ISO 27001 & ISO 22301 Premium Dokumentations-Toolkit

https://advisera.com/27001academy/de/iso-27001-a-iso-22301-premium-dokumentationspaket/

Anmerkung: Die Dokumentation sollte vorzugsweise in der hier aufgelisteten Reihenfolge umgesetzt werden. Die Umsetzungs-Reihenfolge der Dokumentation mit Bezug zu Anhang A ist im Risikobehandlungsplan definiert. Die Dokumentation für betriebliches Kontinuitätsmanagement (Nr. 08, A.17 im Toolkit) wird in der hier aufgelisteten Reihenfolge durchgeführt.

Bitte beachten Sie, dass einige in diesem Toolkit enthaltene Dokumente nicht zwingend vorgeschrieben sind. Abhängig von der Größe und Komplexität Ihrer Firma, haben Sie die Wahl, ob Sie diese umsetzen möchten oder nicht.

Nr.	*Dok. Code im Toolkit*	*Name des Dokumentes*	*Relevante Abschnitte in der Norm*	*Pflicht gem. ISO 27001*	*Pflicht gem. ISO 22301*
	00	**Lenkung von Dokumenten**			
1	00	Verfahren zur Lenkung von Dokumenten und Aufzeichnungen	ISO/IEC 27001 7.5 ISO 22301 7.5		
	01	**Projektvorbereitung**			
2	01	Projektplan			
	02	**Identifikation der Anforderungen**			
3	02	Verfahren zur Identifikation der Anforderungen	ISO/IEC 27001 4.2, A.18.1.1 ISO 22301 4.2		
4	02.1	Anhang 1 – Liste gesetzlicher, amtlicher, vertraglicher und anderer Anforderungen	ISO/IEC 27001 4.2, A.18.1.1 ISO 22301 4.2	✓*	✓
	03	**ISMS Anwendungsbereich**			
5	03	Dokument zum ISMS Anwendungsbereich	ISO/IEC 27001 4.3	✓	
	04	**Allgemeine Politiken**			
6	04	Informationssicherheitspolitik	ISO/IEC 27001 4.2, 5.3	✓	

Nr.	Dok. Code im Toolkit	Name des Dokumentes	Relevante Abschnitte in der Norm	Pflicht gem. ISO 27001	Pflicht gem. ISO 22301
	05	**Risikoeinschaetzung und Risikobehandlung**			
7	05	Methodik zur Risikoeinschätzung und Risikobehandlung	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, 8.3 ISO 22301 8.2.1, 8.2.3	✓	✓
8	05.1	Anhang 1 – Verzeichnis der Risikoeinschätzung	ISO/IEC 27001 6.1.2, 8.2 ISO 22301 8.2.3	✓	
9	05.2	Anhang 2 – Verzeichnis der Risikobehandlung	ISO/IEC 27001 6.1.3, 8.3 ISO 22301 8.3.3	✓	
10	05.3	Anhang 3 – Bericht zur Risikoeinschätzung und Risikobehandlung	ISO/IEC 27001 8.2, 8.3	✓	
	06	**Erklärung zur Anwendbarkeit**			
11	06	Erklärung zur Anwendbarkeit	ISO/IEC 27001 6.1.3 d)	✓	
	07	**Plan zur Risikobehandlung**			
12	07	Plan zur Risikobehandlung	ISO/IEC 27001 6.1.3, 6.2, 8.3	✓	
	08	**Anhang A – Sicherheitsmaßnahmen****			
	A.6	**Organisierung der Informationssicherheit**			
13	A.6.1	Bring Your Own Device (BYOD) Richtlinie	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1		
14	A.6.2	Richtlinie zu Mobilgeräten und Telearbeit	ISO/IEC 27001 A.6.2 A.11.2.6		

Nr.	Dok. Code im Toolkit	Name des Dokumentes	Relevante Abschnitte in der Norm	Pflicht gem. ISO 27001	Pflicht gem. ISO 22301
	A.7	**Personelle Sicherheit**			
15	A.7.1	Vertraulichkeitserklärung	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2	✓*	
16	A.7.2	Erklärung zur Akzeptanz von ISMS-Dokumenten	ISO/IEC 27001 A.7.1.2	✓*	
	A.8	**Management von Werten**			
17	A.8.1	Inventar der Werte	ISO/IEC 27001 A.8.1.1, A.8.1.2	✓*	
18	A.8.2	IT-Sicherheitspolitik	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	Richtlinie zur Klassifizierung von Informationen	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		
	A.9	**Zugangssteuerung**			
20	A.9.1	Zugangssteuerungsrichtlinie	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	✓*	

Nr.	Dok. Code im Toolkit	Name des Dokumentes	Relevante Abschnitte in der Norm	Pflicht gem. ISO 27001	Pflicht gem. ISO 22301
21	A.9.2	Kennwort-Richtlinie (Anmerkung: Sie kann auch als Teil der Zugangssteuerungs-richtlinie umgesetzt werden)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3		
	A.10	**Kryptographie**			
22	A.10	Richtlinie des Einsatzes von Verschlüsselung	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5		
	A.11	**Physische und Umgebungs Sicherheit**			
23	A.11.1	Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm (Anmerkung: Sie kann auch als Teil der IT-Sicherheitspolitik umgesetzt werden)	ISO/IEC 27001 A.11.2.8, A.11.2.9		
24	A.11.2	Richtlinie zur Entsorgung und Vernichtung (Anmerkung: Sie kann auch als Teil des Sicherheitsverfahrens für die IT-Abteilung umgesetzt werden)	ISO/IEC 27001 A.8.3.2, A.11.2.7		
25	A.11.3	Verfahren zur Arbeit in sicheren Bereichen	ISO/IEC 27001 A.11.1.5		
	A.12	**Betriebssicherheit**			
26	A.12.1	Sicherheitsverfahren für die IT-Abteilung	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	✓*	

Nr.	Dok. Code im Toolkit	Name des Dokumentes	Relevante Abschnitte in der Norm	Pflicht gem. ISO 27001	Pflicht gem. ISO 22301
27	A.12.2	Richtlinie zum Änderungs-management (Anmerkung: Sie kann auch als Teil des Sicherheitsverfahrens für die IT-Abteilung umgesetzt werden)	ISO/IEC 27001 A.12.1.2, A.14.2.4		
28	A.12.3	Backup-Richtlinie (Anmerkung: Sie kann auch als Teil des Sicherheitsverfahrens für die IT-Abteilung umgesetzt werden)	ISO/IEC 27001 A.12.3.1		
	A.13	**Kommunikations-sicherheit**			
29	A.13	Richtlinie zur Informations-übertragung (Anmerkung: Sie kann auch als Teil des Sicherheitsverfahrens für die IT-Abteilung umgesetzt werden)	ISO/IEC 27001 A.13.2.1, A.13.2.2		
	A.14	**Systembeschaffung, Entwicklung und Wartung**			
30	A.14	Richtlinie zur Entwicklungssicherheit	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	Anhang 1 – Spezifikation der Sicherheitsanforderungen	ISO/IEC 27001 A.14.1.1		
	A.15	**Beziehungen zu Lieferanten**			
32	A.15.1	Sicherheitspolitik für Lieferanten	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	✓*	

Nr.	Dok. Code im Toolkit	Name des Dokumentes	Relevante Abschnitte in der Norm	Pflicht gem. ISO 27001	Pflicht gem. ISO 22301
33	A.15.2	Sicherheitsabschnitte für Lieferanten und Partner	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3	✓*	
	A.16	**Informationssicherheits Vorfallsmanagement**			
34	A.16	Verfahren zum Vorfallsmanagement	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	Anhang 1 – Verzeichnis der Vorfälle	ISO/IEC 27001 A.16.1.6		
	A.17	**Kontinuitätsmanagement**			
36	A.17.1	Richtlinie zum betrieblichen Kontinuitätsmanagement	ISO 22301 8.2.1, 8.2.2 ISO/IEC 27001 A.17.1.1		✓
37	A.17.2	Methodik der Geschäftauswirkungsanalyse (GAA)	ISO 22301 8.2.2 ISO/IEC 27001 A.17.1.1		✓
38	A.17.2.1	Anhang 1 – Fragebogen zur Geschäftsauswirkungsanalyse (GAA)	ISO 22301 8.2.1, 8.2.2 ISO/IEC 27001 A.17.1.1		✓
39	A.17.3	Strategie für betriebliches Kontinuitätsmanagement	ISO 22301 8.3, 8.4.2 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓
40	A.17.3.1	Anhang 1 – Zielvorgaben der Recovery-Zeiten für Tätigkeiten	ISO 22301 8.2.2 ISO/IEC 27001 A.17.1.1		✓

Nr.	Dok. Code im Toolkit	Name des Dokumentes	Relevante Abschnitte in der Norm	Pflicht gem. ISO 27001	Pflicht gem. ISO 22301
41	A.17.3.2	Anhang 2 – Beispiele für Szenarien von Vorfällen	ISO 22301 8.5 ISO/IEC 27001 A.17.1.1		✓
42	A.17.3.3	Anhang 3 – Vorbereitungsplan für betriebliches Kontinuitätsmanagement	ISO 22301 6.2		✓
43	A.17.3.4	Anhang 4 – Strategie zur Tätigkeiten-Recovery	ISO 22301 8.3 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓
44	A.17.4	Plan für betriebliches Kontinuitätsmanagement	ISO 22301 8.4 ISO/IEC 27001 A.17.1.2	✓	✓
45	A.17.4.1	Anhang 1 – Vorfallreaktionsplan	ISO 22301 8.4.3, 8.4.4 ISO/IEC 27001 A.17.1.2	✓	✓
46	A.17.4.2	Anhang 2 – Vorfallprotokoll	ISO 22301 8.4.3 ISO/IEC 27001 A.17.1.3		✓
47	A.17.4.3	Anhang 3 – Liste der Standorte betrieblichen Kontinuitäts-managements	ISO 22301 8.4.4 ISO/IEC 27001 A.17.1.2		✓
48	A.17.4.4	Anhang 4 – Transportplan	ISO 22301 8.3.2 ISO/IEC 27001 A.17.1.2		✓
49	A.17.4.5	Anhang 5 – Schlüsselkontakte für betriebliches Kontinuitätsmanagement	ISO 22301 8.4.3 ISO/IEC 27001 A.17.1.2		✓
50	A.17.4.6	Anhang 6 – Notfall-wiederherstellungsplan	ISO 22301 8.4.5 ISO/IEC 27001 A.17.1.2	✓*	✓

Nr.	Dok. Code im Toolkit	Name des Dokumentes	Relevante Abschnitte in der Norm	Pflicht gem. ISO 27001	Pflicht gem. ISO 22301
51	A.17.4.7	Anhang 7 – Recovery-Plan für Tätigkeiten	ISO 22301 8.4.5 ISO/IEC 27001 A.17.1.2	✓	✓
52	A.17.5.1	Übungs- und Testplan	ISO 22301 8.5 ISO/IEC 27001 A.17.1.3		
53	A.17.5.2	Anhang 1 – Formblatt für den Übungs- und Testbericht	ISO 22301 8.5 ISO/IEC 27001 A.17.1.3		✓
54	A.17.5.3	Wartungs- und Überprüfungsplan für das BKMS	ISO 22301 9.1.2 ISO/IEC 27001 A.17.1.3		
55	A.17.5.4	Überprüfungsformular zur Anwendung nach Vorfällen	ISO 22301 9.1.2 ISO/IEC 27001 A.17.1.3, A.16.1.6		✓
	09	**Training und Awareness**			
56	09	Plan für Training und Awareness	ISO 22301 7.2, 7.3 ISO/IEC 27001 7.2, 7.3	✓	✓
	10	**Internes Audit**			
57	10	Verfahren für interne Audits	ISO/IEC 27001 9.2 ISO 22301 9.2		
58	10.1	Anhang 1 – Internes Audit-Programm	ISO/IEC 27001 9.2 ISO 22301 9.2	✓	✓
59	10.2	Anhang 2 – Interner Audit-Bericht	ISO/IEC 27001 9.2 ISO 22301 9.2	✓	✓
60	10.3	Anhang 3 – Interne Audit-Checkliste	ISO/IEC 27001 9.2 ISO 22301 9.2		
	11	**Managementbewertung**			

Nr.	*Dok. Code im Toolkit*	*Name des Dokumentes*	*Relevante Abschnitte in der Norm*	*Pflicht gem. ISO 27001*	*Pflicht gem. ISO 22301*
61	11.1	Messbericht	ISO/IEC 27001 6.2, 9.1 ISO 22301 9.1, 9.3	✓	
62	11.2	Protokoll zur Managementbewertung	ISO/IEC 27001 9.3 ISO 22301 9.3	✓	✓
	12	**Korrekturmaßnahmen**			
63	12	Verfahren zu Korrekturmaßnahmen	ISO/IEC 27001 10.1 ISO 22301 10.1		
64	12.1	Anhang 1 – Formblatt der Korrekturmaßnahmen	ISO/IEC 27001 10.1 ISO 22301 10.1	✓	✓

* Die aufgelisteten Dokumente sind nur verpflichtend sofern die entsprechenden Maßnahmen in der Erklärung zur Anwendbarkeit als durchzuführende Maßnahmen identifiziert sind.

**Der Ordner „Anhang A“ enthält keinen gesonderten Ordner für den ISO 27001-Abschnitt „A.18 - Compliance“, da die Dokumentation, die sich auf die Maßnahen aus diesem Abschnitt bezieht, in diesen Ordnern zu finden ist:

- 02 – Verfahren zur Identifikation der Anforderungen
- 08, A.8 – Management von Werten
- 08, A.10 – Kryptographie