# Komunikat z dn. 24.03.2023 w sprawie aktualizacja normy ISO/IEC 27001 Program Certyfikacji ISMS - Informacja dla certyfikowanych Organizacji

Polskie Centrum Badań i Certyfikacji S.A. informuje, że w dniu 25 października 2022 r. zostało opublikowane nowe wydanie normy ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* Wersja normy w języku polskim nie jest jeszcze dostępna.

## Główne zmiany w ISO/IEC 27001:2022 w porównaniu z poprzednim wydaniem normy obejmują między innymi:

1) Zmieniono Załącznik A, który aktualnie odnosi się do zabezpieczeń informacji określonych w znowelizowanej normie ISO/IEC 27002:2022, która zawiera informacje o nazwach kategorii zabezpieczeń i samych zabezpieczeniach;

2) Do uwag w rozdziale 6.1.3 c) wprowadzono zmiany redakcyjne, w tym usunięto cele stosowania zabezpieczeń i użyto sformułowania „zabezpieczenie informacji" zamiast „zabezpieczenie".

3) Tekst rozdziału 6.1.3 d) został przeorganizowany w celu wyeliminowania potencjalnej niejednoznaczności.

4) Dodano nowy punkt 4.2 c) dotyczący określenia tych wymagań stron zainteresowanych, które będą spełniane poprzez system zarządzania bezpieczeństwem informacji (ISMS).

5) Dodano nowy podrozdział 6.3 – Planowanie zmian, stanowiący, że organizacja powinna przeprowadzać zmiany w ISMS w sposób zaplanowany.

6) Zachowano spójność w zakresie czasownika używanego w powiązaniu z wyrażeniem „udokumentowane informacje", np. w rozdziałach 9.1, 9.2.2, 9.3.3 i 10.2 użyto sformułowania „Powinny być dostępne udokumentowane informacje jako dowód XXX".

7) W rozdziale 8 użyto sformułowania „dostarczane z zewnątrz procesy, wyroby i usługi" zamiast „podzlecane procesy" i usunięto termin „podzlecanie".

8) Nadano tytuły podrozdziałom w rozdziałach 9.2 – Audit wewnętrzny i 9.3 – Przegląd zarządzania oraz zmieniono ich kolejność.

9) Zmieniono kolejność dwóch podrozdziałów w rozdziale 10 – Doskonalenie.

10) Zaktualizowano wydania dokumentów związanych wymienionych w Bibliografii, takich jak ISO/IEC 27002 i ISO 31000.


Polskie Centrum Badań i Certyfikacji S.A.
ul. Puławska 469, 02-844 Warszawa
Tel.: +48 22 46 45 200
pcbc@pcbc.gov.pl
NIP 9512063356
REGON 015276609
KRS 0000144813
KAPITAŁ ZAKŁADOWY
16.000.000 ZŁ
(w pełni opłacony)
Konto Bankowe: Bank Pekao S.A.
nr 90 1240 6003 1111 0000 4946 7594
Spółka Zarejestrowana w Sądzie Rejonowym
dla m.st. Warszawy Wydział XIII Gospodarczy

POLSKIE CENTRUM
BADAŃ I CERTYFIKACJI

## Kluczowy harmonogram związany z okresem przejścia z PN-EN ISO/IEC 27001:2017-06 na ISO/IEC 27001:2022

Okres przejściowy dla normy ISO/IEC 27001:2022 zgodnie z dokumentem IAF MD 26:2023 trwa 36 miesięcy od ostatniego dnia miesiąca publikacji normy ISO/IEC 27001:2022 i zakończy się 31 października 2025 r.

PCBC S.A., jako jednostka certyfikująca systemy zarządzania będzie mogła wydawać akredytowane certyfikaty na zgodność z nową normą dopiero po uaktualnieniu zakresu akredytacji. Stosowny wniosek został już złożony w Polskim Centrum Akredytacji.

PCBC S.A. będzie przyjmowało Wnioski na przeprowadzenie procesu certyfikacji / ponownej certyfikacji wg normy PN-EN ISO/IEC 27001:2017-06 wyłącznie do 29 kwietnia 2024 r.

Od dnia 30 kwietnia 2024 r będą przyjmowane wyłącznie Wnioski na przeprowadzenie procesu certyfikacji / ponownej certyfikacji wg normy ISO/IEC 27001:2022.

Zakończenie przez PCBC przejścia na nową normę dla certyfikowanych organizacji nastąpi nie później niż 31 października 2025 r.

Wszystkie certyfikacje oparte o PN-EN ISO/IEC 27001:2017 ulegną zakończeniu lub zostaną cofnięte z końcem okresu przejściowego tj. z dniem 31 października 2025 r.

## Tryb postępowania dla Organizacji posiadających certyfikat PCBC S.A. na zgodność z normą PN-EN ISO/IEC 27001:2017-06

W PCBC S.A., działania dotyczące przejścia na ISO/IEC 27001:2022 będą prowadzone podczas rutynowego auditu nadzoru, auditu ponownej certyfikacji lub auditu oddzielnego, zgodnie z ustaleniami z certyfikowaną Organizacją, w sposób zapewniający zakończenie przejścia przed 31 października 2025 r.

Czas trwania auditu będzie kalkulowany na podstawie uaktualnionych danych Organizacji dotyczących jej systemu zarządzania. Zgodnie z wymaganiami dokumentu IAF MD 26:2023, na działania związane z auditem przejścia doliczony zostanie dodatkowy czas:

a) co najmniej 0,5 auditorodnia na audit przejścia, w przypadku gdy jest on przeprowadzany w połączeniu z auditem ponownej certyfikacji
b) co najmniej 1,0 auditorodzień na audit przejścia, w przypadku gdy jest on przeprowadzany w połączeniu z auditem w nadzorze lub jako oddzielny audit.

W oparciu o wyniki auditu przejścia zostanie podjęta decyzja w sprawie przejścia i zostanie zaktualizowany certyfikat Organizacji, data zakończenia bieżącego cyklu certyfikacji nie ulegnie zmianie.

Aby przejść pomyślnie audit, zaleca się, aby certyfikowane Organizacje podjęły następujące działania:

a) dokonanie analizy luk dotyczących zmian w ISO/IEC 27001,
b) opracowanie planu wdrożenia,
c) zidentyfikowanie procesów i dokumentów Organizacji, na które wpływa zmiana w ISO/IEC 27001 oraz, jeśli ma to zastosowanie, systemów informatycznych wykorzystywanych w certyfikowanej działalności,

d) zapewnienie właściwego szkolenia i świadomości wszystkich stron, które mają wpływ na skuteczność systemu zarzadzania bezpieczeństwem informacji Organizacji,

e) zaktualizowanie obecnego systemu zarządzania bezpieczeństwem informacji w celu spełnienia zmienionych wymagań oraz zapewnienie weryfikacji skuteczności wdrożenia zmian poprzez przeprowadzenie auditu wewnętrznego,

f) nawiązanie kontaktu z PCBC S.A. w celu ustalenia trybu postępowania przy przejściu na nowe wymagania normy.

Zachęcamy aby wymagane działania zostały jak najwcześniej zaplanowane i rozpoczęte, gdyż w przypadku braku przejścia na nową normę w terminie do 31 października 2025, certyfikacja ISO/IEC 27001 zostanie cofnięta.

W przypadku dodatkowych pytań dotyczących procesu przejścia i wymagań związanych z aktualizacją certyfikacji na zgodność z normą ISO/IEC 27001:2022 zachęcamy do kontaktu bezpośrednio z Państwa opiekunem ze strony PCBC SA.

## Tryb postępowania dla Organizacji ubiegających się o certyfikację systemu zarządzania bezpieczeństwem informacji w PCBC S.A.

Aktualnie PCBC S.A. przyjmuje Wnioski na przeprowadzenie procesu certyfikacji / ponownej certyfikacji zarówno w oparciu o PN-EN ISO/IEC 27001:2017-06 jak i ISO/IEC 27001:2022. Od dnia 30 kwietnia 2024 r będą przyjmowane wyłącznie Wnioski na przeprowadzenie procesu certyfikacji / ponownej certyfikacji wg normy ISO/IEC 27001:2022.

Celem uzyskania oferty na proces certyfikacji systemu zarządzania bezpieczeństwem informacji prosimy o wypełnienie i przesłanie na adres sprzedaz@pcbc.gov.pl „Wniosku o wycenę kosztów certyfikacji" dostępnego na naszej stronie internetowej Dokumenty Do Pobrania | PCBC S.A. lub o bezpośredni kontakt z Kierownikiem Zespołu ds. Sprzedaży i Obsługi Klienta panem Krzysztofem Mochem kmoch@pcbc.gov.pl +48 606 459 912.

## System zarządzania bezpieczeństwem informacji - szkolenia PCBC S.A.

W celu sprawnego przygotowania się Organizacji do wdrożenia nowych wymagań dla systemu zarządzania bezpieczeństwem informacji zgodnego z ISO/IEC 27001:2022, PCBC S.A. przygotowało ofertę szkoleniową obejmującą powyższy zakres tematyczny. Więcej informacji można uzyskać na naszej stronie internetowej System zarządzania bezpieczeństwem informacji - PCBC S.A. lub w bezpośrednim kontakcie z panią Natalią Kucharską nkucharska@pcbc.gov.pl +48 669 474 742.

*Joanna Nowak-Milewska*
Dyrektor Biura Certyfikacji Systemów Zarządzania
Polskie Centrum Badań i Certyfikacji S.A.