POLSKIE CENTRUM
BADAŃ I CERTYFIKACJI
www.pcbc.gov.pl

ZASADY CERTYFIKACJI SYSTEMÓW ZARZĄDZANIA
- Informacja dla Organizacji

DBC 14

wydanie 35 z dnia 02.02.2026

Polskie Centrum Badań i Certyfikacji S.A.
Ul. Puławska 469, 02 -844 Warszawa
Tel.: +48 22 46 45 200; pcbc@pcbc.gov.pl

Spis treści

1. Wstęp

Niniejsze zasady certyfikacji systemów zarządzania przeznaczone są dla Organizacji ubiegających się o uzyskanie certyfikatu systemu zarządzania w Polskim Centrum Badań i Certyfikacji S.A. (PCBC S.A.). Niniejsze zasady stanowią wyciągi z procedur PCBC S.A. - Biura Certyfikacji Systemów Zarządzania.

PCBC S.A. posiada akredytacje Polskiego Centrum Akredytacji nr AC 019 na prowadzenie certyfikacji systemów zarządzania w następującym zakresie:

- PN-EN ISO 9001, QMS
- PN-EN ISO 13485, MDMS
- PN-EN ISO 14001, EMS
- PN-EN ISO 45001, H&SMS
- PN-EN ISO 22000, FSMS
- PN-EN ISO/IEC 27001, ISMS
- PN-ISO 37001, ABMS

PCBC S.A. świadczy także usługi certyfikacji systemów zarządzania poza zakresem akredytacji, prowadząc m.in. certyfikację:

- PN-EN ISO 50001, EnMS
- PN-EN ISO 22301, BCMS
- Wewnętrzny System Kontroli (WSK)
- AQAP
- PN-EN 14065
- DPD – Dobra Praktyka Dystrybucyjna
- DPP – Dobra Praktyka Produkcyjna
- zasady i wymagania opisane przez Codex Alimentarius

Zasady dotyczą również certyfikacji systemów zintegrowanych, będących kompilacją ww.

Dokumenty PCBC S.A. związane z procesem certyfikacji są dostępne na stronie internetowej (www.pcbc.gov.pl) oraz na życzenie Organizacji (Klienta) w siedzibie PCBC S.A. Pozostałe dokumenty przywołane w niniejszym dokumencie dostępne są odpowiednio: normy - Polski Komitet Normalizacyjny (www.pkn.pl); dokumenty IAF – Polskie Centrum Akredytacji (www.pca.gov.pl).

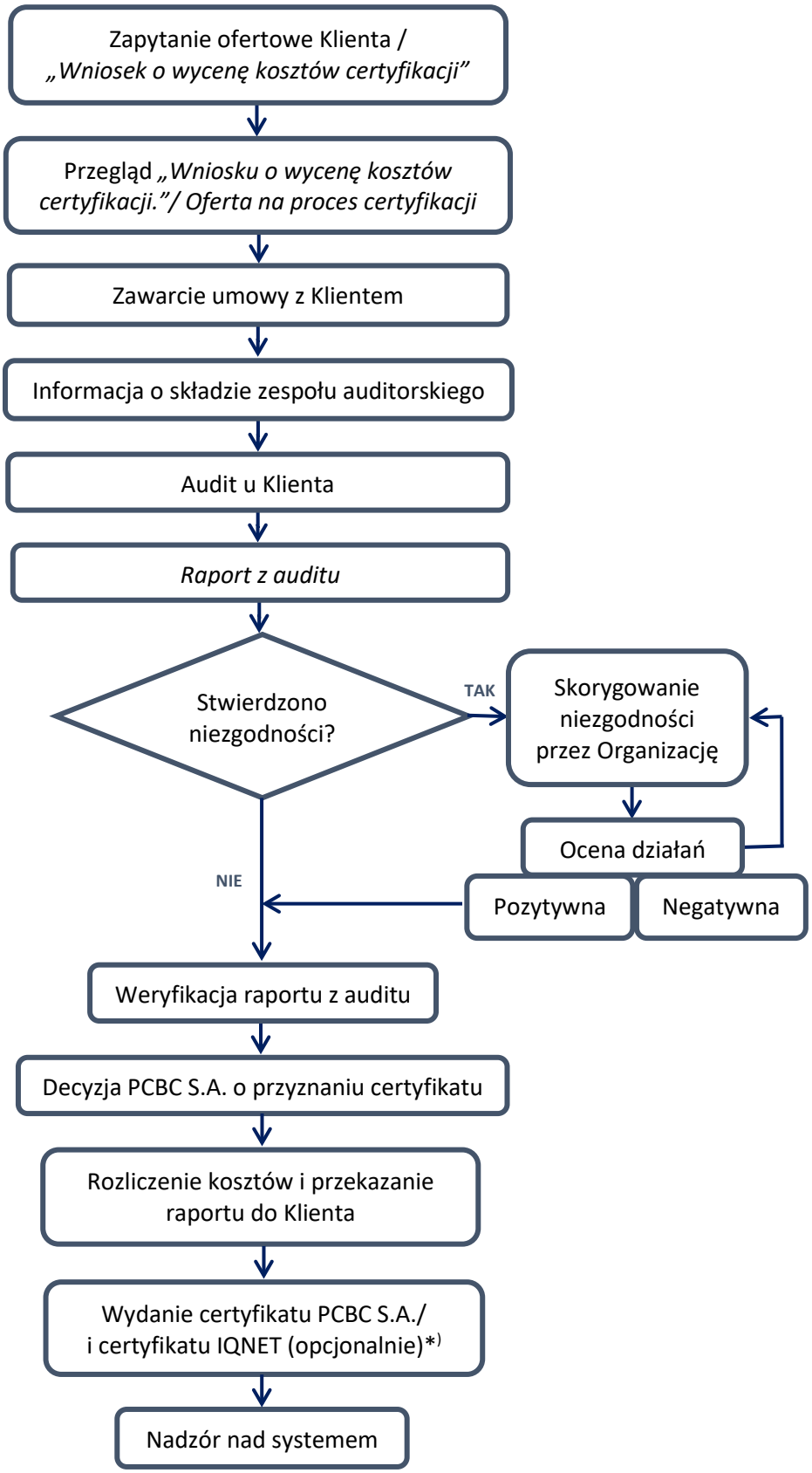
Zasady Certyfikacji Systemów Zarządzania opracowane zostały na podstawie wymagań norm i dokumentów:

- PN-EN ISO 9000 Systemy zarządzania jakością - Podstawy i terminologia,
- PN-EN ISO/IEC 17021-1 Ocena zgodności. Wymagania dla jednostek prowadzących audytowanie i certyfikację systemów zarządzania,
- ISO 22003-1 Food safety - Part 1: Requirements for bodies providing audit and certification of food safety management systems,

- PN-EN ISO/IEC 27006-1 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności -- Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji -- Część 1: Postanowienia ogólne,
- PN-ISO 50003 Systemy zarządzania energią - Wymagania dla jednostek prowadzących audity i certyfikację systemów zarządzania energią,
- IAF MD 1 Dokument obowiązkowy IAF dotyczący auditu i certyfikacji systemów zarządzania organizacji wielooddziałowych,
- IAF MD 2 Dokument obowiązkowy IAF dotyczący przenoszenia akredytowanej certyfikacji systemów zarządzania,
- IAF MD 4 Dokument obowiązkowy IAF dotyczący stosowania technologii informacyjno-komunikacyjnych („ICT") do celów prowadzenia audytów/ocen,
- IAF MD 5 Dokument obowiązkowy IAF ustalanie czasu auditu systemów zarządzania jakością, środowiskowego oraz bezpieczeństwa i higieną pracy,
- IAF MD 9 Dokument obowiązkowy IAF Stosowanie normy ISO/IEC 17021 w systemach zarządzania jakością wyrobów medycznych (ISO 13485),
- IAF MD 11 Dokument obowiązkowy IAF dotyczący stosowania normy ISO/IEC 17021-1 w auditach zintegrowanych systemów zarządzania,
- IAF MD 22 Dokument obowiązkowy IAF Stosowanie normy ISO/IEC 17021-1 w certyfikacji systemów zarządzania bezpieczeństwem i higieną pracy (SZBHP),
- IAF MD 28 Dokument obowiązkowy IAF dotyczący przekazywania danych do IAF Database i ich utrzymywania
- IAF MD 30 Dokument obowiązkowy IAF. WYMAGANIA DOTYCZĄCE PRZEJŚCIA NA ISO 37001:2025
- EA-7/04 - Zgodność z prawem jako część akredytowanej certyfikacji w odniesieniu do ISO 14001:2015.

W miejscach, gdzie niniejszy dokument powołuje się na normy lub inne dokumenty, dotyczy to ich aktualnych wydań.

2. Przebieg procesu certyfikacji systemów zarządzania i główne zasady zarządzania certyfikatem IQNET



*) ***Informacja dla Organizacji otrzymujących certyfikat IQNET***

W ramach umowy o certyfikację podpisanej z PCBC S.A., możliwe jest wydanie przez PCBC S.A. (członek IQNET), zgodnie z poniższymi ogólnymi zasadami, certyfikatu IQNET odpowiedniego dla danego systemu zarządzania:

a) Certyfikat IQNET jest załącznikiem do oświadczenia o uznaniu wydanym przez PCBC S.A., w oparciu o audit i proces certyfikacji przeprowadzony przez PCBC S.A. lub pod jego przewodnictwem. Certyfikat IQNET jest wydany przez PCBC S.A. w imieniu IQNET. Uznanie IQNET jest możliwe, ponieważ ustanowiono zaufanie między członkami IQNET na podstawie wyników ocen rówieśniczych, doświadczenia w ramach współpracy, podpisanej Umowy członka IQNET, która dotyczy wzajemnego uznawania certyfikatów
b) Certyfikat IQNET jest wydawany i będzie modyfikowany lub wycofywany równolegle z wydaniem i modyfikacją lub wycofaniem certyfikatu PCBC S.A.
c) Główna odpowiedzialność za wydanie certyfikatu IQNET spoczywa na PCBC S.A.
d) Procedury i warunki wydawania, modyfikacji i wycofania certyfikatu IQNET są zgodne z zasadami opisanymi w dokumentacji certyfikacji systemów zarządzania PCBC S.A. i w dokumentacji IQNET
e) W przypadku zakończenia członkostwa PCBC S.A. w IQNET, certyfikat IQNET zostanie anulowany i wycofany przez PCBC S.A. w ciągu 30 dni, a posiadacze certyfikatu IQNET zostaną poinformowani pisemnie (list, e-mail z kopią do Siedziby Głównej IQNET), że ważność certyfikatu IQNET wygasła.

3. Zapytanie ofertowe Klienta / „Wniosek o wycenę kosztów certyfikacji / Przegląd „Wniosku o wycenę kosztów certyfikacji”

W odpowiedzi na zapytanie ofertowe Klienta, złożone jako „Wniosek o wycenę kosztów certyfikacji” wraz z załącznikami, który zamieszczony jest na stronie www.pcbc.gov.pl, PCBC S.A., przeprowadza w ciągu 1 dnia przegląd ww. wniosku pod względem jego poprawności w zakresie formalnym i merytorycznym w celu podjęcia decyzji o możliwości przeprowadzeniu procesu certyfikacji.

W przypadku, gdy wniosek jest niekompletny, PCBC S.A. występuje do Klienta z prośbą o jego uzupełnienie, np. czy jakieś zapisy systemu zarządzania bezpieczeństwem informacji (SZBI), które nie mogą być udostępnione do wglądu zespołowi, zawierające informacje poufne lub wrażliwe, bez których auditowanie SZBI nie jest możliwe, wymagają przyznania właściwych uprawnień dostępu do informacji. W przypadku nieuzupełnienia wniosku w ciągu 14 dni od daty otrzymania informacji o jego niekompletności, wniosek jest odrzucany.

W ciągu max. 5 dni roboczych PCBC S.A. przygotowuje ofertę na proces certyfikacji/ponownej certyfikacji/przeniesienia certyfikacji i przesyła ją Klientowi. W przypadku niemożności przeprowadzenia procesu certyfikacji/ponownej certyfikacji/przeniesienia certyfikacji,np. z powodu wystąpienia konfliktu interesów, informuje pisemnie o tym Klienta.

Klient we wniosku zobowiązany jest podać **zakres oczekiwanej certyfikacji**.

Zakres powinien być zgodny z dokumentem opisującym zakres systemu zarządzania Organizacji oraz być sformułowany w sposób jednoznaczny i niewprowadzający w błąd. Zakres certyfikacji powinien obejmować procesy główne tj. działania (np. projektowanie, produkcję wyrobów lub świadczenie usług na rzecz klientów zewnętrznych). W zakresie certyfikacji nie należy podawać procesów wspomagających, wsparcia czy zarządczych. Zakres nie może też zawierać jakichkolwiek oświadczeń promocyjnych, marek lub oświadczeń.

W odniesieniu do systemu zarządzania bezpieczeństwem żywności (FSMS) przy opisywaniu zakresu obowiązują dodatkowo niżej opisane zasady:

- zakres nie może obejmować projektowania, który jest elementem związanym z procesem produkcji
- z zakresu certyfikacji nie można wykluczać działań, procesów, wyrobów lub usług, jeżeli te działania, procesy, wyroby lub usługi mogą mieć wpływ na bezpieczeństwo żywności wyrobów końcowych, jak określono w odpowiedzialności prawnej działalności organizacji

Planując datę certyfikacji Organizacja powinna uwzględnić, że wszystkie audity w cyklu certyfikacji będą realizowane w czasie, gdy realizowana jest produkcja wyrobów /świadczenie usług z zakresu certyfikacji, dotyczy w szczególności Organizacji o sezonowej działalności.

4. Przegląd / Zawarcie umowy z Klientem

Po zaakceptowaniu oferty, Klient przesyła do PCBC S.A. dwa egzemplarze umowy o proces certyfikacji/ponownej certyfikacji (wzór umowy zamieszczony jest na stronie www.pcbc.gov.pl). PCBC S.A. dokonuje przeglądu ww. umowy pod względem jej poprawności w zakresie formalnym i merytorycznym. Podpisany ze strony PCBC S.A. jeden egzemplarz umowy odsyła Klientowi.

Umowa pomiędzy PCBC S.A., a Klientem może zostać zawarta w wersji elektronicznej.

PCBC S.A. przyjmuje dokumentację systemową niezbędną do przeprowadzenia oceny w wersji elektronicznej.

Ze względu na bezpieczeństwo informacji przy przekazywaniu dokumentacji, zaleca się korzystanie z **serwera FTP PCBC S.A.**
Wraz z przekazywaną dokumentacją Klient winien załączyć wykaz przekazywanych dokumentów.

W przypadku dużej ilości dokumentów przekazywanych przez Organizację do PCBC S.A. w drodze uzgodnień pomiędzy PCBC S.A. i Organizacją ustalane jest miejsce do przechowywania dokumentacji. Organizacja może wydzielić taką przestrzeń na własnych zasobach lub konieczne do oceny dokumenty zamieścić na zabezpieczonym serwerze FTP PCBC S.A. PCBC S.A. na potrzeby przeprowadzanego auditu nada prawa do wglądu w te dokumenty Auditorom.

5. Informacja o składzie zespołu auditorskiego

PCBC S.A. na podstawie danych zawartych w przeglądzie wniosku wyznacza kompetentny zespół auditujący do przeprowadzenia procesu certyfikacji/ponownej certyfikacji/przeniesienia certyfikacji (dalej procesu). W każdym zespole wyznacza się auditora wiodącego oraz w zależności od potrzeb /

auditorów technicznych / ekspertów technicznych. Członkowie zespołu wybierani są z zatwierdzonej listy auditorów / ekspertów z uwzględnieniem kompetencji potrzebnych do osiągnięcia celów auditu, wymagań dotyczących bezstronności oraz wymagań danego programu certyfikacji. Zespół auditorski jako całość posiada wszystkie kompetencje do przeprowadzenia procesu. Skład zespołu auditorskiego przekazywany jest Organizacji z wyprzedzeniem minimum 7 dni przed oceną.
Organizacji przysługuje prawo wnioskowania na piśmie o zmianę poszczególnych członków zespołu auditorskiego np. w przypadku sytuacji występującego konfliktu interesów, nieetycznych zachowań. Zgłoszenie wniosku powinno nastąpić w okresie 5 dni od otrzymania informacji z PCBC S.A. o składzie zespołu. W uzasadnionych przypadkach PCBC S.A. dokona zmiany członków proponowanego składu zespołu auditorskiego.
W audicie mogą uczestniczyć auditorzy szkolący się, ewaluatorzy lub obserwatorzy Polskiego Centrum Akredytacji. Udział ww. osób nie obciąża finansowo Organizacji. Koszty pokrywa PCBC S.A. Ponadto udział ww. osób, jest organizowany w taki sposób, aby nie utrudniać prowadzonych działań auditowych członkom zespołu auditorskiego.

6. Audit początkowej certyfikacji prowadzony w dwóch etapach

Audit w Organizacji rozpoczyna się spotkaniem otwierającym. Na spotkaniu otwierającym m.in. auditor wiodący, potwierdza cel, zakres i kryteria auditu, przedstawia metody działań i procedury auditowania PCBC S.A. w tym również informuje o zachowaniu poufności przez członków zespołu auditorskiego.

Każda lokalizacja tymczasowa, do której Klient certyfikacji lub certyfikowana Organizacja dostarcza swoje wyroby lub usługi jest włączona do oceny auditu certyfikującego i programu auditów. Zdalne działania auditowe standardowo nie przekraczają 30% planowanego czasu auditu na miejscu. W przypadku auditowania SZBI, każda lokalizacja włączona do systemu zarządzania bezpieczeństwem informacji (SZBI), obciążona znaczącym ryzykiem, jest auditowana przed certyfikacją. Ponadto zespół auditujący będzie żądać od Klienta wykazania, że ocena ryzyk związanych z bezpieczeństwem informacji jest stosowna i odpowiednia dla działania SZBI w zakresie SZBI ponadto zespół będzie ustalać czy procedury Organizacji Klienta dotyczące identyfikacji, badania i oceny ryzyk związanych z bezpieczeństwem informacji oraz wyniki ich wdrażania są spójne z polityką, celami i zadaniami Organizacji Klienta.

6.1. Etap I auditu

ETAP I ma następujące cele:

a) przegląd udokumentowanych informacji systemu zarządzania Klienta
b) ocenę specyficznych dla lokalizacji Klienta warunków oraz przeprowadzenie rozmów z personelem Klienta w celu określenia gotowości do drugiego etapu
c) przeprowadzenie przeglądu statusu Klienta i zrozumienia przez niego wymagań normy, zwłaszcza w odniesieniu do identyfikacji kluczowych wyników działań lub znaczących aspektów, procesów, celów i działania systemu zarządzania
d) uzyskanie niezbędnych informacji dotyczących zakresu systemu zarządzania, w tym:

- lokalizacji Klienta
- stosowanych procesów i wyposażenia
- poziomów ustalonych środków nadzoru (szczególnie w przypadku Klientów wielooddziałowych)
- mających zastosowanie wymagań przepisów prawnych i regulacyjnych

e) przeprowadzenie przeglądu przydziału zasobów do drugiego etapu i uzgodnienia z Klientem szczegółów drugiego etapu

f) skoncentrowanie się na zaplanowaniu drugiego etapu poprzez osiągnięcie wystarczającego zrozumienia systemu zarządzania Klienta i prowadzonej przez niego działalności w danej lokalizacji w kontekście normy dotyczącej systemu zarządzania lub innego dokumentu normatywnego

g) ocenę, czy są planowane i realizowane audity wewnętrzne i przeglądy zarządzania, oraz czy poziom wdrożenia systemu zarządzania uzasadnia gotowość Klienta do drugiego etapu

h) w przypadku auditowania SZBI dodatkowo ocenę czy są planowane i realizowane Niezależne przeglądy bezpieczeństwa oraz weryfikacja posiadania przez organizację deklaracji stosowania.

Ponadto podczas I etapu auditu z zakresu SZBI, Klient dostarcza zespołowi auditującemu:

a) ogólne informacje dotyczące SZBI i działań, które obejmuje ten system

b) kopię dokumentacji SZBI wymaganą wg PN-EN ISO/IEC 27001, oraz tam, gdzie jest to wymagane - dokumenty związane.

Ponadto, I etap auditu z zakresu FSMS:
Powinien być przeprowadzony w obiektach klienta w celu osiągnięcia celów wyżej określonych. W wyjątkowych okolicznościach lub zdarzeniach całość lub część etapu 1. może odbywać się poza siedzibą klienta lub zdalnie przy wykorzystaniu technologii informacyjno-komunikacyjnych i musi być w pełni uzasadniona.

UWAGA 1 Wyjątkowe okoliczności lub zdarzenia mogą obejmować odległą lokalizację, klęskę żywiołową, pandemię, krótką produkcję sezonową i inne szczególne sytuacje.

Przy określaniu odstępu pomiędzy I a II etapem auditu PCBC S.A. bierze pod uwagę konieczność rozwiązania przez Klienta kwestii zidentyfikowanych podczas I etapu auditu. Przerwa pomiędzy etapem 1 a etapem 2 nie powinna być dłuższa niż sześć miesięcy. Etap 1. powinien być powtórzony, jeśli potrzebna jest dłuższa przerwa.

6.2. Etap II auditu

Celem II ETAPU jest ocena wdrożenia, w tym skuteczności, systemu zarządzania Klienta.

Drugi etap powinien odbywać się w lokalizacji (lokalizacjach) Klienta.

Powinien on obejmować auditowanie co najmniej:

a) informacji i dowodów zgodności ze wszystkimi wymaganiami stosownej normy dotyczącej systemu zarządzania lub innych dokumentów normatywnych

b) monitorowania, pomiarów, raportowania i przeglądania osiągnięć w odniesieniu do kluczowych celów i zadań (zgodnych z oczekiwaniami w stosownej normie dotyczącej systemu zarządzania lub innym dokumencie normatywnym)
c) zdolności systemu zarządzania Klienta i sposobu jego działania odnośnie do spełniania mających zastosowanie wymagań przepisów prawnych, regulacyjnych i umów
d) nadzoru operacyjnego Klienta nad procesami
e) auditów wewnętrznych i przeglądów zarządzania
f) odpowiedzialności kierownictwa za polityki Klienta.

ETAP II auditu w zakresie systemu zarządzania bezpieczeństwem informacji koncentruje się w Organizacji Klienta na:

a) przywództwie i zaangażowaniu najwyższego kierownictwa w politykę bezpieczeństwa informacji i cele bezpieczeństwa informacji
b) wymaganiach dotyczących dokumentacji, wymienionych w PN-EN ISO/IEC 27001
c) zarządzaniu zmianą
d) przeglądzie "podejścia procesowego" (kryteria procesów)
e) weryfikacja i ocena zalecania na zewnątrz – procesy, ale też produkty i usługi
f) weryfikacji metod uzyskiwania wyników – porównywalność i powtarzalność
g) weryfikacji wdrożenia nowych zabezpieczeń
h) ocenie ryzyka związanego z bezpieczeństwem informacji i na tym, aby ta ocena dostarczała spójnych, rzeczywistych i porównywalnych wyników w przypadku jej powtórzenia
i) określeniu celów stosowania zabezpieczeń oraz zabezpieczeń, w oparciu o procesy oceny ryzyka i postępowania z ryzykiem bezpieczeństwa informacji
j) zabezpieczeniu informacji oraz na skuteczności SZBI ocenianych względem celów bezpieczeństwa informacji
k) powiązaniach pomiędzy wybranymi i zastosowanymi zabezpieczeniami, Deklaracją Stosowania, wynikami procesów oceny i postępowania z ryzykiem oraz polityką SZBI i celami
l) wdrożeniu zabezpieczeń (patrz Załącznik A normy PN-EN ISO/IEC 27001), biorąc pod uwagę kontekst zewnętrzny i wewnętrzny, wykonywane przez Organizację pomiary skuteczności zabezpieczeń [patrz d) powyżej], w celu określenia, czy zabezpieczenia są wdrożone i skuteczne w osiąganiu określonych celów
m) programach, procesach, procedurach, zapisach, audytach wewnętrznych i przeglądach skuteczności SZBI w celu upewnienia się, że wynikają z decyzji kierownictwa, polityki SZBI oraz celów.

Audit początkowej certyfikacji 2 etapowy kończy się spotkaniem zamykającym, na którym auditor wiodący przedstawia m. in. wnioski z przebiegu auditu. Wnioski dotyczą pozytywnych aspektów ocenianego systemu oraz ewentualnych uwag i niezgodności.

Klient ma możliwość zadania pytań. Wszelkie rozbieżne opinie pomiędzy zespołem auditującym a Klientem dotyczące ustaleń lub wniosków z auditu powinny być przedyskutowane i jeśli to możliwe rozwiązane. Wszelkie nierozwiązane, rozbieżne opinie powinny być zapisane i skierowane do PCBC S.A.

W przypadku stwierdzenia niezgodności podczas 2 etapowego auditu początkowej certyfikacji, zespół auditujący wystawia kartę niezgodności i objaśnia tryb postępowania z dalszymi działaniami.

Klasyfikacja niezgodności:

- mała niezgodność - niezgodność, która nie wpływa na zdolność systemu zarządzania do osiągnięcia zamierzonych wyników
- duża niezgodność - niezgodność, która wpływa na zdolność systemu zarządzania do osiągnięcia zamierzonych wyników.

Każda niezgodność musi być odniesiona do jednego / kilku wymagań normy lub innego dokumentu, który zawiera wymagania certyfikacyjne.

Organizacja w ciągu 5 dni roboczych (14 dni kalendarzowych w przypadku PN-EN ISO 13485) od daty auditu powinna przekazać do PCBC S.A. z powiadomieniem auditora wiodącego wypełnioną kartę niezgodności zawierającą plan działań korygujących / korekcji. Auditor wiodący dokonuje przeglądu zaproponowanych przez Organizację korekcji i działań korygujących. Dowody korekcji / działań korygujących dla małych niezgodności są ocenione podczas następnego auditu. Dowody potwierdzające przeprowadzenie działań korygujących / korekcji dotyczące dużych niezgodności Organizacja powinna dostarczyć do 2 miesięcy od otrzymania niezgodności.

Działania korygujące / korekcyjne dotyczące dużych niezgodności stwierdzanych podczas auditów wszystkich certyfikowanych systemów zarządzania są oceniane na podstawie auditu dodatkowego lub dowodów, które Organizacja powinna dostarczyć w ww. terminie.

Audit dodatkowy może być przeprowadzony w przypadku stwierdzenia przez PCBC S.A. potrzeby sprawdzenia skuteczności wdrożenia w Organizacji działań korekcyjnych i korygujących w celu zamknięcia stwierdzonych w czasie auditu niezgodności. Audit dodatkowy może być przeprowadzony w pełnym zakresie lub w zakresie ograniczonym obejmującym wyłącznie obszary związane z niezgodnościami i działaniami, których skuteczność realizacji ma być oceniona.

Przeprowadzenie auditu dodatkowego, wymaga akceptacji kosztorysu do umowy.

Pozytywna ocena wykonania korekcji / działań korygujących przez auditora wiodącego jest podstawą do wnioskowania do PCBC S.A. o przyznanie certyfikatu.

Jeżeli PCBC S.A. nie będzie mogła zweryfikować wdrożenia korekcji i działań korygujących dotyczących dużej niezgodności w ciągu sześciu miesięcy od ostatniego dnia drugiego etapu auditu, wówczas wymagane będzie przeprowadzenie ponownego drugiego etapu przed wydaniem rekomendacji dotyczącej certyfikacji. Przeprowadzenie go, wymaga akceptacji kosztorysu do umowy.

Raport z auditu. Zespół auditujący dostarcza do PCBC S.A. raport z auditu, który podlega weryfikacji. W terminie do 30 dni roboczych od zakończenia wszystkich działań przekazany zostanie do Organizacji raport z auditu w wersji elektronicznej zatwierdzonej przez PCBC S.A. Klient może zgłosić do raportu uwagi dotyczące oczywistych omyłek, błędów pisarskich lub nieścisłości formalnych. Uwagi tego rodzaju należy przekazać w terminie 7 dni od daty otrzymania raportu, korzystając z formularza Oceny usług świadczonych Klientowi przesłanego wraz z raportem.

7. Decyzja w sprawie certyfikacji

PCBC S.A. podejmuje decyzje w sprawach o: udzieleniu/odmowie udzielenia/utrzymaniu certyfikacji, rozszerzeniu lub ograniczeniu zakresu certyfikacji, przedłużeniu, zawieszeniu lub wznowieniu, albo cofnięciu certyfikacji m.in. na podstawie:

- raportu z auditu
- komentarzy do niezgodności (jeżeli wystąpiły) i gdzie to jest stosowane, podjętych przez Klienta korekcji i działań korygujących
- potwierdzenia informacji zawartych we Wniosku o wycenę kosztów certyfikacji
- potwierdzenia, że cele auditu zostały osiągnięte
- rekomendacji zespołu auditującego, czy udzielić certyfikacji, czy nie, łącznie ze wszystkimi spostrzeżeniami
- pozytywnej weryfikacji raportu z auditów
- wszelkich mających zastosowanie informacji (np. informacji dostępnych publicznie).

Organizacja jest informowana pisemnie o podjętej decyzji. Dokumentem certyfikacyjnym, który potwierdza udzielenie certyfikacji jest certyfikat PCBC S.A. oraz certyfikat IQNET (opcjonalnie).

<u>Dokument certyfikacyjny i/lub załącznik do certyfikatu:</u>

- podpisywany jest kwalifikowanym podpisem elektronicznym przez Prezesa Zarządu
- jest wydawany Certyfikowanej Organizacji w wersji elektronicznej

8. Rozliczenie kosztów / Przekazanie raportu / Wydanie certyfikatu

Wydanie Klientowi certyfikatu następuje po dokonaniu przez Klienta wpłat za dany proces na podstawie przesłanej faktury przez PCBC S.A.

Raport jest własnością PCBC S.A., elektroniczny egzemplarz raportu z auditu przekazywany jest Klientowi wraz z informacją o podjętej decyzji certyfikacyjnej. Klient może zgłosić do raportu uwagi dotyczące oczywistych omyłek, błędów pisarskich lub nieścisłości formalnych. Uwagi tego rodzaju należy przekazać w terminie 7 dni od daty otrzymania raportu, korzystając z formularza Oceny usług świadczonych Klientowi przesłanego wraz z raportem.
Rozpowszechnianie raportu jako integralnej całości przez auditowaną Organizację nie jest ograniczone. Organizacja nie jest uprawniona do naruszenia integralności raportu i jego dzielenia,

w tym łączenia raportu lub jego fragmentów z innymi dziełami lub utworami, jak też do posługiwania się w obrocie fragmentami (częściami) raportu.

Certyfikat PCBC S.A. i IQNET (opcjonalnie) wydawany jest maksymalnie na trzy lata i nie może być odstępowany na rzecz osób trzecich.

Certyfikat PCBC S.A. dla danego systemu zarządzania podpisywany jest przez Prezesa Zarządu. Wraz z certyfikatem PCBC S.A. wydawany jest certyfikat IQNET - Międzynarodowej Sieci Jednostek Certyfikujących, zrzeszającej wiodące jednostki certyfikujące z całego świata. Certyfikat IQNET podpisywany jest przez Prezesa Zarządu. Klient po pozytywnym przejściu procesu certyfikacji ma prawo do otrzymania znaków certyfikowanego systemu PCBC S.A. oraz znaku IQNET, drogą e-mail. Zasady posługiwania się znakami certyfikowanego systemu określa odrębny dokument DBC 13. Certyfikat jest własnością PCBC S.A. i prawo to nie może być cedowane (odstępowane/przelewane) na podmioty trzecie. Cofnięcie Certyfikatu powoduje utratę jego ważności. Klient (podmiot certyfikowany) jako posiadacz Certyfikatu uprawniony jest do posługiwania się nim w zakresie oznaczonym w zawartej z PCBC S.A. umowie. PCBC S.A. pozostaje właścicielem danych zawartych w Certyfikacie.

PCBC S.A. udostępnia dane Klienta dotyczące udzielonej certyfikacji łącznie z jej statusem (aktywna, zawieszona, cofnięta) zawarte w wystawionych certyfikatach na rzecz prowadzonej przez IAF bazy certyfikowanych organizacji IAF Database, zgodnie z dokumentem IAF MD 28 (dotyczy certyfikatów objętych akredytacją PCA) oraz bazy certyfikowanych organizacji IQNET (dotyczy certyfikatów IQNET).

9. Nadzór nad systemem

W okresie ważności certyfikatu przeprowadzane są co najmniej 2 audity nadzoru. Audity nadzoru powinny być przeprowadzone co najmniej raz w roku kalendarzowym, z wyjątkiem lat, w których ma być prowadzona ponowna certyfikacja. Data pierwszego auditu nadzoru po certyfikacji początkowej nie powinna być późniejsza niż 12 miesięcy od daty podjęcia decyzji o certyfikacji.

Audity w nadzorze są auditami na miejscu i obejmują m.in.

- audity wewnętrzne i przeglądy zarządzania
- przegląd działań podjętych w odniesieniu do niezgodności zidentyfikowanych podczas poprzedniego auditu
- postępowanie ze skargami/reklamacjami
- skuteczność systemu zarządzania pod względem osiągania celów przez certyfikowanego Klienta i zamierzonych wyników odpowiedniego(-ich) systemu(-ów) zarządzania
- rozwój planowanych działań mających na celu ciągłe doskonalenie
- ciągły nadzór operacyjny
- przegląd wszelkich zmian
- stosowanie znaków i/lub wszelkiego powoływania się na certyfikację.

Do innych działań w nadzorze mogą należeć:

a) zapytania jednostki certyfikującej kierowane do certyfikowanego Klienta w sprawie różnych aspektów certyfikacji
b) przeglądanie wszelkich oświadczeń Klienta w odniesieniu do jego działalności (np. materiały promocyjne, strona internetowa)
c) żądania, aby certyfikowany Klient dostarczył udokumentowaną informację (na papierze lub w postaci elektronicznej)
d) inne sposoby monitorowania wyników działalności certyfikowanego Klienta (informacje mogą być przekazywane od PCBC S.A.).

Audity w nadzorze systemu zarządzania bezpieczeństwem informacji poddają przeglądowi:

- elementy utrzymania systemu, jakimi są ocena ryzyka bezpieczeństwa informacji i utrzymanie kontroli, wewnętrzne audyty SZBI, przegląd zarzadzania oraz działania korygujące
- komunikację ze stronami zewnętrznymi, zgodnie z wymaganiami dotyczącej SZBI normy PN-EN ISO/IEC 27001 i innymi dokumentami wymaganymi do przeprowadzenia certyfikacji
- zmiany w udokumentowanych systemach
- obszary przeznaczone do zmian
- wybrane wymagania PN-EN ISO/IEC 27001
- inne wybrane obszary, stosownie do okoliczności
- zapisy dotyczące odwołań i skarg, otrzymane przez PCBC S.A.

Jako minimum, nadzorowi poddawany jest przegląd:

- skuteczność SZBI w związku z osiągnięciem celów polityki bezpieczeństwa informacji Organizacji Klienta
- funkcjonowanie procedur okresowej oceny i przeglądu zgodności z powiązanymi przepisami prawa i regulacjami dotyczącymi bezpieczeństwa informacji
- zmiany ustalone w zabezpieczeniach i wynikające z nich zmiany w Deklaracji Stosowania
- wdrożenie i skuteczność zabezpieczeń zgodnie z programem audytu.

W wyniku przeprowadzonego auditu nadzoru może nastąpić:

- utrzymanie ważności certyfikatu
- utrzymanie ważności certyfikatu po pozytywnej ocenie przekazanych planów działań i/lub dowodów wykonania działań korekcyjnych/korygujących dla stwierdzonych niezgodności poprzez weryfikację dokumentów / audit dodatkowy
- zawieszenie / wznowienie / cofnięcie certyfikatu.

Działania w nadzorze prowadzone są wg trzyletniego programu auditów w celu systematycznego monitorowania obszarów i funkcji objętych zakresem systemu zarządzania.

10. Zawieszenie / cofnięcie ważności certyfikatu / ograniczenie zakresu / rozszerzenie zakresu / audit przejścia na nowe wymagania

10.1. Zawieszenie ważności certyfikatu może nastąpić w następujących przypadkach:

- certyfikowany system zarządzania Organizacji stale lub w poważnym stopniu nie spełnia wymagań certyfikacyjnych, w tym wymagań dotyczących skuteczności systemu zarządzania

- Organizacja nie wyraża zgody na przeprowadzenie auditów w nadzorze lub auditów dla ponownej certyfikacji z wymaganą częstością określoną w umowie z Organizacją
- na wniosek Organizacji
- stwierdzenia przekroczenia przez Organizację praw i obowiązków określonych w umowie z Organizacją
- stwierdzenia niespełnienia zasad dotyczących posługiwania się znakami certyfikowanego systemu
- niespełnienia w terminie zobowiązań finansowych wobec PCBC S.A.
- braku realizacji przez Organizację obowiązków określonych w umowie z Organizacją dotyczących powoływania się na certyfikat i certyfikowany system zarządzania
- wystąpienia w Organizacji incydentu w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG lub rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki in vitro oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE ; (dotyczy: PN-EN ISO 13485)
- wystąpienia incydentów takich jak poważny wypadek lub poważne naruszenie przepisów prawnych BHP, skutkujące koniecznością zaangażowania kompetentnego organu regulacyjnego, przekazana przez certyfikowanego Klienta lub uzyskana bezpośrednio przez zespół auditujący podczas auditu specjalnego; (dotyczy: PN-EN ISO 45001).

Zawieszenie ważności certyfikatu nie może przekraczać sześciu miesięcy. W trakcie zawieszenia, certyfikacja jest czasowo nieważna. W przypadku zawieszenia Certyfikatu, Organizacja powstrzymuje się od dalszego promowania swojej certyfikacji.

PCBC S.A. wznawia zawieszoną certyfikację, jeżeli kwestie, które spowodowały zawieszenie zostały rozwiązane przez Organizację.

10.2. Cofnięcie ważności certyfikatu może nastąpić w następujących przypadkach:

- stwierdzenia, że nie zostały rozwiązane w czasie ustalonym przez PCBC S.A. kwestie, które spowodowały zawieszenie
- stwierdzenia trwałego zaprzestania: prowadzenia działalności, świadczenia usług lub prowadzenia procesów objętych zakresem certyfikatu
- wystąpienia incydentów takich jak poważny wypadek lub poważne naruszenie przepisów prawnych BHP, skutkujące koniecznością zaangażowania kompetentnego organu regulacyjnego, (dotyczy: PN-EN ISO 45001)
- rozwiązania umowy z Organizacją.

Po cofnięciu certyfikatu, Organizacja jest zobowiązana do zaprzestania powoływania się na status Organizacji certyfikowanej i używania certyfikatów we wszystkich działaniach oraz dokumentach handlowych, promocyjnych, reklamowych.

10.3. Ograniczenie zakresu podanego w certyfikacie może nastąpić w następujących przypadkach:

- stwierdzenia, że nie zostały rozwiązane w czasie ustalonym przez PCBC S.A. kwestie, które spowodowały ograniczenie zakresu certyfikacji
- w celu wykluczenia tych części, które nie spełniają wymagań, kiedy Organizacja stale lub w poważnym stopniu nie spełnia wymagań certyfikacyjnych dla tych części zakresu certyfikacji
- na wniosek Organizacji.

Ograniczenie zakresu certyfikacji potwierdzone jest wystawieniem nowego certyfikatu z datą wydania od podjęcia decyzji o ograniczeniu ważności certyfikatu dotychczasowego. Ponadto Organizacja winna na żądanie PCBC S.A. zwrócić dotychczasowy certyfikat.

Zawieszenie / cofnięcie / ograniczenie zakresu certyfikatu poprzedzane jest odpowiednim pismem do Klienta informującym o konieczności zaprzestania posługiwania się certyfikatem i ewentualnym pisemnym ponagleniem dotyczącym zwrotu dokumentów certyfikacyjnych (jeśli wydane były w wersji papierowej) oraz z przypomnieniem o zaprzestaniu stosowania logo certyfikowanego systemu oraz znaku IQNET. Zawieszenie może przejść w cofnięcie certyfikatu po bezskutecznym powyższym działaniu.

Zawieszenie lub cofnięcie certyfikatu pociąga za sobą ten sam skutek dla wszystkich wydanych do niego załączników.

10.4. Rozszerzenie zakresu / obszaru certyfikacji

Rozszerzenie zakresu /obszaru już udzielonej certyfikacji następuje na wniosek Organizacji. Rozszerzenie wymaga złożenia „Wniosku o certyfikację w PCBC S.A.”, na podstawie przeglądu, którego określane są działania auditowe niezbędne do podjęcia decyzji o rozszerzeniu.

W celu oceny nowego zakresu / obszaru certyfikacji przeprowadzany jest audit specjalny lub działania auditowe dotyczące zgłoszonego rozszerzenia mogą być prowadzone w powiązaniu z auditem w nadzorze. Ww. rozszerzenie zakresu obejmuje podpisanie aneksu do umowy i może wiązać się z dodatkowymi kosztami po stronie klienta. Wydanie nowego certyfikatu następuje po przeprowadzonym audicie i pozytywnej decyzji PCBC S.A. Certyfikat wydawany jest w ramach ważności certyfikatu podstawowego. Certyfikowana Organizacja zobowiązana jest do anulowania poprzedniej wersji certyfikatu na zasadach u niej obowiązujących i do posługiwania się aktualną wersją dokumentu certyfikacyjnego.

10.5 Audit przejścia na nowe wymagania normy

Audit przejścia realizowany jest w przypadku opublikowania nowego wydania normy i jest on przeprowadzany zgodnie z wytycznymi zawartymi w komunikatach wydawanych przez PCA oraz w konsekwencji przez PCBC S.A.

Wytyczne obejmują m.in. elementy takie jak:

- okres przejściowy – czyli czas na dostosowanie systemu organizacji do nowego wydania normy
- przeprowadzenie przez organizację samooceny dot. gotowości przejścia na nowe wydanie normy

- informację, iż audit przejścia może być zrealizowany w ramach auditu nadzoru, auditu ponownej certyfikacji lub auditu dodatkowego
- konieczność doliczenia dodatkowego czasu auditu na działania związane z auditem przejścia.

W ramach auditu przejścia organizacja auditowana jest na zgodność zarówno z bieżącym jak i nowym wydaniem normy, celem oceny utrzymywania ciągłości działania systemu zarządzania.

11. Audit z krótkim terminem powiadamiania lub audit niezapowiedziany (audit specjalny)

Audit z krótkim terminem powiadamiania min. 14 dni przed oceną, lub audit niezapowiedziany to audit będący reakcją PCBC S.A. na:
- na skargi zainteresowanych stron do certyfikowanego systemu zarządzania organizacji/klienta
- w wyniku istotnych zmian wprowadzanych w organizacji/klienta
- w ramach dalszego postępowania z organizacją/klientem „zawieszonym”
- po powzięciu wiadomości o wystąpieniu poważnego incydentu, na przykład poważnego wypadku lub poważnego naruszenia przepisu prawa, w celu zbadania, czy nie doszło do pogorszenia działania systemu i czy jego funkcjonowanie jest skuteczne (dotyczy: PN-EN ISO 45001)
- w sytuacji gdy wyroby objęte zakresem certyfikacji wskazują na możliwą znaczącą wadliwość systemu zarządzania jakością (dotyczy: PN-EN ISO 13485)
- w sytuacji gdy PCBC S.A. znane są istotne informacje związane z bezpieczeństwem i działaniem wyrobów (dotyczy: PN-EN ISO 13485)
- gdy są wymagane na mocy przepisów (wymagań) prawnych wynikających z prawa publicznego lub są wymagane przez właściwy organ regulacyjny (dotyczy: PN-EN ISO 13485)
- na uzasadnione obawy jednostki odnośnie do wdrożenia działań korygujących lub odnośnie do zgodności z normą i wymaganiami przepisów (dotyczy: PN-EN ISO 13485).

W przypadku wystąpienia ww. sytuacji PCBC S.A. powiadamiania Klienta min. 14 dni przed oceną o przeprowadzeniu auditu z krótkim terminem powiadamiania, który nie wymaga zgody Organizacji. Skład zespołu auditującego zaakceptowany jest Prezesa Zarządu.

Audity niezapowiedziane realizowane są bez powiadomienia.

11.1. Audity z krótkim terminem powiadamiania lub audity niezapowiedziane w systemach zarządzania jakością wyrobów medycznych mogą być wymagane w sytuacji:

a) wystąpienia czynników zewnętrznych, takich jak:
   - wyroby objęte zakresem certyfikacji wskazujące na możliwą znaczącą wadliwość systemu zarządzania jakością
   - znane PCBC S.A. istotne informacje związane z bezpieczeństwem i działaniem wyrobów

b) wystąpienia istotnych zmian, które zostały przedłożone zgodnie z wymaganiami przepisów lub są znane PCBC S.A. i które mogą wpłynąć na decyzję dotyczącą stanu zgodności klienta z wymaganiami przepisów

c) gdy są wymagane na mocy wymagań prawnych wynikających z prawa publicznego lub przez właściwy organ regulacyjny

Poniżej przedstawiono przykłady takich zmian, które mogą być istotne i mające znaczenie dla PCBC S.A. podczas rozważania, czy wymagane jest przeprowadzenie auditu z krótkim terminem powiadamiania lub auditu niezapowiedzianego, chociaż zaleca się, aby żadne z tych zmian nie powodowały automatycznie przeprowadzenie auditu z krótkim terminem powiadamiania lub auditu niezapowiedzianego:

a) QMS – wpływ i zmiany:

- nowy właściciel
- rozszerzenie o nadzór nad produkcją i/lub projektem
- nowy obiekt, zmiana lokalizacji: zmiany w działaniach w lokalizacji zaangażowanej w działalność produkcyjną (np. przeniesienie działalności produkcyjnej do nowej lokalizacji lub centralizacja działań projektowania i/lub rozwoju dla kilku lokalizacji produkcyjnych)
- nowe procesy, zmiany w procesach: znaczące zmiany w procesach specjalnych (np. zmiana w produkcji ze sterylizacją przez dostawcę na sterylizację na miejscu lub zmiana w metodzie sterylizacji)
- zarządzanie QM, personel: zmiany określonych uprawnień przedstawiciela kierownictwa, które wpływają na:
  - skuteczność systemu zarządzania jakością lub zgodność z przepisami
  - zdolność i uprawnienia dla zapewnienia, że zwalniane są tylko bezpieczne i właściwe wyroby medyczne.

b) Zmiany związane z wyrobami:

- nowe wyroby, kategorie
- dodanie nowej kategorii wyrobów do zakresu produkcji w ramach systemu zarządzania jakością (np. dodanie sterylnych zestawów jednokrotnego użycia do dializy do istniejącego zakresu ograniczonego do sprzętu do hemodializy, lub dodanie obrazowania rezonansem magnetycznym do istniejącego zakresu ograniczonego do sprzętu ultradźwiękowego).

c) zmiany związane z QMS i wyrobami:

- zmiany w normach, przepisach
- działania dotyczące bezpieczeństwa wyrobów (post market surveillance, vigilance).

Przeprowadzenie auditu niezapowiedzianego lub auditu z krótkim terminem powiadamiania może także być konieczne wtedy, gdy CAB ma uzasadnione obawy odnośnie do wdrożenia działań korygujących lub odnośnie do zgodności z normą i wymaganiami przepisów.

12. Ponowna certyfikacja

Audit ponownej certyfikacji to audit przeprowadzany przez PCBC S.A. w trzecim roku, przed upływem daty ważności certyfikatu; stanowi podstawę do wydania decyzji o ponownym przyznaniu certyfikatu na okres trzech lat.

W przypadku gdy działania korekcyjne/korygujące wynikające z dużych niezgodności i dotyczące ponownej certyfikacji nie zostały wdrożone i zweryfikowane przed upływem daty ważności certyfikacji, PCBC S.A. może wznowić certyfikację w ciągu sześciu miesięcy, pod warunkiem

zakończenia niewykonanych działań dotyczących ponownej certyfikacji, w przeciwnym razie należy przeprowadzić co najmniej drugi etap auditu.

Ponowna certyfikacja rozpoczyna się od złożenia przez Organizację „Wniosku o certyfikację w PCBC S.A.". Warunkiem zachowania ciągłości ważności certyfikatu jest złożenie min. na trzy miesiące przed końcem ważności certyfikatu ww. wniosku.

Dalsze postępowanie zgodnie z pkt. 3, 4, 5 niniejszego dokumentu.

Celem auditu dla ponownej certyfikacji jest potwierdzenie przez PCBC S.A. w Organizacji:

a) stałej zgodności i skuteczności systemu zarządzania jako całości
b) stałej odpowiedniości i przydatności systemu zarządzania do zakresu certyfikacji
c) stałego spełnienia wszystkich wymagań zastosowanej normy lub innego dokument normatywnego.

Audit ponownej certyfikacji obejmuje wyniki funkcjonowania systemu zarządzania wraz z uwzględnieniem wyników auditów w nadzorze.

Audit ponownej certyfikacji może wymagać przeprowadzenia pierwszego etapu auditu, w przypadku znaczących zmian w systemie zarządzania Klienta lub w kontekście, w którym działa system zarządzania (np. zmiany legislacyjne) w odniesieniu do poprzedniego auditu.

Audit ponownej certyfikacji przeprowadzany jest w Organizacji Klienta i obejmuje m.in.:

a) skuteczność systemu zarządzania jako całości w świetle zmian wewnętrznych i zewnętrznych oraz jego stałą odpowiedniość i przydatność do zakresu certyfikacji
b) wykazanie zaangażowania w utrzymywaniu skuteczności oraz doskonaleniu systemu zarządzania w celu poprawy ogólnego sposobu działania
c) skuteczność systemu zarządzania pod względem osiągania celów przez certyfikowanego Klienta i zamierzonych wyników odpowiedniego systemu(-ów) zarządzania
d) przegląd raportów z poprzednich auditów nadzoru
e) wyniki funkcjonowania systemu zarządzania w ostatnim cyklu certyfikacji.

Decyzję w sprawie udzielenia ponownej certyfikacji PCBC S.A. podejmuje na podstawie:

a) raportu z auditu wraz z komentarzami do niezgodności i gdzie to jest stosowane, podjętych przez Klienta korekcji i działań korygujących
b) zalecenia, czy udzielić czy nie udzielić certyfikacji łącznie ze wszystkimi warunkami i spostrzeżeniami
c) pozytywnej weryfikacji raportu przeprowadzonej przez Weryfikatora raportów
d) wszelkich mających zastosowanie informacji (np. informacji dostępnych publicznie)
e) wyników przeglądu systemu w okresie certyfikacji
f) ewentualnych skarg otrzymanych od zainteresowanych certyfikacją.

13. Organizacje wielooddziałowe

Certyfikacja wielooddziałowa może być stosowana w Organizacjach posiadających wiele zakładów produkcyjnych lub filii, które spełniają tylko funkcję ich oddziałów.

Certyfikacja wielooddziałowa jest możliwa w przypadku spełnienia m.in. poniższych kryteriów:

a) wszystkie lokalizacje są powiązane z centralą pod względem prawnym
b) we wszystkich lokalizacjach ustanowiono, wdrożono i utrzymuje się jednolity system zarządzania
c) nadzór centralny nad systemem zarządzania sprawuje wyznaczony przez Centrale przedstawiciel najwyższego kierownictwa
d) przeprowadzanie przeglądów zarządzania i auditów wewnętrznych przez kierownictwo we wszystkich zakładach, filiach.

W przypadku systemu zarządzania funkcjonującego w wielu oddziałach, PCBC S.A. ustala, czy dozwolone jest próbkowanie. Próbkowanie grupy oddziałów jest dozwolone w przypadku, gdy każdy z oddziałów realizuje bardzo podobne procesy/działania. Wielkość próbki jest wybierana zgodnie z wymaganiami akredytacyjnymi w poszczególnych programach certyfikacji.

13.1. Dodatkowe wymagania dla Organizacji wielooddziałowych w odniesieniu systemu zarządzania bezpieczeństwem informacji.

W przypadku, gdy Klient ma kilka lokalizacji zgodnych z poniższymi kryteriami:

a) wszystkie lokalizacje działają w ramach tego samego SZBI, który jest centralnie administrowany i audytowany oraz poddawany centralnemu przeglądowi zarządzania
b) wszystkie lokalizacje są włączone do programu wewnętrznego audytu SZBI Organizacji Klienta
c) wszystkie lokalizacje są włączone do programu przeglądu kierownictwa SZBI Organizacji Klienta.

PCBC S.A. stosuje oparte na próbkowaniu podejście do auditu certyfikującego w wielu lokalizacjach.

Próbka obejmująca reprezentatywną liczbę lokalizacji uwzględnia:

a) wyniki audytów wewnętrznych w siedzibie głównej i innych lokalizacjach
b) wyniki przeglądu zarządzania
c) różnice w wielkości lokalizacji
d) różnice pomiędzy lokalizacjami wynikające z celów biznesowych
e) złożoność systemów informacyjnych w poszczególnych lokalizacjach
f) różnice w praktykach pracy
g) różnice w prowadzonych działaniach
h) różnice w przeznaczeniu i działaniu zabezpieczeń
i) potencjalne wzajemne oddziaływanie z krytycznymi systemami informacyjnymi lub systemami przetwarzającymi informacje wrażliwe
j) różnice w wymaganiach prawnych
k) aspekty geograficzne i kulturowe
l) ryzyko obecne w lokalizacjach

m) incydenty związane z bezpieczeństwem informacji w konkretnych lokalizacjach

Reprezentatywna próbka wybierana jest ze wszystkich lokalizacji z zakresu SZBI Organizacji Klienta. Wybór uwzględnia zarówno czynniki opisane powyżej, jak również element losowy.

Każda lokalizacja tymczasowa, do której Klient certyfikacji lub certyfikowana Organizacja dostarcza swoje wyroby lub usługi jest włączona do oceny auditu certyfikującego i programu auditów. Ponadto każda lokalizacja włączona do SZBI, obciążona znaczącym ryzykiem, jest auditowana przed certyfikacją. W przypadku stwierdzenia niezgodności w siedzibie głównej lub w jednej z lokalizacji, procedurę działań korygujących stosuje się w siedzibie głównej oraz we wszystkich lokalizacjach objętych certyfikacją.

W ramach właściwego auditowania systemu opracowywany jest program wyboru oddziałów, przy założeniu, że niezależnie od rodzaju auditu (początkowej certyfikacji, nadzoru, ponownej certyfikacji) zawsze auditowana jest Centrala. W okresie 3 lat, lokalizacje Klienta poddawane są procesowi certyfikacji / ponownej certyfikacji.

13.2. Dodatkowe wymagania dla Organizacji wielooddziałowych w odniesieniu systemu zarządzania jakością dla wyrobów medycznych.

Oddziały, w których prowadzone są projektowanie i rozwój oraz produkcja wyrobów medycznych nie są poddawane próbkowaniu.

13.3. Dodatkowe wymagania dla Organizacji wielooddziałowych w odniesieniu do systemu zarządzania bezpieczeństwem żywności FSMS.

1. Organizacja posiadająca wiele lokalizacji to organizacja posiadająca określoną funkcję centralną, w której planuje się, nadzoruje lub zarządza określonymi działaniami FSMS, oraz sieć oddziałów, w których takie działania są w całości lub częściowo realizowane. Przykładami organizacji wielooddziałowych są:
    a) organizacje działające na zasadzie franczyzy
    b) grupy producenckie (dla kategorii A i B)
    c) przedsiębiorstwo produkcyjne posiadające jeden lub więcej zakładów produkcyjnych oraz sieć biur sprzedaży
    d) organizacje usługowe posiadające wiele oddziałów oferujących podobne usługi
    e) organizacje posiadające wiele oddziałów
2. Stosowanie próbkowania w organizacjach wielooddziałowych dozwolone jest dla kategorii A i B.
3. Stosowanie pobierania próbek w organizacjach wielooddziałowych jest dozwolone także w przypadku kategorii F i G oraz dla kategorii E wyłącznie w przypadku zakładów typu ponownego odgrzewania (np. catering dotyczący imprez, kawiarnie, puby), jak również wyłącznie w przypadku obiektów o ograniczonym przygotowaniu lub gotowaniu (np. ogrzewanie, smażenie). W przypadku organizacji wielooddziałowej liczącej 20 oddziałów lub mniej, auditowi podlegają wszystkie oddziały.
4. Próbkowanie organizacji wielooddziałowych obejmuje wszystkie rodzaje działalności.

5. Zakres certyfikacji obejmuje procesy FSMS zidentyfikowane i wdrożone w każdym oddziale objętym próbkowaniem.
6. Co najmniej raz w roku przeprowadzany jest audit Centrali przed auditami wybranych oddziałów.

14. Skargi / Odwołania

W przypadku złożenia przez Klienta skargi / odwołania, PCBC S.A. postępuje zgodnie trybem postępowania zamieszczonym na stronie www.pcbc.gov.pl.

15. Ochrona informacji i praw własności Klienta

Cały personel PCBC S.A., zarówno wewnętrzny jak i zewnętrzny jest zobowiązany do nieujawniana żadnych informacji dotyczących Klientów.

Pracownicy są odpowiednio przeszkoleni, pouczeni oraz podpisują odpowiednie zobowiązanie o zachowaniu poufności informacji. Auditorzy / eksperci / weryfikatorzy raportów oraz członkowie Komitetu dla Zapewnienia Bezstronności, podpisują również zobowiązanie o zachowaniu poufności informacji.
PCBC S.A. w przypadku udostępniania danych Klientów, jednostkom: PCA, IQNET w zakresie posiadanej akredytacji podczas prowadzonych ocen, dokonywać będzie w miarę możliwości niezwłocznego powiadomienia Klienta przed udzieleniem takich informacji.

16. Opłaty

Opłaty za czynności certyfikacyjne są kalkulowane zgodnie z instrukcją finansową IBC 01.01.

Koszty procesu certyfikacji uwzględniają:

a) Opłaty stałe w procesie certyfikacji systemów zarządzania (opłatę wstępną, opłatę związaną z przeprowadzanym procesem certyfikacji, wydanie certyfikatu, opłatę roczną za uczestnictwo w systemie certyfikowanych Organizacji)
b) Badanie auditowe, przy każdym audicie w cyklu (audit początkowej certyfikacji / audit nadzoru / audit ponownej certyfikacji). Na koszt badań auditowych w tym czas pracy auditorów mają wpływ z następujące czynniki:
   - wielkość zatrudnienia (Tabela nr 1)
   - doświadczenie Organizacji we wdrażaniu systemów zarządzania (posiadane certyfikaty)
   - złożoność Organizacji i realizowanych procesów, zastosowane możliwe wyłączenia, zakres certyfikacji, posiadane oddziały, lokalizacje, liczba oddziałów objętych systemem, rozproszenie geograficzne
   - obszar funkcjonowania Organizacji.

Przy sporządzaniu ofert uwzględniane są czynniki zwiększające i zmniejszające mogące wpływać zarówno na koszty certyfikacji jak i na planowanie czasu pracy auditorów.

Przykłady czynników zwiększających czas pracy auditorów: skomplikowana logistyka obejmująca więcej niż jeden budynek lub lokalizację, w których prowadzona jest działalność,

np. konieczność auditowania samodzielnego Centrum Projektowania, personel mówiący więcej niż jednym językiem (co powoduje konieczność korzystania z tłumacza(-y) lub wyklucza możliwość prowadzenia niezależnych działań przez poszczególnych auditorów), duży obszar objęty auditem w porównaniu z liczbą personelu (np. las), duża liczba przepisów związanych z działalnością (np. żywność, lekarstwa, lotnictwo, energetyka jądrowa, itd.), system obejmuje bardzo skomplikowane procesy lub stosunkowo dużą liczbę nietypowych działań, działania, które wymagają wizytowania oddziałów tymczasowych w celu weryfikacji działań w oddziale (-łach) stałym(-ych), którego(-ych) system zarządzania podlega certyfikacji.

Przykłady czynników zmniejszających czas pracy auditorów: Klient nie jest „odpowiedzialny za projektowanie", lub w zakresie nie ma innych elementów normy (tylko QMS), niskie ryzyko związane z wyrobami lub procesami (dla EMS i H&SMS jest to podane w Tabeli 1), bardzo mały oddział w stosunku do liczby pracowników (np. wyłącznie kompleks biurowy), dojrzałość systemu zarządzania, audit połączony systemu zintegrowanego składającego się z dwóch lub więcej kompatybilnych systemów zarządzania, wcześniejsza znajomość systemu zarządzania Klienta (np. już certyfikowanego według innej normy przez tę samą CAB), gotowość Klienta do certyfikacji (np. Klient już jest certyfikowany lub uznany zgodnie z innym programem strony trzeciej), w składzie personelu znajdują się osoby pracujące „poza lokalizacją", np. handlowcy, kierowcy, personel wykonujący usługi, itd., oraz możliwe jest gruntowne auditowanie zgodności ich działań z systemem w formie przeglądu zapisów, działania o niskiej złożoności.

Tabela nr 1. Wytyczne do określania czasu pracy auditorów do oceny w procesie certyfikacji (liczby dni audytowych).

Zależność między efektywną liczbą personelu i czasem auditu								
Lp.	Efektywna liczba personelu	Czas auditu certyfikacji początkowej Etap I + Etap II. (liczba dni auditowych)						
		QMS / ABMS / BCMS	ISMS	MDMS	EMS / H&SMS			
					Wys.	Śred.	Nisk.	Ogr. [1)]
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**
1	1-5	1,5	5	3	3	2,5	2,5	2,5
	6-10	2	5	4	3,5	3	3	3
2	11-15	2,5	7	4,5	4,5	3,5	3	3
	16-25	3	7	5	5,5	4,5	3,5	3
3	26-45	4	8,5	6	7	5,5	4	3
4	46-65	5	10	7	8	6	4,5	3,5
5	66-85	6	11	8	9	7	5	3,5
6	86-125	7	12	10	11	8	5,5	4

7	126-175	8	13	11	12	9	6	4,5
8	176-275	9	14	12	13	10	7	5
9	276-425	10	15	13	15	11	8	5,5
10	426-625	11	16,5	14	16	12	9	6
11	626-875	12	17,5	15	17	13	10	6,5
12	876-1175	13	18,5	16	19	15	11	7
13	1176-1550	14	19,5	17	20	16	12	7,5
14	1551-2025	15	21	18	21	17	12	8
15	2026-2675	16	22	19	23	18	13	8,5
16	2676-3450	17	23	20	25	19	14	9
17	3451-4350	18	24	21	27	20	15	10
18	4351-5450	19	25	22	28	21	16	11
19	5451-6800	20	26	23	30	23	17	12
20	6801-8500	21	27	24	32	25	19	13
21	8501-10700	22	28	25	34	27	20	14
22	> 10700	Według powyższej tendencji						
1) Nie dotyczy H&SMS								
Wartości podane w wierszach od 1 do 22 określają ogólne ramy czasowe będące punktem wyjścia do planowania czasu trwania auditu.								

17. Programy certyfikacji

- DBC 17-Program 1 Program certyfikacji systemu klienta na zgodność z wymaganiami normy PN-EN ISO 9001
- DBC 17-Program 2 Program certyfikacji systemu klienta na zgodność z wymaganiami normy PN-EN ISO 13485
- DBC 17-Program 3 Program certyfikacji systemu klienta na zgodność z wymaganiami normy PN-EN ISO 14001
- DBC 17-Program 5 Program certyfikacji systemu zarządzania bezpieczeństwem żywności na zgodność z wymaganiami normy PN-EN ISO 22000
- DBC 17-Program 6 Program certyfikacji systemu klienta na zgodność z wymaganiami normy PN-EN ISO/IEC 27001
- DBC 17-Program 7 Program certyfikacji systemu zarządzania bezpieczeństwem i higieną pracy na zgodność z wymaganiami normy PN-EN ISO 45001
- DBC 17-Program 8 Program certyfikacji systemu zarządzania działaniami antykorupcyjnymi PN-ISO 37001 / ISO 37001

- DBC 17-Program 11 Program certyfikacji systemu zarządzania energią klienta na zgodność z wymaganiami normy PN-EN ISO 50001
- DBC 17-Program 12 certyfikacji systemu zarządzania ciągłością działania klienta na zgodność z wymaganiami normy PN-EN ISO 22301.