ISO 27001 & ISO 22301 Premium paket dokumentacije

http://www.iso27001standard.com/hr/usluge/iso-27001-bs-25999-premium-paket-dokumentacije

Napomene: dokumentaciju je najbolje implementirati redoslijedom kojim je navedena u ovom popisu. Redoslijed implementacije dokumentacije vezane za Aneks A se određuje kroz Plan obrade rizika. Dokumentacija za upravljanje kontinuitetom poslovanja (broj 8. A.17 u paketu) se implementira redoslijedom kojim je navedena u ovom popisu.

Imajte na umu, da neki dokumenti u ovom paketu nisu obvezni, ovisno o veličini i složenosti vašeg poduzeća možete odabrati, hoćete li ih implementirati ili ne.

Broj u paketu	***Naziv dokumenta***	***Sukladan točkama norme***	***Dokument je obvezan po ISO 27001***	***Dokument je obvezan po ISO 22301***	***Dokument je obvezan po BS 25999-2***
0.	Procedura za upravljanje dokumentacijom i zapisima	ISO/IEC 27001 ¸7.5 ISO 22301 7.5 BS 25999-2 3.4.2, 3.4.3			✓
1.	Projektni plan				
2.	Procedura za identifikaciju zahtjeva	ISO/IEC 27001 4.2 i A.18.1.1 ISO 22301 4.2			
2.1.	Popis pravnih, regulatornih, ugovornih i ostalih zahtjeva	ISO/IEC 27001 4.2 i A.18.1.1 ISO 22301 4.2	✓*	✓	
3.	Odluka o opsegu ISMS-a	ISO/IEC 27001 4.3	✓		
4.	Politika informacijske sigurnosti	ISO/IEC 27001 5.2 i 5.3	✓		
5.	Metodologija za procjenu i obradu rizika	ISO/IEC 270016.1.2, 6.1.3, 8.2 i 8.3 ISO 22301 8.2.1, 8.2.3 BS 25999-2 4.1.2.1	✓	✓	✓
5.1.	Prilog 1 – Tablica procjene rizika	ISO/IEC 27001 6.1.2 i 8.2 ISO 22301 8.2.3	✓		

Broj u paketu	*Naziv dokumenta*	*Sukladan točkama norme*	*Dokument je obvezan po ISO 27001*	*Dokument je obvezan po ISO 22301*	*Dokument je obvezan po BS 25999-2*
		BS 25999-2 4.1.2			
5.2.	Prilog 2 – Tablica obrade rizika	ISO/IEC 27001 6.1.3 i 8.3 ISO 23301 8.3.3 BS 25999-2 4.1.3.1	✓		
5.3.	Prilog 3 – Izvješće o procjeni i obradi rizika	ISO/IEC 27001 8.2 i 8.3	✓		
6.	Izvješće o primjenjivosti	ISO/IEC 27001 6.1.3 d)	✓		
7.	Plan obrade rizika	ISO/IEC 27001 6.1.3, 6.2 i 8.3	✓		
8.	(Aneks A – kontrole)				
8. A.6	Politika korištenja vlastitih uređaja (BYOD)	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1			
8. A.6	Politika mobilnih uređaja i rada na daljinu	ISO/IEC 27001 A.6.2 A.11.2.6			
8. A.7	Izjava o povjerljivosti	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2	✓*		
8. A.7	Izjava o prihvaćanju dokumenata ISMS-a	ISO/IEC 27001 A.7.1.2	✓*		
8. A.8	Popis resursa	ISO/IEC 27001 A.8.1.1, A.8.1.2	✓*		
8. A.8	Politika pravilne uporabe	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,	✓*		

Broj u paketu	*Naziv dokumenta*	*Sukladan točkama norme*	*Dokument je obvezan po ISO 27001*	*Dokument je obvezan po ISO 22301*	*Dokument je obvezan po BS 25999-2*
		A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2			
8. A.8	Politika klasifikacije informacija	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			
8. A.9	Politika kontrole pristupa	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	✓*		
8. A.9	Politika uporabe lozinki (napomena: može biti implementirana kao dio Politike kontrole pristupa)	ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3			
8. A.10	Politika uporabe kriptografskih kontrola	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5			
8. A.11	Politika čistog stola i čistog ekrana (napomena: može biti implementirana kao dio Politike pravilne uporabe	ISO/IEC 27001 A.11.2.8, A.11.2.9			
8. A.11	Politika uklanjanja i uništavanja (napomena: može biti implementirana kao dio Operativnih	ISO/IEC 27001 A.8.3.2, A.11.2.7			

Broj u paketu	*Naziv dokumenta*	*Sukladan točkama norme*	*Dokument je obvezan po ISO 27001*	*Dokument je obvezan po ISO 22301*	*Dokument je obvezan po BS 25999-2*
	procedura za informacijsku i komunikacijsku tehnologiju)				
8. A.11	Procedure za rad u sigurnim područjima	ISO/IEC 27001 A.11.1.5			
8. A.12	Operativne procedure za informacijsku i komunikacijsku tehnologiju	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	✓*		
8. A.12	Politika upravljanja promjenama (napomena: može biti implementirana kao dio Operativnih procedura za informacijsku i komunikacijsku tehnologiju)	ISO/IEC 27001 A.12.1.2, A.14.2.4			
8. A.12	Politika sigurnosnih kopija (napomena: Može biti implementirana kao dio Operativnih procedura za informacijsku i komunikacijsku tehnologiju)	ISO/IEC 27001 A.12.3.1			
8. A.13	Politika prijenosa informacija (napomena: Može biti implementirana kao dio Operativnih	ISO/IEC 27001 A.13.2.1, A.13.2.2			

Broj u paketu	*Naziv dokumenta*	*Sukladan točkama norme*	*Dokument je obvezan po ISO 27001*	*Dokument je obvezan po ISO 22301*	*Dokument je obvezan po BS 25999-2*
	procedura za informacijsku i komunikacijsku tehnologiju)				
8. A.14	Politika sigurnog razvoja	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, A.14.3.1	✓*		
8. A.14	Specifikacija zahtjeva za informacijski sustav	ISO/IEC 27001 A.14.1.1	✓*		
8. A.15	Politika sigurnosti dobavljača	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			
8. A.15	Prilog – Sigurnosne klauzule za dobavljače i partnere	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3	✓*		
8. A.16	Procedura za upravljanje incidentima	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	✓*		
8. A.16	Prilog – Jedinstveni popis incidenata	ISO/IEC 27001 A.16.1.6			
8. A.17 1.	Politika kontinuiteta poslovanja	ISO 22301 4.1, 4.3, 5.3, 6.2, 9.1.1 BS 25999-2 3.2.1, 3.2.2, 3.2.3 ISO/IEC 27001 A.17.1.1		✓	✓

Broj u paketu	*Naziv dokumenta*	*Sukladan točkama norme*	*Dokument je obvezan po ISO 27001*	*Dokument je obvezan po ISO 22301*	*Dokument je obvezan po BS 25999-2*
8. A.17 2.	Metodologija analize utjecaja na poslovanje	ISO 22301 8.2.1, 8.2.2 BS 25999-2 4.1.1 ISO/IEC 27001 A.17.1.1		✓	
8. A.17 2.1.	Upitnik analize utjecaja na poslovanje	ISO 22301 8.2.1, 8.2.2 BS 25999-2 4.1.1 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.	Strategija kontinuiteta poslovanja	ISO 22301 8.3, 8.4.2 BS 25999-2 4.2 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓	✓
8. A.17 3.1.	Prilog 1 – Popis svih aktivnosti	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.2.	Prilog 2 – Prioriteti oporavka za aktivnosti	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.3.	Prilog 3 – Ciljana vremena oporavka za aktivnosti	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.4.	Prilog 4 – Primjeri scenarija za prekid poslovanja	ISO 22301 8.5 BS 25999-2 4.1.2.2 ISO/IEC 27001 A.17.1.1		✓	
8. A.17 3.5.	Prilog 5 – Plan priprema za kontinuitet poslovanja	ISO 22301 6.2 BS 25999-2 3.2.3.1		✓	✓

Broj u paketu	*Naziv dokumenta*	*Sukladan točkama norme*	*Dokument je obvezan po ISO 27001*	*Dokument je obvezan po ISO 22301*	*Dokument je obvezan po BS 25999-2*
8. A.17 3.6.	Prilog 6 – Strategija oporavka aktivnosti	ISO 22301 8.3 BS 25999-2 4.2 ISO/IEC 27001 A.17.1.1, A.17.2.1		✓	✓
8. A.17 4.	Plan kontinuiteta poslovanja	ISO 22301 8.4 BS 25999-2 4.3 ISO/IEC 27001 A.17.1.2	✓	✓	✓
8. A.17 4.1.	Prilog 1 – Plan odziva na incidente	ISO 22301 8.4.3, 8.4.4 BS 25999-2 4.3.2 ISO/IEC 27001 A.17.1.2	✓	✓	✓
8. A.17 4.2.	Prilog 2 – Jedinstveni popis incidenata	ISO 22301 8.4.3 BS 25999-2 4.3.2 ISO/IEC 27001 A.17.1.3		✓	✓
8. A.17 4.3.	Prilog 3 – Popis lokacija za kontinuitet poslovanja	ISO 22301 8.4.4 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.4.	Prilog 4 – Plan transporta	ISO 22301 8.3.2 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.5.	Prilog 5 – Kontakt podaci ključnih osoba	ISO 22301 8.4.3 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.6.	Prilog 6 – Plan oporavka za aktivnost	ISO 22301 8.4.5 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2	✓	✓	✓

Broj u paketu	*Naziv dokumenta*	*Sukladan točkama norme*	*Dokument je obvezan po ISO 27001*	*Dokument je obvezan po ISO 22301*	*Dokument je obvezan po BS 25999-2*
8. A.17 5.1.	Plan vježbanja i testiranja kontinuiteta poslovanja	ISO 22301 8.5 BS 25999-2 4.4.2 ISO/IEC 27001 A.17.1.3			✓
8. A.17 5.2.	Prilog – Obrazac – Izvješće sa provedene vježbe i testiranja	ISO 22301 8.5 BS 25999-2 4.4.2.2 ISO/IEC 27001 A.17.1.3		✓	✓
8. A.17 5.3.	Plan održavanja i pregledavanja BCMS-a	ISO 22301 9.1.2 BS 25999-2 4.4.3 ISO/IEC 27001 A.17.1.3			✓
8. A.17 5.4.	Obrazac pregleda nakon incidenta	ISO 22301 9.1.2 BS 25999-2 4.4.3.4 ISO/IEC 27001 A.17.1.3, A.16.1.6		✓	✓
9.	Plan obučavanja i osvješćivanja	ISO 22301 7.2, 7.3 BS 25999-2 3.2.4, 3.3 ISO/IEC 27001 7.2, 7.3	✓	✓	✓
10.	Procedura za interni audit	ISO/IEC 27001 9.2 ISO 22301 9.2 BS 25999-2 5.1			✓
10.1.	Prilog 1 – Godišnji plan internih audita	ISO/IEC 27001 9.2 ISO 22301 9.2 BS 25999-2 5.1	✓	✓	✓
10.2.	Prilog 2 – Izvješće o internom auditu	ISO/IEC 27001 9.2 ISO 22301 9.2 BS 25999-2 5.1	✓	✓	✓
10.3.	Prilog 3 – Kontrolni popis za interni audit	ISO/IEC 27001 9.2 ISO 22301 9.2			

Broj u paketu	*Naziv dokumenta*	*Sukladan točkama norme*	*Dokument je obvezan po ISO 27001*	*Dokument je obvezan po ISO 22301*	*Dokument je obvezan po BS 25999-2*
11.	Zapisnik sa pregleda od strane menadžmenta	ISO/IEC 27001 9.3 ISO 22301 9.3 BS 25999-2 5.2	✓	✓	✓
12.	Procedura za korektivne mjere	ISO/IEC 27001 10.1 ISO 22301 10.1 BS 25999-2 6.1			✓
12.1.	Prilog – Obrazac za korektivnu mjeru	ISO/IEC 27001 10.1 ISO 22301 10.1 BS 25999-2 6.1	✓	✓	✓

*Navedeni dokumenti su obvezni jedino ukoliko su kontrole kojima pripadaju propisane kao primjenjive kroz Izvješće o primjenjivosti

Za pomoć oko ispunjavanja ovih dokumenata pogledajte:

1) Našu seriju video tutorijala http://www.iso27001standard.com/video-tutorijali
2) Naše webinare http://www.iso27001standard.com/webinari