


Pakiet Dokumentacji Premium dla ISO 27001 oraz ISO 22301


Uwaga: Wdrażanie dokumentacji powinno w miarę możliwości być realizowane w kolejności podanej poniżej. Kolejność wdrażania dokumentacji związanej z Aneksem A jest określona w Planie postępowania z ryzykiem. Dokumentacja związana z zarządzaniem ciągłością działania (Nr 8. A.17 w pakiecie) jest wdrażana w kolejności podanej poniżej. Należy zwrócić uwagę, że nie wszystkie dokumenty zawarte w Pakiecie Dokumentacji Premium dla ISO 27001 oraz ISO 22301 są obowiązkowe – można podjąć decyzję o ich zastosowaniu w zależności od wielkości i stopnia złożoności organizacji.

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiązkowy zgodnie z ISO 27001	Obowiązkowy zgodnie z ISO 22301	Obowiązkowy zgodnie z BS 25999-2
0.	Procedura zarządzania dokumentami i rejestrami	ISO/IEC 27001 7.5 ISO 22301 7.5 BS 25999-2 3.4.2, 3.4.3			✓
1.	Plan projektu				
2.	Procedura identyfikacji wymagań	ISO/IEC 27001 4.2 oraz A.18.1.1 ISO 22301 4.2			
2.1.	Załącznik – Lista wymagań prawnych, branżowych, umownych i innych	ISO/IEC 27001 4.2 oraz A.18.1.1 ISO 22301 4.2	✓*	✓	
3.	Zakres SZBI	ISO/IEC 27001 4.3	✓		
4.	Polityka bezpieczeństwa informacji	ISO/IEC 27001 5.2 oraz 5.3	✓		

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001	Obowiazkowy zgodnie z ISO 22301	Obowiazkowy zgodnie z BS 25999-2
5.	Metodyka szacowania i postepowania z ryzykiem	ISO/IEC 27001 6.1.2, 6.1.3, 8.2, oraz 8.3 ISO 22301 8.2.1, 8.2.3 BS 25999-2 4.1.2.1	✓	✓	✓
5.1.	Załącznik 1 – Tabela szacowania ryzyka	ISO/IEC 27001 6.1.2 oraz 8.2 ISO 22301 8.2.3 BS 25999-2 4.1.2	✓		
5.2.	Załącznik 2 – Tabela postepowania z ryzykiem	ISO/IEC 27001 6.1.3 oraz 8.3 ISO 22301 8.3.3 BS 25999-2 4.1.3.1	✓		
5.3.	Załącznik 3 – Raport z szacowania i postepowania z ryzykiem	ISO/IEC 27001 8.2 oraz 8.3	✓		
6.	Deklaracja stosowania	ISO/IEC 27001 6.1.3 d)	✓		
7.	Plan postepowania z ryzykiem	ISO/IEC 27001 6.1.3, 6.2 oraz 8.3	✓		
8.	(Aneks A – zabezpieczenia)				
8. A.6	Polityka uzytkowania własnych urzadzzeń elektronicznych (Polityka BYOD)	ISO/IEC 27001 A.6.2.1, A.6.2.2, A.13.2.1			

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001	Obowiazkowy zgodnie z ISO 22301	Obowiazkowy zgodnie z BS 25999-2
8. A.6	Polityka użytkowania urządzeń mobilnych i telepracy	ISO/IEC 27001 A.6.2 A.11.2.6			
8. A.7	Zobowiązanie do zachowania poufności	ISO/IEC 27001 A.7.1.2, A.13.2.4, A.15.1.2	✓*		
8. A.7	Zobowiązanie do stosowania polityk i procedur SZBI	ISO/IEC 27001 A.7.1.2	✓*		
8. A.8	Inwentaryzacja aktywów	ISO/IEC 27001 A.8.1.1, A.8.1.2	✓*		
8. A.8	Polityka akceptowalnego użytkowania	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	✓*		
8. A.8	Polityka klasyfikacji informacji	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			

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001	Obowiazkowy zgodnie z ISO 22301	Obowiazkowy zgodnie z BS 25999-2
8. A.9	Polityka kontroli dostępu	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	Polityka zarządzania hasłami (Uwaga: może być częścią Polityki kontroli dostępu)	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	Polityka stosowania zabezpieczeń kryptograficznych	ISO/IEC 27001 A.10.1.1, A.10.1.2, A.18.1.5			
8. A.11	Polityka czystego biurka i czystego ekranu (Uwaga: może być częścią Polityki akceptowalnego użytkownika)	ISO/IEC 27001 A.11.2.8, A.11.2.9			
8. A.11	Polityka usuwania i niszczenia informacji (Uwaga: może być częścią Procedur operacyjnych dla systemów teleinformatycznych)	ISO/IEC 27001 A.8.3.2, A.11.2.7			
8. A.11	Procedury pracy w strefach bezpieczeństwa	ISO/IEC 27001 A.11.1.5			

Numer w pakiecie	Nazwa dokumentu	Odnoszące sekcje norm	Obowiązkowy zgodnie z ISO 27001	Obowiązkowy zgodnie z ISO 22301	Obowiązkowy zgodnie z BS 25999-2
8. A.12	Procedury operacyjne dla systemów teleinformatycznych	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	Polityka zarządzania zmianami (Uwaga: może być częścią Procedur operacyjnych dla systemów teleinformatycznych)	ISO/IEC 27001 A.12.1.2, A.14.2.4			
8. A.12	Polityka zarządzania kopiami zapasowymi (Uwaga: może być częścią Procedur operacyjnych dla systemów teleinformatycznych)	ISO/IEC 27001 A.12.3.1			
8. A.13	Polityka przekazywania informacji (Uwaga: może być częścią Procedur operacyjnych dla systemów teleinformatycznych)	ISO/IEC 27001 A.13.2.1, A.13.2.2			

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001	Obowiazkowy zgodnie z ISO 22301	Obowiazkowy zgodnie z BS 25999-2
8. A.14	Polityka bezpiecznego rozwoju systemów	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	✓*		
8. A.14	Załącznik – Specyfikacja wymagań dla systemu przetwarzania informacji	ISO/IEC 27001 A.14.1.1	✓*		
8. A.15	Polityka bezpieczeństwa dotycząca dostawców	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	Załącznik – Klauzule bezpieczeństwa dla dostawców i partnerów	ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3	✓*		

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001	Obowiazkowy zgodnie z ISO 22301	Obowiazkowy zgodnie z BS 25999-2
8. A.16	Procedura zarządzania incydentami	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	Załącznik – Dziennik incydentów	ISO/IEC 27001 A.16.1.6			
8. A.17 1.	Polityka ciągłości działania	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		✓	✓
8. A.17 2.	Metodyka analizy wpływu na działalność	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.	Załącznik – Kwestionariusz analizy wpływu na działalność	ISO 22301 8.2.1, 8.2.2 BS 25999-2 4.1.1 ISO/IEC 27001 A.17.1.1		✓	✓

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001	Obowiazkowy zgodnie z ISO 22301	Obowiazkowy zgodnie z BS 25999-2
8. A.17 3.	Strategia ciągłości działania	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.	Załącznik 1 – Lista działań	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.2.	Załącznik 2 – Priorytety odtwarzania działań	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.3.	Załącznik 3 – Docelowe okresy odtworzenia działań	ISO 22301 8.2.2 BS 25999-2 4.1.1.2 ISO/IEC 27001 A.17.1.1		✓	✓
8. A.17 3.4.	Załącznik 4 – Przykładowe scenariusze incydentów	ISO 22301 8.5 BS 25999-2 4.1.2.2 ISO/IEC 27001 A.17.1.1		✓	
8. A.17 3.5.	Załącznik 5 – Plan przygotowań do zachowania ciągłości działania	ISO 22301 6.2 BS 25999-2 3.2.3.1		✓	✓

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001	Obowiazkowy zgodnie z ISO 22301	Obowiazkowy zgodnie z BS 25999-2
8. A.17 3.6.	Załącznik 6 – Strategia odtworzenia dzialan	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 zapewnienia ciaglosci dzialania	ISO 22301 8.4 BS 25999-2 4.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.1.	Załącznik 1 – Plan reagowania na incydenty	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.	Załącznik 2 – Dziennik incydentow	ISO 22301 8.4.3 BS 25999-2 4.3.2 ISO/IEC 27001 A.17.1.3		✓	✓
8. A.17 4.3.	Załącznik 3 – Lista obiektow sluzacych zachowaniu ciaglosci dzialania	ISO 22301 8.4.4 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.4.	Załącznik 4 – Plan transportu	ISO 22301 8.3.2 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001	Obowiazkowy zgodnie z ISO 22301	Obowiazkowy zgodnie z BS 25999-2
8. A.17 4.5.	Załącznik 5 – Kluczowe kontakty	ISO 22301 8.4.3 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 4.6.	Załącznik 6 – Plan odtworzenia po katastrofie	ISO 22301 8.4.5 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2	✓ *	✓	✓
8. A.17 4.7.	Załącznik 7 – Plan odtworzenia działań	ISO 22301 8.4.5 BS 25999-2 4.3.3 ISO/IEC 27001 A.17.1.2		✓	✓
8. A.17 5.1.	Plan ćwiczeń i testów	ISO 22301 8.5 BS 25999-2 4.4.2 ISO/IEC 27001 A.17.1.3			✓
8. A.17 5.2.	Załącznik – Formularz – Raport z ćwiczeń i testów	ISO 22301 8.5 BS 25999-2 4.4.2.2 ISO/IEC 27001 A.17.1.3		✓	✓
8. A.17 5.3.	Plan obsługi i przeglądów BCMS	ISO 22301 9.1.2 BS 25999-2 4.4.3 ISO/IEC 27001 A.17.1.3			✓

Numer w pakiecie	Nazwa dokumentu	Odnosne sekcje norm	Obowiazkowy zgodnie z ISO 27001	Obowiazkowy zgodnie z ISO 22301	Obowiazkowy zgodnie z BS 25999-2
8. A.17 5.4.	Formularz przeglądu po incydencie	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 szkolenia i uświadamiania	ISO 22301 7.2, 7.3 BS 25999-2 3.2.4, 3.3 ISO/IEC 27001 7.2, 7.3	✓	✓	✓
10.	Procedura audytu wewnętrznego	ISO/IEC 27001 sekcja 9.2 ISO 22301 9.2 BS 25999-2 5.1			✓
10.1.	Załącznik 1 – Roczny program audytu wewnętrznego	ISO/IEC 27001 sekcja 9.2 ISO 22301 9.2 BS 25999-2 5.1	✓	✓	✓
10.2.	Załącznik 2 – Raport z audytu wewnętrznego	ISO/IEC 27001 sekcja 9.2 ISO 22301 9.2 BS 25999-2 5.1	✓	✓	✓
10.3.	Załącznik 3 – Lista kontrolna audytu wewnętrznego	ISO/IEC 27001 sekcja 9.2 ISO 22301 sekcja 9.2			
11.	Protokół z przeglądu dokonanego przez kierownictwo	ISO/IEC 27001 sekcja 9.3 ISO 22301 9.3 BS 25999-2 5.2	✓	✓	✓

Numer w pakiecie	Nazwa dokumentu	Oдноśne sekcje norm	Obowiązkowy zgodnie z ISO 27001	Obowiązkowy zgodnie z ISO 22301	Obowiązkowy zgodnie z BS 25999-2
12.	Procedura działań naprawczych	ISO/IEC 27001 sekcja 10.1 ISO 22301 10.1 BS 25999-2 6.1			✓
12.1.	Załącznik – Formularz działania naprawczego	ISO/IEC 27001 sekcja 10.1 ISO 22301 10.1 BS 25999-2 6.1	✓	✓	✓

*Podane dokumenty są obowiązkowe tylko wtedy, jeśli odnośne zabezpieczenia są wskazane do zastosowania w Zakresie SZBI.

Aby zobaczyć, jak wypełniać wymienione wyżej dokumenty, zapoznaj się z:

- 1) Naszymi wideo-szkoleniami <http://advisera.com/27001academy/documentation-tutorials/>
- 2) Naszymi seminariami internetowymi <http://advisera.com/27001academy/webinars/>