodology	ISO 27001 6.1.2; 6.1.3; 8.2; 8.3 ISO 27017 4.4 ISO 27018 0.2	✓		
10	06.1	Appendix 1 – Risk Assessment Table	ISO 27001 6.1.2; 8.2	✓		
11	06.2	Appendix 2 – Risk Treatment Table	ISO 27001 6.1.3; 8.3	✓		
12	06.3	Appendix 3 – Risk Assessment and Treatment Report	ISO 27001 8.2; 8.3	✓		
	07	**Applicability of Controls**				

No.	*Doc. code*	*Document name*	*Relevant clauses in the standard*	*Mandatory according to ISO 27001*	*Mandatory according to ISO 27017**	*Mandatory according to ISO 27018**
13	07	Statement of Applicability	ISO 27001 6.1.3d) ISO 27017 all clauses from sections 5 to 18, and Annex A ISO 27018 all clauses from sections 5 to 18, and Annex A	✓		
	08	**Implementation Plan**				
14	08	Risk Treatment Plan	ISO 27001 6.1.3; 6.2; 7.1; 8.3; 9.1	✓		
	09	**Annex A – Security Controls**				
15	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 ISO 27017 5.1.1 ISO 27018 5.1.1; A.10.2	✓**	✓	✓
16	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			

No.	Doc. code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
17	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 ISO 27017 11.2.6 ISO 27018 11.2.6		✓	✓
18	09.04	Bring Your Own Device (BYOD) Policy	ISO 27001 A.5.14; A.6.7; A.8.1 ISO 27018 13.2.1; A.10.2			✓
19	09.05	Procedures for Working in Secure Areas	ISO 27001 A.7.4; A.7.6			
20	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; A.8.12 ISO 27017 15.1.2	✓**	✓	
21	09.07	Inventory of Assets	ISO 27001 A.5.9 ISO 27017 8.1.1; 8.1.2	✓**	✓	

No.	Doc. code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
22	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 ISO 27017 11.2.7; 12.1.2; 12.1.3; 12.3.1; 12.4.1; 12.4.3 ISO 27018 11.2.7; 12.1.4; 12.3.1; 12.4.1; 13.2.1; A.10.2; A.11.4; A.11.5; A.11.6; A.12.2	✓**	✓	✓
23	09.09	Change Management Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO 27001 A.8.32 ISO 27017 12.1.2 ISO 27018 A.10.2		✓	✓
24	09.10	Backup Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO 27001 A.8.13 ISO 27017 12.3.1 ISO 27018 12.3.1; A.10.2		✓	✓

No.	Doc. code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
25	09.11	Information Transfer Policy (Note: This can be implemented as part of the Security Procedures for IT Department.)	ISO 27001 A.5.14 ISO 27018 A.10.2; A.10.3; A.11.4; A.11.5			✓
26	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 ISO 27017 11.2.7 ISO 27018 11.2.7; A.10.2; A.11.7; A.11.13		✓	✓
27	09.13	Policy on the Use of Encryption	ISO 27001 A.5.31; A.8.24 ISO 27017 10.1.1; 18.1.5 ISO 27018 A.10.2; A.12.1		✓	✓

No.	Doc. code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
28	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 ISO 27017 6.1.1; 9.2.1; 9.2.2.; 9.2.3; 9.2.4; 9.2.5; 9.2.6; 9.3.1; 9.4.1; 9.4.2; 9.4.3 ISO 27018 6.1.1; 9.1; 9.2.1; 9.2.2; 9.2.3; 9.2.4; 9.2.5; 9.2.6; 9.4.2; A.10.2; A.11.8; A.11.9; A.11.10		✓	✓
29	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 ISO 27017 9.2.4 ISO 27018 9.2.1; A.10.2		✓	✓

No.	Doc. code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
30	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 ISO 27017 14.2.1; 14.2.9 ISO 27018 A.10.2	✓**	✓	✓
31	09.17	Appendix 1 – Specification of Information System Requirements	ISO 27001 A.8.26 ISO 27017 14.1.1 ISO 27018 A.5.1		✓	✓
32	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 ISO 27017 7.2.2; 15.1.2; 15.1.3; CLD.8.1.5 ISO 27018 7.2.2; A.10.2		✓	✓

No.	Doc. code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
33	09.19	Security Clauses for Clients, Suppliers and Partners	ISO 27001 A.5.20; A.5.21; A.6.2; A.6.6; A.8.30 ISO 27017 6.1.1; 6.1.3; 8.2.2; 9.2.1; 9.2.2; 9.2.4; 9.4.1; 9.4.4; 10.1.1; 11.2.7; 12.1.2; 12.1.3; 12.3.1; 12.4.1; 12.4.4; 12.6.1; 14.1.1; 14.2.1; 15.1.2; 15.1.3; 16.1.1; 16.1.2; 16.1.7; 18.1.1; 18.1.3; 18.1.5; 18.2.1; CLD.6.3.1; CLD.8.1.5 ISO 27018 5.1.1; 6.1.1; 6.1.3; 9.2; 9.4.1; 10.1.1; 12.1.4; 12.3.1; 12.4.1; 16.1; 18.2.1; A.2.1; A.6.1; A.10.1; A.11.1; A.11.3; A.11.4; A.11.5; A.11.6; A.11.11; A.11.12; A.12.1		✓	✓

No.	Doc. code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
34	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 ISO 27017 16.1.1; 16.1.2; 16.1.7; 18.1.2 ISO 27018 16.1.1; A.10.2	✓**	✓	✓
35	09.21	Appendix 1 – Incident Log	ISO 27001 A.5.27			
36	09.22	Disaster Recovery Plan	ISO 27001 7.4; A.5.29; A.5.30; A.8.14			
37	09.23	Confidentiality Statement	ISO 27001 A.5.20; A.6.2; A.6.5; A.6.6 ISO 27017 7.1.2; 13.2.4; 15.1.2 ISO 27018 7.1; 13.2.4; 15; A.11.1	✓**	✓	✓
38	09.24	Statement of Acceptance of ISMS Documents	ISO 27001 A.6.2 ISO 27017 7.1.2 ISO 27018 7.1		✓	✓
	10	**Training & Awareness**				
39	10	Training and Awareness Plan	ISO 27001 7.2; 7.3; 7.4; A.6.3	✓		
	11	**Internal Audit**				

No.	Doc. code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
40	11	Internal Audit Procedure	ISO 27001 9.2; A.5.30; A.5.35; A.8.34			
41	11.1	Appendix 1 – Annual Internal Audit Program	ISO 27001 9.2	✓		
42	11.2	Appendix 2 – Internal Audit Report	ISO 27001 9.2	✓		
43	11.3	Appendix 3 – Internal Audit Checklist	ISO 27001 9.2 ISO 27017 all clauses from sections 5 to 18, and Annex A ISO 27018 all clauses from sections 5 to 18, and Annex A		✓	✓
	12	**Management Review**				
44	12.1	Measurement Report	ISO 27001 6.2; 9.1	✓		
45	12.2	Management Review Minutes	ISO 27001 9.3	✓		
	13	**Corrective Actions**				
46	13	Procedure for Corrective Action	ISO 27001 10.1; A.5.27			
47	13.1	Appendix 1 – Corrective Action Form	ISO 27001 10.1; 10.2	✓		

*The marked documents are developed according to ISO 27017 and/or ISO 27018.

**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.