Dokument obowiązkowy IAF

WYMAGANIA DOTYCZĄCE PRZEJŚCIA NA ISO/IEC 27001:2022

Wydanie 2

(IAF MD 26:2023)

Data wydania: 15 lutego 2023 r. Data wejścia w życie: 15 lutego 2023 r. IAF MD 26:2023, Wydanie 2

© International Accreditation Forum, Inc. 2023

International Accreditation Forum, Inc. (IAF) ułatwia handel oraz wspiera przemysł i organy regulacyjne poprzez międzynarodowe porozumienie dotyczące wzajemnego uznawania między jednostkami akredytującymi (ABs) mające na celu globalne uznawanie wyników wydawanych przez jednostki oceniające zgodność (CABs) akredytowane przez członków IAF.

Akredytacja zmniejsza ryzyko przedsiębiorstw i ich klientów poprzez zapewnienie, że akredytowane CABs są kompetentne do wykonywania pracy, jakiej podejmują się w zakresie posiadanej akredytacji. Wymaga się, aby ABs będące członkami IAF i akredytowane przez nie CABs prowadziły działalność zgodnie z właściwymi normami międzynarodowymi i dokumentami obowiązkowymi IAF w celu spójnego stosowania tych norm.

ABs będące sygnatariuszami Porozumienia o Wielostronnym Uznawaniu IAF (IAF MLA) są regularnie poddawane ocenie równorzędnej, prowadzonej przez wyznaczone zespoły, w celu zapewnienia zaufania do funkcjonowania ich programów akredytacji. Struktura IAF MLA jest szczegółowo przedstawiona w dokumencie IAF PL 3 – Policies and Procedures on the IAF MLA Structure and for Expansion of the Scope of the IAF MLA. Zakres IAF MLA jest szczegółowo przedstawiony w dokumencie IAF MLA Status.

Struktura IAF MLA ma pięć poziomów: Poziom 1 określa kryteria obowiązkowe ISO/IEC 17011, które mają zastosowanie do wszystkich ABs. Połączenie działania (działań) Poziomu 2 oraz odpowiedniego(-ich) dokumentu(-ów) normatywnego(-ych) Poziomu 3 jest określane jako główny zakres MLA, a połączenie dokumentów normatywnych Poziomu 4 (jeżeli ma to zastosowanie) i Poziomu 5 jest określane jako podzakres MLA.

- Główny zakres MLA obejmuje działania, np. certyfikację wyrobów, oraz związane obowiązkowe normy, np. ISO/IEC 17065. Atestacje wykonane przez CABs na poziomie głównego zakresu są uznawane jako równie wiarygodne.
- Podzakres MLA obejmuje wymagania dotyczące oceny zgodności, np. ISO 9001, oraz specyficzne wymagania programu, jeżeli ma to zastosowanie, np. ISO 22003-1. Atestacje wykonane przez CABs na poziomie podzakresu są uznawane jako równoważne.

IAF MLA daje zaufanie niezbędne dla akceptacji wyników oceny zgodności przez rynek. Atestacja wydana w zakresie IAF MLA przez jednostkę, która jest akredytowana przez AB będącą sygnatariuszem IAF MLA, może być uznawana na świecie, co ułatwia handel międzynarodowy.

© International Accreditation Forum, Inc. 2023

SPIS TREŚCI

Wydanie 2
Opracowane przez: Komitet Techniczny IAF
Zatwierdzone przez: Członków IAF Data: 3 lutego 2023 r.
Data wydania: 15 lutego 2023 r. Data wejścia w życie: 15 lutego 2023 r.
Osoba do kontaktu: Elva Nilsen
IAF Corporate Secretary
Tel.: +1 613 454-8159
Email: secretary@iaf.nu

Wprowadzenie do tłumaczenia

Oryginał publikacji: Transition Requirements for ISO/IEC 27001:2022, Issue 2 of 15 February 2023

Tłumaczenie: Polskie Centrum Akredytacji, 20.03.2023 r., www.pca.gov.pl

Tekst tłumaczenia nie może być kopiowany w celu sprzedaży. Wersją oficjalną (rozstrzygającą) jest wersja w języku angielskim.

© International Accreditation Forum, Inc. 2023

© International Accreditation Forum, Inc. 2023

Wprowadzenie do dokumentów obowiązkowych IAF

Słów „zaleca się”[1] użyto w niniejszym dokumencie do wskazania uznanych sposobów spełnienia wymagań normy. Jednostka oceniająca zgodność (CAB) może spełnić te wymagania w równoważny sposób, pod warunkiem, że potrafi to wykazać jednostce akredytującej (AB). Słów „powinien; należy”[2] użyto w niniejszym dokumencie do wskazania tych postanowień, które, odzwierciedlając wymagania stosownej normy, są obowiązkowe.

[1] Przypis PCA: w oryginalnej, angielskiej wersji dokumentu występuje słowo „should”
[2] Przypis PCA: w oryginalnej, angielskiej wersji dokumentu występuje słowo „shall”

© International Accreditation Forum, Inc. 2023

Wymagania dotyczące przejścia na ISO/IEC 27001:2022

1. WPROWADZENIE

Wszystkie dokumenty przedstawiające informacje dotyczące przejścia na dokumenty normatywne będą dokumentami obowiązkowymi do stosowania przez jednostki akredytujące (ABs) będące sygnatariuszami IAF MLA i akredytowane przez nie jednostki oceniające zgodność (CABs), o zakresie określonym w niniejszym dokumencie. Niniejszy dokument został opracowany przez wyznaczony Zespół Zadaniowy Komitetu Technicznego IAF i zgodnie z IAF PR 7:2022 *Requirements for Producing IAF Mandatory Documents on Transitions*.

Niniejszy dokument przedstawia wymagania dotyczące przejścia na następujący dokument i jest obowiązkowy dla właściwych ABs będących sygnatariuszami IAF MLA i akredytowanych przez nie CABs:

Dokument normatywny:	ISO/IEC 27001:2022
Zastępujący:	ISO/IEC 27001:2013
Aktualny status (w momencie publikacji dokumentu obowiązkowego (MD)):	Norma Międzynarodowa (IS)
Okres przejściowy:	3 lata (36 miesięcy)

2. PODSUMOWANIE NAJWAŻNIEJSZYCH ZMIAN

2.1 Informacje ogólne

Zgodnie ze stosowną polityką ISO, ISO/IEC FDIS 27001:2022 została opracowana poprzez scalenie normy ISO/IEC 27001:2013 z ISO/IEC 27001:2013/COR 1:2014, ISO/IEC 27001:2013/COR 2:2015 oraz ISO/IEC 27001:2013/DAmd1 w lipcu 2022 r. Ponadto wymogiem ISO było dostosowanie ISO/IEC FDIS 27001:2022 do zharmonizowanej struktury norm systemu zarządzania (MSS) określonej w Załączniku SL Dyrektyw ISO/IEC, Część 1, Skonsolidowany Suplement ISO, 2022 r. W oparciu o wynik głosowania nad Końcowym Projektem Normy Międzynarodowej (FDIS), ISO opublikowała normę ISO/IEC 27001:2022 w dniu 25 października 2022 r.

Uwaga 1: ISO/IEC 27001:2013/DAmd1, aktualizującą Załącznik A i uwagi w rozdziale 6.1.3 c), opracowano w celu zachowania zgodności z normą ISO/IEC 27002:2022. DAmd jest skrótem oznaczającym Draft Amendment (Projekt Zmiany).

Uwaga 2: Nie należy publikować więcej niż dwóch odrębnych dokumentów w formie zmian modyfikujących aktualną Normę Międzynarodową (patrz Dyrektywy ISO/IEC, Część 1, 2022 r., rozdział 2.10.3), dlatego po opracowaniu ISO/IEC 27001:2013/DAmd1 musiało zostać opublikowane nowe wydanie normy ISO/IEC 27001.

© International Accreditation Forum, Inc. 2023

2.2 Najważniejsze zmiany

Główne zmiany w ISO/IEC 27001:2022 w porównaniu z ISO/IEC 27001:2013 obejmują między innymi co następuje:

1) Załącznik A odnosi się do zabezpieczeń informacji określonych w 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.
11) Niektóre występujące w normie ISO/IEC 27001:2013 odstępstwa w odniesieniu do podstawowej struktury, identycznego tekstu podstawowego, wspólnych terminów i podstawowych definicji norm systemu zarządzania (MSS) skorygowano w celu uzyskania spójności ze zharmonizowaną strukturą MSS, np. rozdział 6.2 d).

Uwaga 1: Pierwsze dwie pozycje pochodzą z ISO/IEC 27001:2013/DAmd1, trzecia z ISO/IEC 27001:2013/COR 2:2015, natomiast pozostałe zmiany wynikają ze zharmonizowanej struktury MSS.

Uwaga 2: W porównaniu z poprzednim wydaniem, liczba zabezpieczeń informacji w ISO/IEC 27002:2022 uległa zmniejszeniu ze 114 zabezpieczeń w 14 rozdziałach do 93 zabezpieczeń w 4 rozdziałach. Jeśli chodzi o zabezpieczenia w ISO/IEC 27002:2022, 11 z nich to nowe zabezpieczenia, 24 powstały w wyniku połączenia dotychczasowych zabezpieczeń, a 58 zabezpieczeń zostało zaktualizowanych. Znowelizowano ponadto strukturę zabezpieczeń poprzez wprowadzenie „atrybutu" i „celu" dla każdego zabezpieczenia i zaprzestanie stosowania „celów" dla grup zabezpieczeń.

Uwaga 3: ISO/IEC 27001:2013/COR 1:2014 dotyczy Załącznika A i pokrywa się z ISO/IEC 27001:2013/DAMD1.

© International Accreditation Forum, Inc. 2023

2.3 Wpływ

Wpływ zmian w ISO/IEC 27001:2022 obejmuje między innymi wprowadzenie nowego Załącznika A oraz rozdziału 6.3 – Planowanie zmian, ponieważ:

1) ISO/IEC 27001:2013/COR 2:2015 została już opublikowana i wdrożona.
2) Załącznik A ma charakter normatywny.
3) Zharmonizowana struktura MSS jest uznawana za niewielką nowelizację związaną z podstawową strukturą, identycznym tekstem podstawowym, wspólnymi terminami i podstawowymi definicjami MSS, w przypadku której większość zmian uznaje się za zmiany o charakterze redakcyjnym.

Wymagania w ISO/IEC 27001 odnoszące się do wzorcowego wykazu zabezpieczeń przedstawionego w Załączniku A dotyczą procesu porównania zabezpieczeń informacji określonych przez organizację z zabezpieczeniami wymienionymi w Załączniku A (6.1.3 c)) oraz sporządzenia deklaracji stosowania (6.1.3 d)). Porównując niezbędne zabezpieczenia informacji z zabezpieczeniami w Załączniku A, organizacja może potwierdzić, że żadne zabezpieczenie informacji z wzorcowego wykazu w Załączniku A ISO/IEC 27001:2022 nie zostało przypadkowo pominięte.

Porównanie takie może nie doprowadzić do odkrycia żadnego przypadkowo pominiętego koniecznego zabezpieczenia informacji. Jeżeli jednak przypadkowo pominięte niezbędne zabezpieczenia informacji zostaną odkryte, organizacja powinna zaktualizować swoje plany postępowania z ryzykiem w celu uwzględnienia dodatkowych niezbędnych zabezpieczeń informacji i ich wdrożenia.

Jak zasugerowano powyżej, wpływ ISO/IEC 27001:2022 na organizacje, które wdrożyły system zarządzania bezpieczeństwem informacji (ISMS) nie musi być znaczący.

3. KLUCZOWY HARMONOGRAM

Działanie	Termin realizacji
AB	
Gotowość AB do prowadzenia ocen według normy ISO/IEC 27001:2022 nie później niż	6 miesięcy od ostatniego dnia miesiąca publikacji ISO/IEC 27001:2022 (tj. 30 kwietnia 2023 r.)
Rozpoczęcie przez AB prowadzenia ocen początkowych wyłącznie na zgodność z ISO/IEC 27001:2022 nie później niż	6 miesięcy od ostatniego dnia miesiąca publikacji ISO/IEC 27001:2022 (tj. 30 kwietnia 2023 r.)
Zakończenie przez AB przejścia dla wszystkich CABs w ciągu	12 miesięcy od ostatniego dnia miesiąca publikacji ISO/IEC 27001:2022 (tj. 31 października 2023 r.)
CAB	
Rozpoczęcie przez CAB prowadzenia certyfikacji początkowej i ponownej certyfikacji wyłącznie według ISO/IEC 27001:2022 nie później niż	18 miesięcy od ostatniego dnia miesiąca publikacji ISO/IEC 27001:2022 (tj. 30 kwietnia 2024 r.)

© International Accreditation Forum, Inc. 2023

Działanie	Termin realizacji
Zakończenie przez CAB przejścia dla wszystkich certyfikowanych klientów w ciągu	36 miesięcy od ostatniego dnia miesiąca publikacji ISO/IEC 27001:2022 (tj. 31 października 2025 r.)

4. DZIAŁANIA W RAMACH PROCESU PRZEJŚCIA

4.1 Działania AB

Działanie	T/N	Uwagi
Przygotowania AB	T	1) AB powinna opracować ustalenia dotyczące przejścia na ISO/IEC 27001:2022 z uwzględnieniem wymagań niniejszego dokumentu. 2) Ustalenia dotyczące przejścia powinny określać, co powinna zrobić AB i co powinny zrobić CABs. AB może mieć kilka odrębnych dokumentów określających ustalenia dotyczące przejścia. 3) Ustalenia dotyczące przejścia powinny obejmować uwzględnienie co najmniej: • Zmian w ISO/IEC 27001 oraz analizy luk. • Kompetencji odpowiedniego personelu w zakresie ISO/IEC 27001:2022 i procesu przejścia. Uwaga: Zespół oceniający, jako całość, powinien posiadać wiedzę w zakresie technologii i praktyk bezpieczeństwa informacji (patrz IAF MD 13:2020, 4.2). Jak wszyscy wiemy, ISO/IEC 27002 przedstawia wzorcowy wykaz ogólnych zabezpieczeń informacji wraz z wytycznymi dotyczącymi ich wdrażania. • Identyfikacji tych procesów i dokumentów AB, na które wpływa zmiana w ISO/IEC 27001, jak również systemów informatycznych służących do zarządzania działalnością akredytacyjną, jeśli ma to zastosowanie. • Programu ocen dotyczących przejścia. • Przekazania CABs w odpowiednim czasie informacji na temat programu ocen dotyczących przejścia, takich jak informacje o ramach czasowych i podejściu do oceny dotyczącej przejścia oraz konsekwencjach niedokonania przejścia w terminie. 4) Zachęca się ABs, aby jak najwcześniej zaplanowały i rozpoczęły wymagane działania.

© International Accreditation Forum, Inc. 2023

Działanie	**T/N**	**Uwagi**
Przegląd dokumentacji CAB	N	
Przegląd dokumentacji technicznej CAB	T	1) AB powinna przeprowadzić przegląd dokumentacji technicznej w celu potwierdzenia, czy CABs są kompetentne w zakresie ISO/IEC 27001:2022. 2) AB powinna określić stosowność opracowanych przez CABs ustaleń dotyczących przejścia oraz, jeśli ma to zastosowanie, skuteczność ich wdrożenia, poprzez przegląd następujących informacji przedstawionych przez CABs: • Analizy luk dotyczącej zmian w ISO/IEC 27001:2022. • Ustaleń dotyczących przejścia i dowodów ich wdrożenia. • Upoważnienia właściwego personelu. • Innych istotnych informacji uznanych za niezbędne przez AB.
Ocena techniczna (na miejscu lub zdalna) w siedzibie głównej CAB	Jeśli dotyczy	Jeżeli AB jest w stanie pozyskać wystarczające dowody w ramach przeglądu dokumentacji technicznej CAB, ocena w siedzibie głównej CAB nie jest wymagana. Jeżeli AB nie jest w stanie zweryfikować skutecznego wdrożenia i zgodności z ustaleniami dotyczącymi przejścia CAB, wymagana jest ocena w siedzibie.
Obserwacja oceny (ocen) przeprowadzanej(-ych) przez CAB	N	
Czy na przejście może być potrzebny dodatkowy czas?	T	Ocena powinna obejmować co najmniej dodatkowe 0,5 dnia oceny w celu potwierdzenia przejścia CAB, w przypadku gdy przeprowadzana jest osobna ocena dotycząca przejścia.
Inne	T	1) AB może określić w programie ocen dotyczących przejścia ramy czasowe, w których CABs powinny złożyć wnioski o przejście. 2) AB powinna podjąć decyzję w sprawie przejścia w oparciu o wynik oceny (ocen) dotyczącej(-ych) przejścia. 3) W stosownych przypadkach, jeżeli zostały wykazane kompetencje akredytowanych CABs w zakresie ISO/IEC 27001:2022, AB powinna zaktualizować informacje

© International Accreditation Forum, Inc. 2023

Działanie	T/N	Uwagi
		dotyczące akredytacji tych CABs (np. certyfikaty akredytacji). 4) Jeżeli akredytowana CAB nie zakończy pomyślnie oceny dotyczącej przejścia przed upływem terminu wymienionego w punkcie 3, data ważności jej akredytacji dla ISO/IEC 27001:2013 nie powinna być późniejsza niż koniec okresu przejściowego.

4.2 Działania CAB

Działanie	T/N	Uwagi
Przygotowania CAB	T	1) CAB powinna opracować ustalenia dotyczące przejścia na ISO/IEC 27001:2022 z uwzględnieniem wymagań niniejszego dokumentu oraz ustaleń dotyczących przejścia określonych przez właściwą AB. 2) Ustalenia dotyczące przejścia powinny określać, co powinna zrobić CAB i co powinni zrobić jej klienci. CAB może mieć kilka odrębnych dokumentów określających ustalenia dotyczące przejścia. 3) Ustalenia dotyczące przejścia powinny obejmować uwzględnienie co najmniej: • Zmian w ISO/IEC 27001 oraz analizy luk. • Potrzeby modyfikacji powiązanych procesów certyfikacji, dokumentów oraz, jeśli ma to zastosowanie, systemów informatycznych służących do zarządzania działalnością certyfikacyjną. • Kompetencji odpowiedniego personelu w zakresie ISO/IEC 27001:2022 i procesu przejścia. • Zespół auditujący, jako całość, powinien posiadać wiedzę w zakresie wszystkich zabezpieczeń informacji zawartych w ISO/IEC 27002:2022 i ich wdrażania (patrz ISO/IEC 27006:2015, 7.1.2.1.3 b)). • Programu auditów przejścia. • Przekazania klientom w odpowiednim czasie informacji na temat programu przejścia, takich jak informacje o ramach czasowych i podejściu do auditu przejścia oraz konsekwencjach niedokonania przez klienta przejścia w terminie. 4) Zachęca się CABs, aby jak najwcześniej zaplanowały i rozpoczęły wymagane działania.

© International Accreditation Forum, Inc. 2023

Działanie	**T/N**	**Uwagi**
Audit przejścia	T	1) CAB może przeprowadzić audit przejścia w połączeniu z auditem w nadzorze, auditem ponownej certyfikacji lub jako oddzielny audit. 2) Audit przejścia nie powinien się opierać wyłącznie na przeglądzie dokumentów, szczególnie w przypadku przeglądu technicznych zabezpieczeń informacji. 3) Audit przejścia powinien obejmować między innymi: • Analizę luk dotyczącą ISO/IEC 27001:2022, a także potrzebę zmian w ISMS klienta. • Aktualizację deklaracji stosowania (SoA). • Jeśli ma to zastosowanie, aktualizację planu postępowania z ryzykiem. • Wdrożenie i skuteczność nowych lub zmienionych zabezpieczeń informacji wybranych przez klienta. 4) CAB może przeprowadzić audit przejścia zdalnie pod warunkiem zapewnienia, że cele auditu przejścia zostaną zrealizowane.
Czy na przejście może być potrzebny dodatkowy czas?	T	1) Co najmniej 0,5 auditorodnia na audit przejścia, w przypadku gdy jest on przeprowadzany w połączeniu z auditem ponownej certyfikacji. 2) Co najmniej 1,0 auditorodzień na audit przejścia, w przypadku gdy jest on przeprowadzany w połączeniu z auditem w nadzorze lub jako oddzielny audit.
Inne	T	1) CAB może określić w programie auditów przejścia ramy czasowe, w których certyfikowani klienci powinni złożyć wnioski o przejście. 2) CAB powinna podjąć decyzję w sprawie przejścia w oparciu o wynik auditu przejścia. 3) CAB powinna zaktualizować dokumenty certyfikacyjne certyfikowanego klienta, jeżeli jego ISMS spełnia wymagania normy ISO/IEC 27001:2022. Uwaga: W przypadku gdy dokument certyfikacyjny zostaje zaktualizowany, ponieważ klient pomyślnie ukończył tylko audit przejścia, data zakończenia jego bieżącego cyklu certyfikacji nie ulegnie zmianie. 4) Wszystkie certyfikacje oparte na ISO/IEC 27001:2013 powinny ulec zakończeniu lub zostać cofnięte z końcem okresu przejściowego.

© International Accreditation Forum, Inc. 2023

4.3. Inne

4.3.1 Ocena w siedzibie CAB po podjęciu decyzji w sprawie przejścia powinna się koncentrować na weryfikacji wdrożenia ustaleń dotyczących przejścia przed całkowitym zakończeniem realizacji tych ustaleń przez CAB. Ocena w siedzibie powinna dotyczyć co najmniej:

- Wdrożenia zmienionych procesów i procedur CAB.
- Wykazania kompetencji właściwego personelu przed jego zaangażowaniem się w działania certyfikacyjne w odniesieniu do ISO/IEC 27001:2022.
- Postępów w przechodzeniu certyfikowanych klientów na ISO/IEC 27001:2022.

4.3.2 Wszystkie obserwacje wybrane po podjęciu decyzji w sprawie przejścia powinny się opierać na ISO/IEC 27001:2022 i skupiać na kompetencjach CAB do przeprowadzania auditów w oparciu o ISO/IEC 27001:2022.

Koniec dokumentu obowiązkowego IAF przedstawiającego wymagania dotyczące przejścia na ISO/IEC 27001:2022

Dalsze informacje

Dalsze informacje dotyczące niniejszego lub innych dokumentów IAF można uzyskać kontaktując się z członkiem IAF lub Sekretariatem IAF.

Dane kontaktowe członków IAF znajdują się na stronach IAF: http://www.iaf.nu.

Sekretariat:

Elva Nilsen
IAF Corporate Secretary
Tel.: +1 (613) 454-8159
Email: secretary@iaf.nu

© International Accreditation Forum, Inc. 2023