ISO 27001 Dokumentations-Toolkit

https://advisera.com/27001academy/de/iso-27001-dokumentationspaket/

Hinweis: Die Dokumentation sollte vorzugsweise in der Reihenfolge umgesetzt werden, in der sie hier aufgeführt ist. Die Reihenfolge der Umsetzung der Dokumentation in Bezug auf Anhang A ist im Risikobehandlungsplan festgelegt.

Nr.	*Dokumentencode*	*Name des Dokumentes*	*Relevante Abschnitte in ISO 27001*	*Obligatorisch gemäß ISO 27001*
	01	**Lenkung von Dokumenten**		
1	01	Verfahren zur Lenkung von Dokumenten und Aufzeichnungen	7.5; A.5.33	
	02	**Projektvorbereitung**		
2	02	Projektplan		
	03	**Identifikation der Anforderungen**		
3	03	Verfahren zur Identifikation der Anforderungen	4.2; A.5.31	
4	03.1	Anhang 1 – Liste gesetzlicher, amtlicher, vertraglicher und anderer Anforderungen	4.2; A.5.29; A.5.31	✓*
	04	**ISMS Anwendungsbereich**		
5	04	Dokument zum ISMS Anwendungsbereich	4.3	✓
	05	**Allgemeine Politiken**		
6	05	Informationssicherheitspolitik	5.2; 5.3**; 6.2; 7.4; A.6.3	✓
	06	**Risikoeinschätzung und Risikobehandlung**		
7	06	Methodik zur Risikoeinschätzung und Risikobehandlung	6.1.2; 6.1.3; 8.2; 8.3	✓
8	06.1	Anhang 1 – Verzeichnis der Risikoeinschätzung	6.1.2; 8.2	✓

Nr.	*Dokumentencode*	*Name des Dokumentes*	*Relevante Abschnitte in ISO 27001*	*Obligatorisch gemäß ISO 27001*
9	06.2	Anhang 2 – Verzeichnis der Risikobehandlung	6.1.3; 8.3	✓
10	06.3	Anhang 3 – Bericht zur Risikoeinschätzung und Risikobehandlung	8.2; 8.3	✓
	07	**Anwendbarkeit der Maßnahmen**		
11	07	Erklärung zur Anwendbarkeit	6.1.3 d)	✓
	08	**Umsetzungsplan**		
12	08	Plan zur Risikobehandlung	6.1.3; 6.2; 7.1; 8.3; 9.1	✓
	09	**Anhang A – Sicherheitsmaßnahmen**		
13	09.01	IT-Sicherheitspolitik	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	Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm (Hinweis: Dies kann als Teil der IT-Sicherheitspolitik umgesetzt werden.)	A.7.7; A.8.1	
15	09.03	Richtlinie zu Mobilgeräten, Telearbeit und zur von zu Hause aus Arbeit (Hinweis: Dies kann als Teil der IT-Sicherheitspolitik umgesetzt werden.)	A.6.7; A.7.9; A.8.1	

Nr.	*Dokumentencode*	*Name des Dokumentes*	*Relevante Abschnitte in ISO 27001*	*Obligatorisch gemäß ISO 27001*
16	09.04	Bring Your Own Device (BYOD) Richtlinie	A.5.14; A.6.7; A.8.1	
17	09.05	Verfahren zur Arbeit in sicheren Bereichen	A.7.4; A.7.6	
18	09.06	Richtlinie zur Klassifizierung von Informationen	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	✔*
19	09.07	Inventar der Werte	A.5.9	✔*
20	09.08	Sicherheitsverfahren für die IT-Abteilung	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	Richtlinie zum Änderungsmanagement (Hinweis: Dies kann als Teil der Sicherheitsverfahren für die IT-Abteilung umgesetzt werden.)	A.8.32	
22	09.10	Backup-Richtlinie (Hinweis: Dies kann als Teil der Sicherheitsverfahren für die IT-Abteilung umgesetzt werden.)	A.8.13	

Nr.	*Dokumentencode*	*Name des Dokumentes*	*Relevante Abschnitte in ISO 27001*	*Obligatorisch gemäß ISO 27001*
23	09.11	Richtlinie zur Informationsübertragung (Hinweis: Dies kann als Teil der Sicherheitsverfahren für die IT-Abteilung umgesetzt werden.)	A.5.14	
24	09.12	Richtlinie zur Entsorgung und Vernichtung (Hinweis: Dies kann als Teil der Sicherheitsverfahren für die IT-Abteilung umgesetzt werden.)	A.7.10; A.7.14; A.8.10	
25	09.13	Richtlinie des Einsatzes von Verschlüsselung	A.5.31; A.8.24	
26	09.14	Zugangssteuerungsrichtlinie	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	Kennwort-Richtlinie (Hinweis: Dies kann als Teil der Zugangssteuerungsrichtlinie umgesetzt werden.)	A.5.16; A.5.17; A.5.18	
28	09.16	Richtlinie zur Entwicklungssicherheit	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	Anhang 1 – Spezifikation der Anforderungen an Informationssysteme	A.8.26	

Nr.	*Dokumentencode*	*Name des Dokumentes*	*Relevante Abschnitte in ISO 27001*	*Obligatorisch gemäß ISO 27001*
30	09.18	Sicherheitspolitik für Lieferanten	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	Sicherheitsabschnitte für Lieferanten und Partner	A.5.20; A.5.21; A.6.2; A.6.6; A.8.30	
32	09.20	Verfahren zum Vorfallmanagement	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	Anhang 1 – Verzeichnis der Vorfälle	A.5.27	
34	09.22	Notfallwiederherstellungsplan	7.4; A.5.29; A.5.30; A.8.14	
35	09.23	Vertraulichkeitserklärung	A.5.20; A.6.2; A.6.5; A.6.6	✓*
36	09.24	Erklärung zur Akzeptanz von ISMS Dokumenten	A.6.2	
	10	**Training & Awareness**		
37	10	Plan für Training und Awareness	7.2; 7.3; 7.4; A.6.3	✓
	11	**Internes Audit**		
38	11	Verfahren für interne Audits	9.2; A.5.30; A.5.35; A.8.34	
39	11.1	Anhang 1 – Jährliches internes Audit- Programm	9.2	✓

Nr.	*Dokumentencode*	*Name des Dokumentes*	*Relevante Abschnitte in ISO 27001*	*Obligatorisch gemäß ISO 27001*
40	11.2	Anhang 2 – Interner Audit-Bericht	9.2	✓
41	11.3	Anhang 3 – Interne Audit-Checkliste	9.2	
	12	**Managementbewertung**		
42	12.1	Messbericht	6.2; 9.1	✓
43	12.2	Protokoll zur Managementbewertung	9.3	✓
	13	**Korrekturmaßnahmen**		
44	13	Verfahren zu Korrekturmaßnahmen	10.1; A.5.27	
45	13.1	Anhang 1 – Formblatt der Korrekturmaßnahmen	10.1; 10.2	✓

* Die aufgeführten Dokumente sind nur dann obligatorisch, wenn die entsprechenden Maßnahmen in der Erklärung zur Anwendbarkeit als anwendbar gekennzeichnet sind.

** Allgemeine Rollen und Verantwortlichkeiten sind in der Informationssicherheitspolitik beschrieben, während detaillierte Rollen und Verantwortlichkeiten in jedem Dokument dieses Toolkits aufgeführt sind.