PCBC

Czy Twoja organizacja jest gotowa na proces certyfikacji zgodnie z aktualną wersją normy ISO/IEC 27001?

CERTYFIKACJA. BADANIA. SZKOLENIA.

PCBC

31.10.2025 r. kończy się okres przejściowy dla normy ISO/IEC 27001.

Wszystkie organizacje chcące posiadać certyfikację w zakresie bezpieczeństwa informacji mają dokładnie rok, aby dostosować się do wymagań znowelizowanej normy.

Nasza cheklista pomoże samodzielnie zweryfikować stopień gotowości organizacji do przejścia lub certyfikacji na zgodność z PN-EN ISO/IEC 27001:2023-08 oraz zidentyfikować obszary, które mogą skutkować niezgodnościami podczas procesu certyfikacji.

Zanim przejdziesz do checklisty....

- Czy dokonano analizy luk dotyczących zmian w ISO/IEC 27001?
- Czy opracowano plan wdrożenia?
- Czy zidentyfikowano procesy i dokumenty Organizacji, na które wpływa zmiana w ISO/IEC 27001 oraz, jeśli ma to zastosowanie, systemy informatyczne wykorzystywane w certyfikowanej działalności?
- Czy zapewniono właściwe szkolenia i świadomość wszystkich stron, które mają wpływ na skuteczność systemu zarządzania bezpieczeństwem informacji Organizacji?
- Czy zapewniono weryfikację skuteczności wdrożenia zmian poprzez przeprowadzenie auditu wewnętrznego?

23 pytania, które pomogą w samoocenie:

l.p.	Wymagane elementy PN-EN ISO/IEC 27001:2023-08	TAK	NIE
1.	Czy określono kontekst wewnętrzny i zewnętrzny organizacji? [4.1; 4.2]	◯	◯
	Komentarz własny:		
2.	Czy określono, które z wymagań stron zainteresowanych zostały uwzględnione w ramach SZBI? [4.2 c)]	◯	◯
	Komentarz własny:		
3.	Czy określono zakres systemu bezpieczeństwa informacji (w tym granice i możliwości) w formie udokumentowanej informacji? [4.3]	◯	◯
	Komentarz własny:		
4.	Czy jest ustanowiona i udokumentowana Polityka Bezpieczeństwa Informacji? [5.2]	◯	◯
	Komentarz własny:		
5.	Czy są opracowanie i wdrożenie procesy szacowania ryzyka (metodyki) oraz czy są udokumentowane informacje z procesu szacowania ryzyka w bezpieczeństwie informacji? [6.1]	◯	◯
	Komentarz własny:		
6.	Czy opracowano i wdrożono proces postępowania z ryzykiem? [6.1]	◯	◯
	Komentarz własny:		
7.	Czy określono zabezpieczenia informacji zgodne z planem postępowania z ryzykiem? [6.1]	◯	◯
	Komentarz własny:		
8.	Czy opracowano Deklarację Stosowania zawierającą wykaz niezbędnych zabezpieczeń? [6.1];[Załącznik A]	◯	◯
	Komentarz własny:		

9.	Czy sformułowano plan postępowania z ryzykiem?[6.1]	○	○

Komentarz własny:

10.	Czy uzyskano akceptację właścicieli ryzyk dla ryzyk rezydualnych (szczątkowych)? [6.1]	○	○

Komentarz własny:

11.	Czy są udokumentowane informacje z procesu postępowania z ryzykiem?[6.1]	○	○

Komentarz własny:

12.	Czy są udokumentowane informacje dotyczące celów bezpieczeństwa informacji, czy cele te są monitorowane? [6.2]	○	○

Komentarz własny:

13.	Czy zmiany w systemie bezpieczeństwa informacji przeprowadzane są w sposób zaplanowany? [6.3]	○	○

Komentarz własny:

14.	Czy są udokumentowane informacje dot. kompetencji osób wykonujących pracę mającą wpływ na wyniki dotyczące bezpieczeństwa informacji? [7.2]	○	○

Komentarz własny:

15.	Czy są udokumentowane informacje potwierdzające, że ustalono kryteria dla procesów oraz zgodnie z kryteriami wdrożono nadzór nad procesami potrzebnymi do spełnienia wymagań dotyczących bezpieczeństwa informacji? [8.1]	○	○

Komentarz własny:

16.	Czy dostarczane z zewnątrz, procesy, wyroby lub usługi , które są istotne dla systemu zarządzania bezpieczeństwem informacji są nadzorowane? [8.1]	○	○

Komentarz własny:

17.	Czy są udokumentowane informacje dotyczące wyników szacowania/oceny ryzyka w bezpieczeństwie informacji? [8.2]	○	○

Komentarz własny:

18.	Czy są udokumentowane informacje dotyczące wyników postępowania z ryzykiem?	◯	◯

Komentarz własny:

19.	Czy określano zakres monitorowania zabezpieczeń i pomiarów ich skuteczności oraz czy są udokumentowane informacje jako dowód wyników monitorowania i pomiarów? [9.1]	◯	◯

Komentarz własny:

20.	Czy prowadzony jest program auditów wewnętrznych i dokumentowane są wyniki auditów? [9.2]	◯	◯

Komentarz własny:

21.	Czy w zaplanowanych odstępach czasu prowadzone są przeglądy zarządzania i czy są udokumentowane ich wyniki? [9.3] *Uwaga: Dane wejściowe do przeglądu zarządzania powinny uwzględniać m.in.: „zmiany potrzeb i oczekiwań stron zainteresowanych dla systemu zarządzania bezpieczeństwem informacji".*	◯	◯

Komentarz własny:

22.	Czy przeprowadzono Niezależny przegląd bezpieczeństwa ? [Zał. A 5.35]	◯	◯

Komentarz własny:

23.	Czy udokumentowane są niezgodności i działania korygujące? [10.2]	◯	◯

Komentarz własny:

… a Twoja organizacja jest już gotowa na proces certyfikacji?