

ISO 27001 i ISO 22301 Premium paket dokumentacije

<https://advisera.com/27001academy/hr/iso-27001-iso-22301-premium-paket-dokumentacije/>

Napomena: Ako je moguće, dokumentaciju bi trebalo implementirati redoslijedom kojim je ovdje navedena. Redoslijed implementacije dokumentacije vezane uz Aneks A utvrđen je Planom obrade rizika.

Br.	Kod dok.	Naslov dokumenta	Relevantne točke norme	Obvezan prema ISO 27001	Obvezan prema ISO 22301
	01	Upravljanje dokumentima			
1	01	Procedura za upravljanje dokumentima i zapisima	ISO 27001 7.5; A.5.33 ISO 22301 7.5		
	02	Pripreme za projekt			
2	02	Projektni plan			
	03	Identifikacija zahtjeva			
3	03	Procedura za identifikaciju zahtjeva	ISO 27001 4.2; A.5.31 ISO 22301 4.2		
4	03.01	Prilog 1 – Popis pravnih, regulatornih, ugovornih i ostalih zahtjeva	ISO 27001 4.2; A.5.29; A.5.31 ISO 22301 4.2	✓ *	✓
	04	Opseg ISMS-a			
5	04	Odluka o opsegu ISMS-a	ISO 27001 4.3	✓	
	05	Opće politike			
6	05	Politika informacijske sigurnosti	ISO 27001 5.2; 5.3**; 6.2; 7.4; A.6.3	✓	
	06	Procjena i obrada rizika			
7	06	Metodologija za procjenu i obradu rizika	ISO 27001 6.1.2; 6.1.3; 8.2; 8.3 ISO 22301 8.2.1; 8.2.3	✓	

Br.	Kod dok.	Naslov dokumenta	Relevantne točke norme	Obvezan prema ISO 27001	Obvezan prema ISO 22301
8	06.01	Prilog 1 – Tablica procjene rizika	ISO 27001 6.1.2; 8.2 ISO 22301 8.2.3	✓	
9	06.02	Prilog 2 – Tablica obrade rizika	ISO 27001 6.1.3; 8.3 ISO 22301 8.2.3	✓	
10	06.03	Prilog 3 – Izvješće o procjeni i obradi rizika	ISO 27001 8.2; 8.3 ISO 22301 8.2.3	✓	
	07	Primjenjivost mjera			
11	07	Izvješće o primjenjivosti	ISO 27001 6.1.3 d)	✓	
	08	Plan implementacije			
12	08	Plan obrade rizika	ISO 27001 6.1.3; 6.2; 7.1; 8.3; 9.1	✓	
	09	ISO 27001 Aneks A – sigurnosne mjere			
13	09.01	Politika sigurnosti informacijskog sustava	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	Politika čistog stola i čistog ekrana (Napomena: Može se implementirati kao dio Politike sigurnosti informacijskog sustava.)	ISO 27001 A.7.7; A.8.1		
15	09.03	Politika mobilnih uređaja, rada na daljinu i rada od kuće (Napomena: Može se implementirati kao dio Politike sigurnosti informacijskog sustava.)	ISO 27001 A.6.7; A.7.9; A.8.1		
16	09.04	Politika korištenja vlastitih uređaja (BYOD)	ISO 27001 A.5.14; A.6.7; A.8.1		
17	09.05	Procedure za rad u sigurnim područjima	ISO 27001 A.7.4; A.7.6		

Br.	Kod dok.	Naslov dokumenta	Relevantne točke norme	Obvezan prema ISO 27001	Obvezan prema ISO 22301
18	09.06	Politika klasifikacije informacija	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	Popis resursa	ISO 27001 A.5.9	✓ *	
20	09.08	Sigurnosne procedure za IT odjel	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	Politika upravljanja promjenama (Napomena: Može se implementirati kao dio Sigurnosnih procedura za IT odjel.)	ISO 27001 A.8.32		
22	09.10	Politika sigurnosnih kopija (Napomena: Može se implementirati kao dio Sigurnosnih procedura za IT odjel.)	ISO 27001 A.8.13		
23	09.11	Politika prijenosa informacija (Napomena: Može se implementirati kao dio Sigurnosnih procedura za IT odjel.)	ISO 27001 A.5.14		
24	09.12	Politika odlaganja i uništavanja (Napomena: Može se implementirati kao dio Sigurnosnih procedura za IT odjel.)	ISO 27001 A.7.10; A.7.14; A.8.10		
25	09.13	Politika o uporabi enkripcije	ISO 27001 A.5.31; A.8.24		
26	09.14	Politika kontrole pristupa	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		

Br.	Kod dok.	Naslov dokumenta	Relevantne točke norme	Obvezan prema ISO 27001	Obvezan prema ISO 22301
27	09.15	Politika uporabe lozinki (Napomena: Može se implementirati kao dio Politike kontrole pristupa.)	ISO 27001 A.5.16; A.5.17; A.5.18		
28	09.16	Politika sigurnog razvoja	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	Prilog 1 – Specifikacija zahtjeva za informacijski sustav	ISO 27001 A.8.26		
30	09.18	Politika sigurnosti dobavljača	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	Sigurnosne klauzule za dobavljače i partnere	ISO 27001 A.5.20; A.5.21; A.6.2; A.6.6; A.8.30		
32	09.20	Procedura za upravljanje incidentima	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	Prilog 1 – Dnevnik incidenata	ISO 27001 A.5.27		
34	09.22	Izjava o povjerljivosti	ISO 27001 A.5.20; A.6.2; A.6.5; A.6.6	✓ *	
35	09.23	Izjava o prihvaćanju dokumenata ISMS-a	ISO 27001 A.6.2		
	10	ISO 22301 temeljni dokumenti za kontinuitet poslovanja			
36	10.01	Politika kontinuiteta poslovanja	ISO 22301 4.1; 4.3; 5.2; 5.3; 6.2; 6.3; 9.1.1 ISO 27001 A.5.29		✓

Br.	Kod dok.	Naslov dokumenta	Relevantne točke norme	Obvezan prema ISO 27001	Obvezan prema ISO 22301
37	10.02	Metodologija analize utjecaja na poslovanje	ISO 22301 8.2.1, 8.2.2 ISO 27001 A.5.29		
38	10.03	Prilog 1 – Upitnik analize utjecaja na poslovanje	ISO 22301 8.2.1, 8.2.2 ISO 27001 A.5.29		
39	10.04	Strategija kontinuiteta poslovanja	ISO 22301 8.3, 8.4.2 ISO 27001 A.5.5; A.5.29		
40	10.05	Prilog 1 – Ciljana vremena oporavka za aktivnosti	ISO 22301 8.2.2 ISO 27001 A.5.29		
41	10.06	Prilog 2 – Primjeri scenarija za incidente koji remete poslovanje	ISO 22301 8.5 ISO 27001 A.5.29		
42	10.07	Prilog 3 – Plan priprema za kontinuitet poslovanja	ISO 22301 6.2		
43	10.08	Prilog 4 – Strategija oporavka za aktivnost	ISO 22301 8.3 ISO 27001 A.5.29		
44	10.09	Plan kontinuiteta poslovanja	ISO 22301 8.4 ISO 27001 A.5.29		✓
45	10.10	Prilog 1 – Plan odziva na incident	ISO 22301 8.4.3, 8.4.4 ISO 27001 A.5.5; A.5.26; A.5.29		✓
46	10.11	Prilog 2 – Dnevnik incidenata	ISO 22301 8.4.3		✓
47	10.12	Prilog 3 – Popis lokacija za kontinuitet poslovanja	ISO 22301 8.4.4 ISO 27001 A.5.29		✓
48	10.13	Prilog 4 – Plan transporta	ISO 22301 8.3.2 ISO 27001 A.5.29		
49	10.14	Prilog 5 – Ključni kontakti	ISO 22301 8.4.3 ISO 27001 A.5.29		✓

Br.	Kod dok.	Naslov dokumenta	Relevantne točke norme	Obvezan prema ISO 27001	Obvezan prema ISO 22301
50	10.15	Prilog 6 – Plan oporavka od katastrofe	ISO 22301 8.4.5 ISO 27001 7.4; A.5.29; A.5.30; A.8.14	✓ *	✓
51	10.16	Prilog 7 – Plan oporavka za aktivnost	ISO 22301 8.4.5 ISO 27001 A.5.29		✓
52	10.17	Plan vježbanja i testiranja	ISO 22301 8.5 ISO 27001 A.5.29		
53	10.18	Prilog 1 – Izvješće o vježbanju i testiranju	ISO 22301 8.5 ISO 27001 A.5.29		
54	10.19	Plan održavanja i pregledavanja BCMS-a	ISO 22301 8.6 ISO 27001 A.5.29		
55	10.20	Obrazac pregleda nakon incidenta	ISO 22301 8.6 ISO 27001 A.5.27; A.5.29		
	11	Obučavanje i osvježavanje			
56	11	Plan obučavanja i osvježavanja	ISO 27001 7.2; 7.3; 7.4; A.6.3 ISO 22301 7.2; 7.3	✓	✓
	12	Interni audit			
57	12	Procedura za interni audit	ISO 27001 9.2; A.5.30; A.5.35; A.8.34 ISO 22301 9.2		
58	12.01	Prilog 1 – Godišnji program internih audita	ISO 27001 9.2 ISO 22301 9.2	✓	✓
59	12.02	Prilog 2 – Izvješće o internom auditu	ISO 27001 9.2 ISO 22301 9.2	✓	✓

Br.	Kod dok.	Naslov dokumenta	Relevantne točke norme	Obvezan prema ISO 27001	Obvezan prema ISO 22301
60	12.03	Prilog 3 – Kontrolni popis za interni audit	ISO 27001 9.2 ISO 22301 9.2		
	13	Pregled od strane menadžmenta			
61	13.01	Izvešće o mjerenju	ISO 27001 6.2; 9.1 ISO 22301 9.1; 9.3	✓	
62	13.02	Zapisnik s pregleda od strane menadžmenta	ISO 27001 9.3 ISO 22301 9.3	✓	✓
	14	Popravne radnje			
63	14	Procedura za popravnu radnju	ISO 27001 10.1; A.5.27 ISO 22301 10.1		
64	14.01	Prilog 1 – Obrazac za popravnu radnju	ISO 27001 10.1; 10.2 ISO 22301 10.1	✓	✓

* Navedeni dokumenti su obvezni jedino ako su sigurnosne mjere kojima pripadaju označene kao primjenjive kroz Izvešće o primjenjivosti.

** Opće uloge i odgovornosti opisane su u Politici informacijske sigurnosti, dok su detaljne uloge i odgovornosti navedene u svakom dokumentu ovog Paketa.