














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.







<i>Number in the package</i>	<i>Document name</i>	<i>Relevant clauses in the Standard</i>	<i>Mandatory according to ISO 27001</i>	<i>Required by ISO 27017**</i>	<i>Required by ISO 27018**</i>
0.	Procedure for Document and Record Control	ISO/IEC 27001 7.5 ISO/IEC 27018 A.9.2			
1.	Project Plan				
2.	Procedure for Identification of Requirements	ISO/IEC 27001 4.2 and A.18.1.1 ISO/IEC 27017 18.1.1 ISO/IEC 27018 A.9.2 and A.11.1			
2.1.	Appendix – List of Legal, Regulatory, Contractual and Other Requirements	ISO/IEC 27001 4.2 and A.18.1.1 ISO/IEC 27017 18.1.1 ISO/IEC 27018 A.11.1	 *		
3.	ISMS Scope Document	ISO/IEC 27001 4.3			

Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
4.	Information Security Policy	ISO/IEC 27001 5.2 and 5.3 ISO/IEC 27017 5.1.1 ISO/IEC 27018 5.1.1 and A.9.2	✓	✓	✓
4.	Cloud Security Policy	ISO/IEC 27001 standard, 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 and CLD.13.1.4 ISO/IEC 27018 12.4.1 and A.9.2		✓	✓

Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
4.	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 and 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 and A.10.2			
5.	Risk Assessment and Risk Treatment Methodology	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, and 8.3			
5.1.	Appendix 1 – Risk Assessment Table	ISO/IEC 27001 6.1.2 and 8.2			
5.2.	Appendix 2 – Risk Treatment Table	ISO/IEC 27001 6.1.3 and 8.3			
5.3.	Appendix 3 – Risk Assessment and Treatment Report	ISO/IEC 27001 8.2 and 8.3			








Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
6.	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	✓	✓	✓
7.	Risk Treatment Plan	ISO/IEC 27001 6.1.3, 6.2 and 8.3	✓		
8.	(Annex A – controls)				
8. A.6	Bring Your Own Device (BYOD) Policy	ISO/IEC 27001 A.6.2.1, A.6.2.2 and A.13.2.1 ISO/IEC 27018 13.2.1 and A.9.2			✓
8. A.6	Mobile Device and Teleworking Policy	ISO/IEC 27001 A.6.2 and A.11.2.6 ISO/IEC 27017 11.2.6 ISO/IEC 27018 11.2.6		✓	✓

Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
8. A.7	Confidentiality Statement	ISO/IEC 27001 A.7.1.2, A.13.2.4 and A.15.1.2 ISO/IEC 27017 7.1.2, 13.2.4 and 15.1.2 ISO/IEC 27018 7.1, 13.2.4, 15 and A.10.1	 *		
8. A.7	Statement of Acceptance of ISMS Documents	ISO/IEC 27001 A.7.1.2 ISO/IEC 27017 7.1.2 ISO/IEC 27018 7.1	 *		
8. A.8	Inventory of Assets	ISO/IEC 27001 A.8.1.1 and A.8.1.2 ISO/IEC 27017 8.1.1 and 8.1.2	 *		
8. A.8	Acceptable Use 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 and A.18.1.2	 *		




Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
8. A.8	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 and A.13.2.3 ISO/IEC 27017 15.1.2			
8. A.9	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 and 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 and 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 and A.10.10			
8. A.9	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 and A.9.4.3 ISO/IEC 27017 9.2.4 ISO/IEC 27018 9.2.1 and A.9.2			








Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
8. A.10	Policy on the Use of Cryptographic Controls	ISO/IEC 27001 A.10.1.1, A.10.1.2 and A.18.1.5 ISO/IEC 27017 10.1.1 and 18.1.5 ISO/IEC 27018 A.9.2 and A.11.1		✓	✓
8. A.11	Clear Desk and Clear Screen Policy (Note: it may be implemented as part of Acceptable Use Policy)	ISO/IEC 27001 A.11.2.8 and A.11.2.9			
8. A.11	Disposal and Destruction Policy (Note: it may be implemented as part of Operating Procedures for ICT)	ISO/IEC 27001 A.8.3.2 and A.11.2.7 ISO/IEC 27017 11.2.7 ISO/IEC 27018 11.2.7, A.9.2, A.10.7 and A.10.13		✓	✓
8. A.11	Procedures for Working in Secure Areas	ISO/IEC 27001 A.11.1.5			

Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
8. A.12	Operating Procedures for Information and Communication Technology	<p>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 and A.14.2.4</p> <p>ISO/IEC 27017 11.2.7, 12.1.2, 12.1.3, 12.3.1, 12.4.1 and 12.4.3</p> <p>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 and A.11.2</p>	✓*	✓	✓
8. A.12	Change Management Policy (Note: it may be implemented as part of Operating Procedures for ICT)	<p>ISO/IEC 27001 A.12.1.2 and A.14.2.4</p> <p>ISO/IEC 27017 12.1.2</p> <p>ISO/IEC 27018 A.9.2</p>		✓	✓
8. A.12	Backup Policy (Note: it may be implemented as part of Operating Procedures for ICT)	<p>ISO/IEC 27001 A.12.3.1</p> <p>ISO/IEC 27017 12.3.1</p> <p>ISO/IEC 27018 A.12.3.1 and A.9.2</p>		✓	✓

Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
8. A.13	Information Transfer Policy (Note: it may be implemented as part of Operating Procedures for ICT)	ISO/IEC 27001 A.13.2.1, A.13.2.2 ISO/IEC 27018 A.9.2, A.9.3, A.10.4 and A.10.5			
8. 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 and A.14.3.1 ISO/IEC 27017 14.2.1 and 14.2.9 ISO/IEC 27018 A.9.2			
8. A.14	Appendix – Security Requirements Specification	ISO/IEC 27001 A.14.1.1 ISO/IEC 27017 14.1.1 ISO/IEC 27018 A.4.1			

Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
8. A.15	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 and A.15.2.2 ISO/IEC 27017 7.2.2, 15.1.2, 15.1.3 and CLD.8.1.5 ISO/IEC 27018 7.2.2 and A.9.2		✓	✓

Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
8. A.15	Appendix – Security Clauses for Clients, Suppliers and Partners	<p>ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2 and A.15.1.3,</p> <p>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 and CLD.8.1.5</p> <p>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 and A.11.1</p>			

Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
8. 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 and A.16.1.7 ISO/IEC 27017 16.1.1, 16.1.2, 16.1.7 and 18.1.2 ISO/IEC 27018 16.1.1 and A.9.2	 *		
8. A.16	Appendix – Incident Log	ISO/IEC 27001 A.16.1.6			
8. A.17	Disaster Recovery Plan	ISO/IEC 27001 A.17.1.2	 *		
9.	Training and Awareness Plan	ISO/IEC 27001 7.2 and 7.3			
10.	Internal Audit Procedure	ISO/IEC 27001 9.2			
10.1.	Appendix 1 – Annual Internal Audit Program	ISO/IEC 27001 9.2			
10.2.	Appendix 2 – Internal Audit Report	ISO/IEC 27001 9.2			

Number in the package	Document name	Relevant clauses in the Standard	Mandatory according to ISO 27001	Required by ISO 27017**	Required by ISO 27018**
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 Minutes	ISO/IEC 27001 9.3	✓		
12.	Procedure for Corrective Action	ISO/IEC 27001 10.1			
12.1.	Appendix – Corrective Action Form	ISO/IEC 27001 10.1	✓		

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

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

To learn how to fill in these documents see:

- 1) Our series of video tutorials <http://advisera.com/27001academy/documentation-tutorials/>
- 2) Our series of webinars <http://advisera.com/27001academy/webinars/>