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 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 27017**	*Mandatory according to ISO 27018**
	00	**Document Management**				
1	00	Procedure for Document and Record Control	ISO/IEC 27001 7.5 ISO/IEC 27018 A.9.2			✓
	01	**Preparations for the Project**				
2	01	Project Plan				
	02	**Identification of Requirements**				
3	02	Procedure for Identification of Requirements	ISO/IEC 27001 4.2, A.18.1.1 ISO/IEC 27017 18.1.1 ISO/IEC 27018 A.9.2, A.11.1		✓	✓
4	02.1	Appendix 1 – List of Legal, Regulatory, Contractual and Other Requirements	ISO/IEC 27001 4.2, A.18.1.1 ISO/IEC 27017 18.1.1 ISO/IEC 27018 A.11.1	✓**	✓	✓

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
	03	**ISMS Scope**				
5	03	ISMS Scope Document	ISO/IEC 27001 4.3	✓		
	04	**General Policies**				
6	04.1	Information Security Policy	ISO/IEC 27001 5.2, 5.3 ISO/IEC 27017 5.1.1 ISO/IEC 27018 5.1.1, A.9.2	✓	✓	✓
7	04.2	Cloud Security Policy	ISO/IEC 27001, clauses A.12.1.1, A.12.1.3, A.12.4.1, A.12.4.3, A.12.4.4, A.13.1.3, A.14.2.4 ISO/IEC 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/IEC 27018 12.4.1, A.9.2		✓	✓

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
8	04.3	Policy for Data Privacy in the Cloud	ISO/IEC 27001 A.5.1.1, A.7.1.2, A.12.4.1, A.12.4.2, A.14.3.1, A.16.1.2, A.18.1.4 ISO/IEC 27017 5.1.1, 12.4.1, 16.1.2 ISO/IEC 27018 5.1.1, 11.2.7, 12.4.1, 12.4.2, 12.4.3, 16.1.2, A.1.1, A.2.1, A.2.2, A.5.1, A.5.2, A.7.1, A.9.1, A.9.2, A.10.1, A.10.2		✓	✓
	05	**Risk Assessment and Risk Treatment**				
9	05	Risk Assessment and Risk Treatment Methodology	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, 8.3	✓		
10	05.1	Appendix 1 – Risk Assessment Table	ISO/IEC 27001 6.1.2, 8.2	✓		
11	05.2	Appendix 2 – Risk Treatment Table	ISO/IEC 27001 6.1.3, 8.3	✓		
12	05.3	Appendix 3 – Risk Assessment and Treatment Report	ISO/IEC 27001 8.2, 8.3	✓		
	06	**Applicability of Controls**				

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
13	06	Statement of Applicability	ISO/IEC 27001 6.1.3 d) ISO 27017, all clauses from sections 5 to 18 and Annex A ISO 27018, all clauses from sections 5 to 18 and Annex A	✓	✓	✓
	07	**Implementation Plan**				
14	07	Risk Treatment Plan	ISO/IEC 27001 6.1.3, 6.2, 8.3	✓		
	08	**Annex A – Security Controls*** **				
	A.6	**Organization of Information Security**				
15	A.6.1	Bring Your Own Device (BYOD) Policy	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1 ISO/IEC 27018 13.2.1, A.9.2			✓
16	A.6.2	Mobile Device and Teleworking Policy	ISO/IEC 27001 A.6.2, A.11.2.6 ISO/IEC 27017 11.2.6 ISO/IEC 27018 11.2.6		✓	✓

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
	A.7	**Human Resource Security**				
17	A.7.1	Confidentiality Statement	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2 ISO/IEC 27017 7.1.2, 13.2.4, 15.1.2 ISO/IEC 27018 7.1, 13.2.4, 15, A.10.1	✓**	✓	✓
18	A.7.2	Statement of Acceptance of ISMS Documents	ISO/IEC 27001 A.7.1.2 ISO/IEC 27017 7.1.2 ISO/IEC 27018 7.1	✓**	✓	✓
	A.8	**Asset Management**				
19	A.8.1	Inventory of Assets	ISO/IEC 27001 A.8.1.1, A.8.1.2 ISO/IEC 27017 8.1.1, 8.1.2	✓**	✓	

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
20	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	✓**		
21	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 ISO/IEC 27017 15.1.2		✓	
	A.9	**Access Control**				

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
22	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 ISO/IEC 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/IEC 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.9.2, A.10.8, A.10.9, A.10.10	✓**	✓	✓
23	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 ISO/IEC 27017 9.2.4 ISO/IEC 27018 9.2.1, A.9.2		✓	✓
	A.10	**Cryptography**				

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
24	A.10	Policy on the Use of Encryption	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5 ISO/IEC 27017 10.1.1, 18.1.5 ISO/IEC 27018 A.9.2, A.11.1		✓	✓
	A.11	**Physical and Environmental Security**				
25	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			
26	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 ISO/IEC 27017 11.2.7 ISO/IEC 2701811.2.7, A.9.2, A.10.7, A.10.13		✓	✓
27	A.11.3	Procedures for Working in Secure Areas	ISO/IEC 27001 A.11.1.5			
	A.12	**Operations Security**				

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
28	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 ISO/IEC 27017 11.2.7, 12.1.2, 12.1.3, 12.3.1, 12.4.1, 12.4.3 ISO/IEC 27018 11.2.7, 12.1.4, 12.3.1, 12.4.1, 13.2.1, A.9.2, A.10.4, A.10.5, A.10.6, A.11.2	✓**	✓	✓
29	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 ISO/IEC 27017 12.1.2 ISO/IEC 27018 A.9.2		✓	✓

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
30	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 ISO/IEC 27017 12.3.1 ISO/IEC 27018 A.12.3.1, A.9.2		✓	✓
	A.13	**Communications Security**				
31	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 ISO/IEC 27018 A.9.2, A.9.3, A.10.4, A.10.5			✓
	A.14	**System Acquisition Development and Maintenance**				
32	A.14	Secure Development Policy	ISO/IEC 27001 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 ISO/IEC 27017 14.2.1, 14.2.9 ISO/IEC 27018 A.9.2	✓**	✓	✓

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
33	A.14.1	Appendix 1 – Specification of Information System Requirements	ISO/IEC 27001 A.14.1.1 ISO/IEC 27017 14.1.1 ISO/IEC 27018 A.4.1	✓**	✓	✓
	A.15	**Supplier Relationships**				
34	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 ISO/IEC 27017 7.2.2, 15.1.2, 15.1.3, CLD.8.1.5 ISO/IEC 27018 7.2.2, A.9.2	✓**	✓	✓

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
35	A.15.2	Security Clauses for Clients, Suppliers and Partners	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3, ISO/IEC 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/IEC 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.1.1, A.5.1, A.9.1, A.10.1, A.10.3, A.10.4, A.10.5, A.10.6, A.10.11, A.10.12, A.11.1	✓**	✓	✓

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
	A.16	**Information Security Incident Management**				
36	A.16	Incident Management Procedure	ISO/IEC 27001 A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7 ISO/IEC 27017 16.1.1, 16.1.2,16.1.7, 18.1.2 ISO/IEC 27018 16.1.1, A.9.2	✓**	✓	✓
37	A.16.1	Appendix 1 – Incident Log	ISO/IEC 27001 A.16.1.6			
	A.17	**Business Continuity**				
38	A.17	Disaster Recovery Plan	ISO/IEC 27001 A.17.1.2	✓**		
	09	**Training & Awareness**				
39	09	Training and Awareness Plan	ISO/IEC 27001 7.2, 7.3	✓		
	10	**Internal Audit**				
40	10	Internal Audit Procedure	ISO/IEC 27001 9.2			

No.	Document code	Document name	Relevant clauses in the standard	Mandatory according to ISO 27001	Mandatory according to ISO 27017*	Mandatory according to ISO 27018*
41	10.1	Appendix 1 – Annual Internal Audit Program	ISO/IEC 27001 9.2	✓		
42	10.2	Appendix 2 – Internal Audit Report	ISO/IEC 27001 9.2	✓		
43	10.3	Appendix 3 – Internal Audit Checklist	ISO/IEC 27001 9.2 ISO/IEC 27017, all clauses from sections 5 to 18 and Annex A ISO/IEC 27018, all clauses from sections 5 to 18 and Annex A		✓	✓
	11	**Management Review**				
44	11.1	Measurement Report	ISO/IEC 27001 6.2, 9.1	✓		
45	11.2	Management Review Minutes	ISO/IEC 27001 9.3	✓		
	12	**Corrective Actions**				
46	12	Procedure for Corrective Action	ISO/IEC 27001 10.1			
47	12.1	Appendix 1 – Corrective Action Form	ISO/IEC 27001 10.1	✓		

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

**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