

ISO 27001 & ISO 22301 Premium Documentatie Toolkit

<https://advisera.com/27001academy/nl/iso-27001-iso-22301-premium-documentatie-toolkit/>

Opmerking: De documentatie dient bij voorkeur geïmplementeerd te worden in de volgorde waarin het is vermeld. De volgorde van de implementatie in relatie tot Bijlage A is gedefinieerd in het Plan voor Risicobehandeling.

Nr.	Doc. code	Document naam	Relevante clausules in de norm	Verplicht volgens ISO 27001	Verplicht volgens ISO 22301
	01	Documentbeheer			
1	01	Procedure voor Beheersing van Documenten en Registraties	ISO 27001 7.5; A.5.33 ISO 22301 7.5		
	02	Vorbereidingen voor het Project			
2	02	Projectplan			
	03	Identificatie van Vereisten			
3	03	Procedure voor Identificatie van Vereisten	ISO 27001 4.2; A.5.31 ISO 22301 4.2		
4	03.1	Bijlage 1 - Lijst van Wettelijke, Reglementaire, Contractuele en Andere Vereisten	ISO 27001 4.2; A.5.29; A.5.31 ISO 22301 4.2	✓ *	✓
	04	ISMS Toepassingsgebied			
5	04	Document Toepassingsgebied ISMS	ISO 27001 4.3	✓	
	05	Algemene Beleiden			
6	05	Informatiebeveiligingsbeleid	ISO 27001 5.2; 5.3**; 6.2; 7.4; A.6.3	✓	
	06	Risicobeoordeling en Risicobehandeling			
7	06	Methodologie voor Risicobeoordeling en Risicobehandeling	ISO 27001 6.1.2; 6.1.3; 8.2; 8.3 ISO 22301 8.2.1; 8.2.3	✓	

Nr.	Doc. code	Document naam	Relevante clausules in de norm	Verplicht volgens ISO 27001	Verplicht volgens ISO 22301
8	06.1	Bijlage 1 – Tabel voor Risicobeoordeling	ISO 27001 6.1.2; 8.2 ISO 22301 8.2.3	✓	
9	06.2	Bijlage 2 – Tabel voor Risicobehandeling	ISO 27001 6.1.3; 8.3 ISO 22301 8.2.3	✓	
10	06.3	Bijlage 3 – Rapport van Risicobeoordeling en Risicobehandeling	ISO 27001 8.2; 8.3 ISO 22301 8.2.3	✓	
	07	Toepasselijkheid van Beheersmaatregelen			
11	07	Verklaring van Toepasselijkheid	ISO 27001 6.1.3 d)	✓	
	08	Implementatieplan			
12	08	Plan voor Risicobehandeling	ISO 27001 6.1.3; 6.2; 7.1; 8.3; 9.1	✓	
	09	ISO 27001 Bijlage A – Beveiligingsbeheersmaatregelen			
13	09.01	IT-Beveiligingsbeleid	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	✓ *	
14	09.02	Clear Desk en Clear Screen Beleid (Opmerking: dit kan worden geïmplementeerd als onderdeel van het IT-Beveiligingsbeleid.)	ISO 27001 A.7.7; A.8.1		
15	09.03	Beleid voor Draagbare Apparaten, Telewerken en Thuiswerken (Opmerking: dit kan worden geïmplementeerd als onderdeel van het IT-Beveiligingsbeleid.)	ISO 27001 A.6.7; A.7.9; A.8.1		

Nr.	Doc. code	Document naam	Relevante clauses in de norm	Verplicht volgens ISO 27001	Verplicht volgens ISO 22301
16	09.04	Beleid voor Bring Your Own Device (BYOD)	ISO 27001 A.5.14; A.6.7; A.8.1		
17	09.05	Procedures voor Werken in Beveiligde Ruimtes	ISO 27001 A.7.4; A.7.6		
18	09.06	Informatie Classificatie Beleid	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	✓ *	
19	09.07	Inventarisatie van Bedrijfsmiddelen	ISO 27001 A.5.9	✓ *	
20	09.08	Beveiligingsprocedures voor de IT-Afdeling	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	✓ *	
21	09.09	Beleid voor Wijzigingsbeheer (Opmerking: dit kan geïmplementeerd worden als onderdeel van de Beveiligingsprocedures voor de IT-Afdeling.)	ISO 27001 A.8.32		
22	09.10	Beleid voor Back-up (Opmerking: dit kan geïmplementeerd worden als onderdeel van de Beveiligingsprocedures voor de IT-Afdeling.)	ISO 27001 A.8.13		
23	09.11	Beleid voor Informatieoverdracht (Opmerking: dit kan worden geïmplementeerd als onderdeel van de Beveiligingsprocedures voor de IT-Afdeling.)	ISO 27001 A.5.14		

Nr.	Doc. code	Document naam	Relevante clausules in de norm	Verplicht volgens ISO 27001	Verplicht volgens ISO 22301
24	09.12	Beleid voor Verwijdering en Vernietiging (Opmerking: dit kan geïmplementeerd worden als onderdeel van de Beveiligingsprocedures voor de IT Afdeling.)	ISO 27001 A.7.10; A.7.14; A.8.10		
25	09.13	Beleid inzake het Gebruik van Encryptie	ISO 27001 A.5.31; A.8.24		
26	09.14	Toegangsbeleid	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		
27	09.15	Wachtwoordenbeleid (Opmerking: dit kan geïmplementeerd worden als onderdeel van het Toegangsbeleid.)	ISO 27001 A.5.16; A.5.17; A.5.18		
28	09.16	Beleid voor Beveiligde Ontwikkeling	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	✓ *	
29	09.17	Bijlage 1 – Specificatie van de Vereisten voor Informatiesystemen	ISO 27001 A.8.26		
30	09.18	Beveiligingsbeleid Leverancier	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		
31	09.19	Beveiligingsclausules voor Leveranciers en Partners	ISO 27001 A.5.20; A.5.21; A.6.2; A.6.6; A.8.30		
32	09.20	Procedure voor Incidentbeheer	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	✓ *	
33	09.21	Bijlage 1 - Incidentlogboek	ISO 27001 A.5.27		
34	09.22	Geheimhoudingsverklaring	ISO 27001 A.5.20; A.6.2; A.6.5; A.6.6	✓ *	

Nr.	Doc. code	Document naam	Relevante clausules in de norm	Verplicht volgens ISO 27001	Verplicht volgens ISO 22301
35	09.23	Verklaring van Aanvaarding van ISMS-Documenten	ISO 27001 A.6.2		
	10	ISO 22301 Kerndocumenten voor Bedrijfscontinuïteit			
36	10.01	Bedrijfscontinuïteitsbeleid	ISO 22301 4.1; 4.3; 5.2; 5.3; 6.2; 6.3; 9.1.1 ISO 27001 A.5.29		✓
37	10.02	Methodologie voor Business Impact Analyse	ISO 22301 8.2.1, 8.2.2 ISO 27001 A.5.29		
38	10.03	Bijlage 1 – Vragenlijst voor Business Impact Analyse	ISO 22301 8.2.1, 8.2.2 ISO 27001 A.5.29		
39	10.04	Bedrijfscontinuïteitsstrategie	ISO 22301 8.3, 8.4.2 ISO 27001 A.5.5; A.5.29		
40	10.05	Bijlage 1 – Hersteltijd doelstellingen voor Activiteiten	ISO 22301 8.2.2 ISO 27001 A.5.29		
41	10.06	Bijlage 2 – Voorbeelden van Versturende Incidentscenario's	ISO 22301 8.5 ISO 27001 A.5.29		
42	10.07	Bijlage 3 – Voorbereidingsplan voor Bedrijfscontinuïteit	ISO 22301 6.2		
43	10.08	Bijlage 4 – Herstelstrategie voor Activiteiten	ISO 22301 8.3 ISO 27001 A.5.29		
44	10.09	Bedrijfscontinuïteitsplan	ISO 22301 8.4 ISO 27001 A.5.29		✓
45	10.10	Bijlage 1 – Plan voor Respons bij Incidenten	ISO 22301 8.4.3, 8.4.4 ISO 27001 A.5.5; A.5.26; A.5.29		✓
46	10.11	Bijlage 2 – Incidentlogboek	ISO 22301 8.4.3		✓

Nr.	Doc. code	Document naam	Relevante clausules in de norm	Verplicht volgens ISO 27001	Verplicht volgens ISO 22301
47	10.12	Bijlage 3 – Lijst van Bedrijfscontinuïteits Locaties	ISO 22301 8.4.4 ISO 27001 A.5.29		✓
48	10.13	Bijlage 4 – Vervoersplan	ISO 22301 8.3.2 ISO 27001 A.5.29		
49	10.14	Bijlage 5 – Belangrijke Contacten	ISO 22301 8.4.3 ISO 27001 A.5.29		✓
50	10.15	Bijlage 6 – Rampenherstelplan	ISO 22301 8.4.5 ISO 27001 7.4; A.5.29; A.5.30; A.8.14	✓*	✓
51	10.16	Bijlage 7 – Herstelplan voor Activiteiten	ISO 22301 8.4.5 ISO 27001 A.5.29		✓
52	10.17	Oefen- en Testplan	ISO 22301 8.5 ISO 27001 A.5.29		
53	10.18	Bijlage 1 – Oefen- en Testrapport	ISO 22301 8.5 ISO 27001 A.5.29		
54	10.19	BCMS Onderhouds- en Beoordelingsplan	ISO 22301 8.6 ISO 27001 A.5.29		
55	10.20	Post Incident Beoordelingsformulier	ISO 22301 8.6 ISO 27001 A.5.27; A.5.29		
	11	Training & Bewustzijn			
56	11	Plan voor Training en Bewustzijn	ISO 27001 7.2; 7.3; 7.4; A.6.3 ISO 22301 7.2; 7.3	✓	✓
	12	Interne Audit			

Nr.	Doc. code	Document naam	Relevante clausules in de norm	Verplicht volgens ISO 27001	Verplicht volgens ISO 22301
57	12	Interne Audit Procedure	ISO 27001 9.2; A.5.30; A.5.35; A.8.34 ISO 22301 9.2		
58	12.1	Bijlage 1 - Jaarlijkse Interne Auditprogramma	ISO 27001 9.2 ISO 22301 9.2	✓	✓
59	12.2	Bijlage 2 – Rapport voor Interne Audit	ISO 27001 9.2 ISO 22301 9.2	✓	✓
60	12.3	Bijlage 3 – Checklist Interne Audit	ISO 27001 9.2 ISO 22301 9.2		
	13	Directiebeoordeling			
61	13.1	Meetrapport	ISO 27001 6.2; 9.1 ISO 22301 9.1; 9.3	✓	
62	13.2	Notulen van de Directiebeoordeling	ISO 27001 9.3 ISO 22301 9.3	✓	✓
	14	Corrigerende Maatregelen			
63	14	Procedure voor Corrigerende Maatregelen	ISO 27001 10.1; A.5.27 ISO 22301 10.1		
64	14.1	Bijlage 1 – Formulier voor Corrigerende Maatregelen	ISO 27001 10.1; 10.2 ISO 22301 10.1	✓	✓

* De vermelde documenten zijn alleen verplicht indien de corresponderende beheersmaatregelen zijn aangegeven als van toepassing in de Verklaring van Toepasselijkheid.

** Algemene rollen en verantwoordelijkheden worden beschreven in het Informatiebeveiligingsbeleid, terwijl gedetailleerde rollen en verantwoordelijkheden worden gespecificeerd in elk document van deze toolkit.