INFORMATOR ISOCERT
„Certyfikacja systemów zarządzania”

WYDANIE: 2-2024
DATA WYDANIA: 16.04.2024

1. INFORMACJE DOTYCZĄCE DZIAŁALNOŚCI CERTYFIKACYJNEJ I WYMAGAŃ

ISOCERT jest jednostką certyfikującą systemy zarządzania organizacji dostępną dla wszystkich wnioskodawców.
Nie są stawiane nieuzasadnione wymagania finansowe, a dostęp do certyfikacji nie zależy od wielkości organizacji ani członkostwa w jakimkolwiek stowarzyszeniu lub ugrupowaniu.
Działalność ISOCERT finansowana jest z działalności gospodarczej.
ISOCERT prowadzi księgowość i sprawozdania statystyczne zgodnie z obowiązującymi w tym zakresie przepisami.

Zasady certyfikacji systemów zarządzania opracowane zostały na podstawie:

- PN-EN ISO/IEC 17021-1:2015 "Ocena zgodności. Wymagania dla jednostek prowadzących audity i certyfikację systemów zarządzania”
- PN-EN ISO/IEC 17021-2 „Ocena zgodności — Wymagania dla jednostek prowadzących audity i certyfikację systemów zarządzania — Część 2: Wymagania dotyczące kompetencji do auditowania i certyfikacji systemów zarządzania środowiskowego”
- PN-EN ISO/IEC 17021-3 „Ocena zgodności — Wymagania dla jednostek prowadzących audity i certyfikację systemów zarządzania — Część 3: Wymagania dotyczące kompetencji do auditowania i certyfikacji systemów zarządzania jakością”
- PKN-ISO/IEC TS 17021-10:2019-11 Ocena zgodności -- Wymagania dla jednostek prowadzących audity i certyfikację systemów zarządzania -- Część 10: Wymagania dotyczące kompetencji do auditowania i certyfikacji systemów zarządzania bezpieczeństwem i higieną pracy
- PN-EN ISO/IEC 27006:2021-05 Technika informatyczna - Techniki bezpieczeństwa - Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji.
- PN-EN ISO 9001:2015 „Systemy zarządzania jakością – Wymagania”
- PN-EN ISO 9000:2006 „Systemy Zarządzania Jakością - Podstawy i terminologia”
- PN-EN ISO 14001:2015 „Systemy zarządzania środowiskowego. Wymagania i wytyczne stosowania.”
- PN-EN ISO 45001:2024 “Systemy zarządzania bezpieczeństwem i higieną pracy - Wymagania iwytyczne stosowania”
- PN-EN ISO/IEC 27001:2017-06 „Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania”.
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- EA-7/04 „Zgodność z prawem jako część akredytowanej certyfikacji w odniesieniu do ISO 14001:2015”
- IAF MD1:2023 Dokument obowiązkowy IAF dotyczący auditu i certyfikacji systemów zarządzania organizacji wielooddziałowych
- IAF MD 2:2023 „Dokument obowiązkowy IAF dotyczący przenoszenia akredytowanej certyfikacji systemów zarządzania”
- IAF MD 4:2023 „Dokument obowiązkowy IAF dotyczący stosowania technologii informacyjno-komunikacyjnych („ICT”) do celów prowadzenia auditów/ocen”
- IAF MD 5:2023 „Dokument obowiązkowy IAF dotyczący ustalenia czasu auditu systemów zarządzania jakością, środowiskowego oraz bezpieczeństwa i higieny pracy”
- IAF MD 11:2023 „Dokument obowiązkowy IAF dotyczący stosowania normy ISO/IEC 17021 w auditach zintegrowanych systemów zarządzania”
- IAF MD 22:2023 „Stosowanie normy ISO/IEC 17021-1 w certyfikacji systemów zarządzania bezpieczeństwem i higieną pracy (OH&SMS)”
- IAF MD23:2023 „Nadzór nad podmiotami działającymi w imieniu akredytowanych jednostek certyfikujących systemy zarządzania”
- IAF ID3:2011 „Dokument informacyjny IAF do zarządzania zdarzeniami nadzwyczajnymi i okolicznościami wpływającymi na Jednostki Akredytujące, Jednostki certyfikujące systemy zarządzania i certyfikowane organizacje”.

2. PRAWA I OBOWIĄZKI ORGANIZACJI

Organizacja ma prawo do:

- wnioskowania o zmianę poszczególnych członków zespołu auditującego, przedstawiając racjonalne uzasadnienie np. sytuacji występującego konfliktu interesów, nieetycznych zachowań,

- powoływania się na certyfikacje zgodnie z zasadami określonymi w niniejszym informatorze,
- stosowania znaków certyfikacji , zgodnie z zasadami określonymi w niniejszym informatorze,
- wymagania od ISOCERT zachowania poufności wszelkich informacji związanych z certyfikacją systemu zarządzania Organizacji,
- otrzymywania od ISOCERT informacji dotyczących zmian uregulowań związanych z certyfikacją,
- odwołań i reklamacji, zgodnie z zasadami określonymi w niniejszym informatorze,
- rozszerzenia swojego zakresu określonego w przyznanym przez ISOCERT certyfikacie o wymagania kolejnych dokumentów odniesienia lub o nowy obszar objęty systemem,
- wystąpienia z wnioskiem o przerwanie procesu certyfikacji, zawieszenie ważności certyfikacji, ponowną ocenę lub wznowienie ważności certyfikacji.

Organizacja zgłaszająca się do certyfikacji zobowiązuje się, że:

- umożliwi ISOCERT przeprowadzanie auditu początkowej certyfikacji w ustalonym terminie.
- umożliwi ISOCERT przeprowadzanie auditów w nadzorze przynajmniej raz w roku w nieprzekraczalnych terminach ustalonych w dokumentach certyfikacyjnych z zastrzeżeniem, że data pierwszego auditu nadzoru po początkowej certyfikacji nie powinna być późniejsza niż 12 miesięcy od daty podjęcia decyzji o udzieleniu certyfikacji.
- umożliwi ISOCERT przeprowadzanie auditów specjalnych w przypadku powstania zasadnych wątpliwości co do spełnienia przez Organizację warunków certyfikacji; wystąpieniu poważnego incydentu związanego z BHP, np.: poważnego wypadku lub poważnego naruszenia przepisu prawa (dotyczy SZBHP); w przypadku rozszerzenia zakresu certyfikacji na wniosek Organizacji.
- zapewni warunki do działania obserwatorów obecnych na auditach (np. auditorów PCA lub auditorów szkolonych).
- będzie utrzymywać system zarządzania zgodny z wymaganiami normy, na zgodność z którą został wydany certyfikat.
- będzie regularnie prowadzić rejestrację wszelkich reklamacji oraz podejmować w tym zakresie korekcje i/lub działania korygujące.
- będzie powiadamiać ISOCERT o wszelkich zmianach, które mogą wpływać na zgodność systemu zarządzania, w tym: statusu prawnego, handlowego, organizacyjnego lub własnościowego, struktury organizacyjnej i zarządzania, zakresu działania objętego certyfikowanym systemem zarządzania i miejsc prowadzenia działalności, głównych zmian w systemie, adresów kontaktowych.
- będzie bezzwłocznie informować ISOCERT o wystąpieniu poważnego incydentu lub naruszenia przepisów powodującego konieczność zaangażowania kompetentnego organu regulacyjnego (dotyczy SZBHP)
- nie będzie składać lub dopuszczać do składania jakichkolwiek wprowadzających w błąd oświadczeń odnoszących się do swojej certyfikacji.
- nie będzie stosować lub dopuszczać do stosowania certyfikatu/ów lub jakiejkolwiek jego części w sposób wprowadzający w błąd.
- po zawieszeniu lub cofnięciu certyfikacji zaprzestanie stosowania certyfikatu/ów oraz znaków ISOCERT we wszystkich materiałach reklamowych zawierających powoływanie się na certyfikację, zgodnie z poleceniem ISOCERT.
- będzie uaktualniać wszystkie materiały reklamowe w przypadku ograniczenia zakresu certyfikacji.
- zwróci w terminie 7 dni wystawiony przez ISOCERT certyfikat/y, w przypadku decyzji o cofnięciu lub ograniczeniu zakresu certyfikacji.
- nie będzie dopuszczać do powoływania się na certyfikację w taki sposób, aby sugerowało to, że jednostka certyfikuje wyrób, usługę lub proces.
- nie będzie sugerować, że certyfikacja odnosi się do działalności, które są poza zasięgiem certyfikacji.
- będzie stosować się do decyzji ISOCERT podejmowanych w związku ze zmianami wymagań procesu certyfikacyjnego.
- będzie stosować znak certyfikacji oraz powoływać się na certyfikacje wyłącznie według zasad określonych w dokumencie „Specyfikacja oraz użytkowanie znaku certyfikacji”

3. PROCES CERTYFIKACJI

W przypadku certyfikacji systemów zarządzania, certyfikacji może być poddany wdrożony w organizacji system, to znaczy, że:

- istnieje wystarczająca ilość obiektywnych dowodów dokumentujących skuteczne wdrożenie systemu,
- przeprowadzono audity wewnętrzne,
- dokonano przeglądu systemu przez kierownictwo.
- istnieją wystarczające dowody na to, że ustalenia dotyczące auditów wewnętrznych i przeglądów zarządzania zostały wdrożone, są skuteczne i będą nadal utrzymywane.

3.1 Wniosek o certyfikację

„Wniosek o certyfikację” dostępny jest na stronie internetowej www.isocert.org.pl.
Wypełnienie i przesłanie przez organizację „Wniosku o certyfikację” nie zobowiązuje jej do podpisania

umowy na prowadzenie procesu certyfikacji przez ISOCERT.
Wypełniony „Wniosek o certyfikację" dostarcza ISOCERT niezbędne informacje do ustalenia:

- pożądanego zakresu certyfikacji,
- ogólnej charakterystyki wnioskującej organizacji, w tym jej nazwy i adresu (adresów) jej fizycznych lokalizacji, ustalenia funkcji centralnej, znaczących aspektów jej procesów i działań wraz z podziałem na lokalizacje w tym informację dotyczącą oddziałów tymczasowych oraz wirtualnych oraz wszelkich mających zastosowanie zobowiązań prawnych,
- potwierdzenie, że w całej organizacji jest wdrożony pojedynczy system zarządzania,
- ogólnych informacji, stosownie do wnioskowanego obszaru certyfikacji, dotyczących wnioskującej organizacji, takich jak jej działalność, zasoby ludzkie i techniczne, funkcje i powiązania w większej korporacji, jeżeli takie są,
- informacji dotyczących wszystkich podzlecanych procesów stosowanych przez organizację, które mogą oddziaływać na zgodność z wymaganiami,
- norm lub innych wymagań, w odniesieniu do których organizacja wnioskująca ubiega się o certyfikację,
- informacji dotyczących korzystania z konsultacji w odniesieniu do systemu zarządzania.

Dodatkowo w zakresie BHP:

- kluczowych zagrożeń i ryzyk BHP związanych z procesami, najważniejszych materiałów niebezpiecznych, wszelkich istotnych obowiązków prawnych ze wskazaniem jakiej lokalizacji one dotyczą
- informacji odnoście wystąpienia poważnego incydentu lub naruszenia przepisów powodujący konieczność zaangażowania kompetentnego organu regulującego
- informacje odnośnie różnic w działalności każdego oddziału
- informacji odnośnie liczby firm (pod)wykonawców i ich pracowników wraz z uszczegółowieniem jakie czynności realizują
- informacji odnoście wypadkowości oraz zapadalności na choroby zawodowe

Dodatkowo w zakresie EMS:

- aspektów środowiskowych i zezwoleń środowiskowych
- potwierdzenia dot. większej wrażliwości w odbiorze środowiska, dodatkowych/nadzwyczajnych aspektów środowiska, dodatkowych/nadzwyczajnych pozwoleń/przepisów dla sektora odpowiadającego Organizacji

Dodatkowo w zakresie ISMS:

- informacje dotyczące wysokości ryzyka w zakresie bezpieczeństwa informacji,
- podjętych działań w organizacji w związku z oceną ryzyka,
- informacje dotyczące deklaracji stosowania
- informacje odnośnie lokalizacji zapasowych, miejsc odzyskiwania danych po awarii, krytyczności sektorów biznesowych, procesów i zadań, poziomu ustanowienia systemu, złożoności infrastruktury, zależności od zlecania na zewnątrz i dostawców, rozwoju systemów informatycznych

„Wniosek o certyfikację" powinien także zawierać informację na temat danych, które nie mogę zostać udostępnione jednostce ponieważ zawierają informacje poufne lub wrażliwe.
ISOCERT rozpatruje „Wniosek o certyfikację" zwracając szczególną uwagę na aspekty niezależności, bezstronności i eliminacji przyczyn potencjalnego konfliktu interesów. W przypadku istnienia możliwości przeprowadzenia początkowej certyfikacji ISOCERT przygotowuje i wysyła do Organizacji ofertę/umowę o przeprowadzenie procesu certyfikacji.
W przypadku braku możliwości przeprowadzenia procesu certyfikacji Organizacja wnioskująca jest informowana pisemnie/mailowo (w zależności od formy złożenia wniosku przez Organizację) o przyczynie odmowy przyjęcia wniosku.
Istnieje możliwość opracowania oferty bez formalnego złożenia przez organizację „Wniosku o certyfikację", na podstawie pisemnych lub ustnych informacji przekazanych przez organizację.
Opłaty związane z certyfikacją, nadzorem oraz ponowną certyfikacją ponosi certyfikowana Organizacja.
Opłaty uzależnione są od wielkości organizacji, a cena danego auditu ustalana jest w zależności od stopnia złożoności organizacji i innych czynników mających zastosowanie w Organizacji. Liczba auditoro-dni wyliczana jest według zasad określonych w szczegółowych instrukcjach dotyczących poszczególnych programów certyfikacji. ISOCERT przygotowuje i wysyła do organizacji umowę na prowadzenie procesu certyfikacji załączając dokument „Specyfikacja oraz użytkowanie znaku certyfikacji".

3.2 Audit początkowej certyfikacji

Audit początkowej certyfikacji przeprowadzany jest w dwóch etapach. Terminy I i II etapu auditu zaplanowane są w uzgodnieniu z organizacją. W przypadku, kiedy auditor po I etapie auditu stwierdzi możliwość przeprowadzenia auditu uzgadnia dogodny termin w porozumieniu z certyfikowana organizacją. Dopuszcza się wykonanie II etapu auditu bezpośrednio po I etapie (wyłącznie w przedsiębiorstwach nie przekraczających w efektywnej licznie personelu 10 etatów), z uwzględnieniem faktu, że zostały osiągnięte cele I etapu auditu.

3.2.1 I etap auditu

I etap auditu obejmuje:

- auditowanie dokumentacji organizacji,
- ocenę lokalizacji klienta i specyficznych dla lokalizacji warunków oraz przeprowadzenie rozmów z personelem organizacji w celu określenia gotowości do II etapu auditu,
- przeprowadzenie przeglądu statusu organizacji i zrozumienia przez niego wymagań normy, zwłaszcza w odniesieniu do identyfikacji kluczowych aspektów sposobu działania lub znaczących aspektów, procesów, celów i działania systemu zarządzania,
- zebranie niezbędnych informacji dotyczących zakresu systemu zarządzania, procesów, lokalizacji klienta oraz związanych z nimi statutowych i prawnych aspektów oraz zgodności (np. aspektów jakościowych, środowiskowych, prawnych działalności organizacji, związane z nimi ryzyko, itp.),
- przeprowadzenie przeglądu przydziału zasobów do II etapu auditu i uzgodnienia z organizacją szczegółów II etapu,
- skoncentrowanie się na zaplanowaniu II etapu auditu poprzez osiągniecie wystarczającego zrozumienia systemu zarządzania organizacji i działalności w lokalizacji w kontekście możliwych znaczących aspektów,
- ocenę czy planowane i realizowane audity wewnętrzne i przeglądy zarządzania oraz czy poziom wdrożenia systemu zarządzania uzasadnia gotowość organizacji do drugiego etapu auditu,
- opracowanie planu II etapu auditu.

Dodatkowo w przypadku auditu ISMS I etap auditu obejmuje:

- ocenę czy oszacowane ryzyko bezpieczeństwa informacji (szczególnie w obszarze ryzyka krytycznego) właściwie odzwierciedla zakres działalności organizacji i wymagań ISO 27001,
- sprawdzenie, czy w ocenie ryzyka uwzględniono interfejsy z usługami lub działalnością, które nie w pełni wchodzą w zakres ISMS i czy zostały one ujęte w ramy ISMS.

W przypadku auditu zintegrowanego systemu zarządzania może być przeprowadzona sesja planowania przed rozpoczęciem I etapem auditu lub w jego trakcie, w celu potwierdzenia integracji systemu.

ISOCERT informuje z wyprzedzeniem o składzie zespołu auditorów wyznaczonych do przeprowadzenia auditu. Organizacja ma prawo zgłosić zastrzeżenie do składu auditorów lub żądać dodatkowych informacji o członkach zespołu auditorów. Z przeprowadzonego I etapu auditu organizacja otrzymuje „Ustalenia z I etapu auditu". Po przeprowadzeniu I etapu, ISOCERT może w porozumieniu z organizacją przesunąć terminu II etapu auditu lub wprowadzić zmiany w przygotowaniach do II etapu auditu.

W przypadku, jeśli w Organizacji zajdą znaczące zmiany wpływające na system zarządzania może okazać się koniecznie powtórzenie I etapu auditu lub jego części. Wyniki I etapu mogą prowadzić do przesunięcia lub odwołania II etapu auditu początkowej certyfikacji.

3.2.2 II etap auditu

Na podstawie ustaleń z I etapu auditu Auditor wiodący opracowuje „Plan auditu".

Planu auditu auditor wiodący przesyła organizacji z wyprzedzeniem umożliwiającym zgłoszenie uwag przez organizację przed auditem w organizacji.

II etap auditu rozpoczyna się spotkaniem otwierającym. Spotkanie otwierające ma służyć przedstawieniu celu oraz zakresu auditu, omówiony powinien zostać plan auditu przygotowany przez auditora wiodącego, ogólnie działania jakie będą wykonywane w jego trakcie. W spotkaniu otwierającym powinny wziąć udział osoby odpowiedzialne za główne funkcje lub procesy, które będą auditowane, z możliwością zadawania pytań dotyczących bezpośrednio czynności auditowych. Na spotkaniu otwierającym powinno być obecne kierownictwo certyfikowanej organizacji.

II etap auditu (w programach QMS, EMS, ISMS, OHS) obejmuje co najmniej:

- zebranie informacji i dowodów zgodności z wymaganiami odpowiedniej normy systemu zarządzania,
- monitorowanie, pomiary, raportowanie i przeglądanie osiągnięć w odniesieniu do kluczowych celów i zadań (wg stosownej normy systemu zarządzania),
- system zarządzania i sposób działania pod względem zgodności z prawem,
- kontrolę operacyjną procesów klienta,
- audity wewnętrzne i przeglądy zarządzania,
- odpowiedzialność kierownictwa za politykę organizacji,
- powiązanie pomiędzy wymaganiami normatywnymi, polityką, celami i zadaniami dotyczącymi osiągnięć (wg stosownej normy systemu zarządzania), mającymi zastosowanie przepisami prawnymi,

odpowiedzialnością, kompetencjami personelu, działaniami, procedurami, danymi dotyczącymi osiągnięć oraz ustaleniami i wnioskami z auditów wewnętrznych.

Dodatkowo w przypadku certyfikacji ISMS:

- wybór celów stosowania zabezpieczeń oraz zabezpieczeń, w oparciu o procesy oceny ryzyka i postępowania z ryzykiem
- wdrożenie zabezpieczeń, biorąc pod uwagę wykonane przez organizacje pomiary skuteczności zabezpieczeń, w celu określenia, czy zabezpieczenia są wdrożone i skuteczne w osiąganiu określonych celów
- wykazanie, że analiza zagrożeń bezpieczeństwa ma związek z działalnością organizacji klienta i jest odpowiednia dla tej działalności
- ustalenie czy procedury organizacji klienta dotyczące identyfikacji, sprawdzenia i oceny związanych z bezpieczeństwem informacji zagrożeń dla aktywów, podatności i skutków oraz wyniki ich wdrożenia są zgodne z polityką organizacji klienta, celami i zadaniami.

Auditorzy przeprowadzają badanie funkcjonowania SZ organizacji zgodnie z planem auditu.
Stwierdzone podczas auditu niezgodności są dokumentowane na Kartach niezgodności z odniesieniem w stosunku do kryteriów auditu (przyporządkowanie odpowiedniego wymogu normy lub innego dokumentu stanowiącego podstawę certyfikacji, oraz dowodu i udokumentowania jej istnienia). Oprócz tego odnośnikiem dla niezgodności może być również odpowiedni punkt z dokumentacji SZ organizacji.
Po audicie początkowej certyfikacji, w przypadku niezgodności dużych wdrożenie przez organizację działań korekcyjnych i korygujących, łącznie z pozytywną weryfikacją ich wdrożenia przez zespół auditowy, nie może przekraczać 90 dni kalendarzowych od daty wystawienia niezgodności.
W przypadku niezgodności małych oceniany jest plan działań korekcyjnych i korygujących, a w przypadku akceptacji planu weryfikacja wprowadzonych działań i ich skuteczność przeprowadzana jest na kolejnym audicie.
Na zakończenie auditu zespół auditowy analizuje wszystkie informacje i dowody z auditu zebrane podczas I i II etapu z auditu i dokonuje przeglądu ustaleń z auditu i uzgadnia wnioski.
Następnie spotyka się z Kierownictwem i, jeśli to właściwe, z osobami odpowiedzialnymi za auditowane funkcje lub procesy. W przypadku SZBHP w spotkaniu zamykającym oprócz przedstawiciela Organizacji powinni uczestniczyć członkowie kierownictwa prawnie odpowiedzialni za BHP, personel odpowiedzialny za monitorowanie stanu zdrowia pracowników oraz przedstawiciela/i pracowników odpowiedzialnego/ych za BHP

3.2.3 Audit dodatkowy

Audit dodatkowy przeprowadzany jest w przypadku wystąpienia podczas auditu początkowej certyfikacji niezgodności dużej (jednej lub większej ilości), w przypadku której (których) weryfikacja działań korekcyjnych i korygujących nie jest możliwa na podstawie przesłanych przez organizację dowodów wykonanych działań.
W zależności od ilości niezgodności i obszarów jakich dotyczą, audit może być pełny lub ograniczony. Decyzje podejmuje auditor wiodący.

3.2.4 Wnioski z auditu początkowej certyfikacji

Auditor wiodący, sporządza „Raport z auditu początkowej certyfikacji".
Raport przesyłany jest organizacji. Organizacja, przesyła do ISOCERT ewentualne uwagi do tego raportu. Brak takich uwag oznacza, że organizacja akceptuje jego treść.

4. UDZIELENIE CERTYFIKACJI

Decyzję o udzieleniu certyfikacji lub o odmowie udzielenia certyfikacji systemu zarządzania organizacji podejmuje ISOCERT, na podstawie:

- opinii i informacji publicznie dostępnych
- informacji zebranych podczas procesu początkowej certyfikacji,
- akceptacji planu działań korekcyjnych i korygujących (dla niezgodności małych), wykonanych działań korekcyjnych i korygujących i przyjęcia dowodów na wykonanie działań korekcyjnych i korygujących (dla niezgodności dużych)
- weryfikacji dokumentacji dotyczącej początkowej certyfikacji

Decyzja musi zostać podjęta w terminie do 90 dni od daty pozytywnej weryfikacji działań korekcyjnych i korygujących lub od daty zakończenia auditu u organizacji (w przypadku braku niezgodności podczas auditu).
ISOCERT powiadamia organizację pismem o decyzji odnośnie udzielenia certyfikacji.
W przypadku odmowy udzielenia certyfikacji w piśmie powiadamiającym zawarte jest uzasadnienie.
Certyfikacja jest ważna 3 lata od daty podjęcia decyzji o certyfikacji, chyba że wymagania akredytacyjne stanowią inaczej. W przypadku jeśli data ważności certyfikatu uwarunkowana jest wymaganiami akredytacyjnymi lub innymi wymaganiami stawianymi ISOCERT certyfikat posiada ważność zgodnie z tymi wymaganiami.

5. DZIAŁANIA W NADZORZE

W okresie ważności certyfikacji ISOCERT przeprowadza działania w nadzorze.
Działania w nadzorze obejmują:

- audity nadzoru - oceniające spełnianie przez system zarządzania organizacji wymagań normy systemu zarządzania,
- zapytania do organizacji w sprawie aspektów certyfikacji,
- przeglądanie strony internetowej i materiałów promocyjnych,
- monitorowanie informacji ogólnie dostępnych dotyczących nadzorowanej organizacji,
- żądania dostarczenia dokumentów i zapisów od organizacji.

Audit nadzoru obejmuje co najmniej:

- audity wewnętrzne i przeglądy zarządzania,
- weryfikację oraz skuteczność zaplanowanych działań podjętych w odniesieniu do niezgodności małych zidentyfikowanych podczas poprzedniego auditu oraz spostrzeżeń
- skuteczność działań podjętych w odniesieniu do niezgodności dużych zidentyfikowanych podczas poprzedniego auditu,
- postępowanie ze skargami,
- skuteczność systemu zarządzania pod względem osiągania celów organizacji
- postęp planowanej działalności mającej na celu ciągłe doskonalenie,
- ciągłą kontrole operacyjną,
- przegląd zmian,

Audity nadzoru przeprowadzane są co najmniej raz w roku. Data pierwszego auditu nadzoru po początkowej certyfikacji nie powinna być późniejsza niż 12 miesięcy od daty decyzji o udzieleniu certyfikacji. Decyzja o utrzymaniu certyfikacji podejmowana jest na podstawie przeglądu poprawności przebiegu certyfikacji (w tym działań w nadzorze), „Raportu z auditu" i pozytywnych wniosków auditora wiodącego.

6. PONOWNA CERTYFIKACJA

Ponowna certyfikacja nie wymaga składania przez organizację „Wniosku o certyfikację". Audit ponownej certyfikacji powinien być zaplanowany i przeprowadzony w sposób obejmujący potwierdzenie ciągłego spełnienia wszystkich wymagań programu certyfikacji lub innych dokumentów normatywnych. Audit należy przeprowadzić w terminie umożliwiającym zachowanie ciągłości ważności certyfikacji.
Jeżeli w organizacji nastąpiły znaczące zmiany w systemie zarządzania lub w wymaganiach prawnych dotyczących organizacji to przeprowadzany jest również I etap auditu.
Decyzję o przedłużeniu certyfikacji lub o odmowie przedłużenia certyfikacji systemu zarządzania organizacji podejmuje ISOCERT.
Przy podejmowaniu decyzji uwzględniane są skargi na organizację oraz wyniki funkcjonowania systemu w okresie certyfikacji.
Jeżeli nie zakończono auditu ponownej certyfikacji lub nie została zamknięta duża niezgodność przed upływem ważności certyfikacji, decyzja o przedłużeniu certyfikacji nie może zostać podjęta, a certyfikacja nie może zostać przedłużona.
Możliwe jest przeprowadzenie auditu na zasadach auditu ponownej certyfikacji w ciągu 6 miesięcy od daty wygaśnięcia certyfikacji. W takim przypadku certyfikat wystawiany jest po podjęciu decyzji certyfikacyjnej, a okres ważności certyfikacji odnosi się do pierwotnego okresu ważności.

7. ADITY SPECJALNE

7.1 Rozszerzenie zakresu certyfikacji

Rozszerzenie zakresu certyfikacji może nastąpić na wniosek organizacji.
W przypadku wystąpienia organizacji o rozszerzenie zakresu certyfikacji o obszary działania lub elementy systemu zarządzania, które nie były objęte certyfikacją, sposób i zakres oceny określa ISOCERT.

7.2 Audity z krótkim terminem powiadamiania

Audity z krótkim terminem powiadamiania przeprowadzane są w celu:

- zbadania skarg,
- w odpowiedzi na zmiany (wpływające na zdolność systemu zarządzania do spełniania wymagań odnośnej normy systemu zarządzania),
- dalszego postępowania w przypadku zawieszenia certyfikacji
- Zbadania czy nie doszło do pogorszenia działania systemu BHP i jego skuteczności w przypadku powzięcia informacji przez ISOCERT na przykład o wystąpieniu poważnego incydentu związanego z BHP (np. poważny wypadek lub poważnego naruszenia przepisów prawa) – dotyczy SZBHP

Decyzję o potrzebie przeprowadzenia podejmuje ISOCERT.

7.3 Zmiana lokalizacji

Zmiana lokalizacji może nastąpić na wniosek organizacji.
W przypadku wystąpienia organizacji o zmianę lokalizacji, sposób i zakres oceny określa ISOCERT.

8. ZAWIESZENIE CERTYFIKACJI

Zawieszenie certyfikacji może nastąpić gdy:

- system zarządzania organizacji stale lub w poważnym stopniu nie spełnia wymagań certyfikacyjnych, w tym wymagań dotyczących skuteczności systemu zarządzania,
- organizacja nie wykonała w uzgodnionym terminie działań korekcyjnych i korygujących wynikających z niezgodności ujawnionych podczas auditów,
- organizacja nie podjęła w uzgodnionym terminie działań dla wprowadzenia zmian w SZ wynikających ze zmiany wymagań zawartych w kryteriach auditu,
- organizacja nie pozwala na przeprowadzenie auditów w nadzorze lub auditów ponownej certyfikacji z wymaganą częstością,
- organizacja dobrowolnie poprosiła o zawieszenie,
- organizacja nie poinformowała ISOCERT o wprowadzeniu w SZ istotnych zmian,
- organizacja nie spełnia swoich zobowiązań finansowych wobec ISOCERT,
- istnieją inne powody określone wymaganiami lub też pisemnie uzgodnione pomiędzy organizacją a ISOCERT.

W okresie zawieszenia certyfikacji organizacja nie może powoływać się na certyfikację.
Okres zawieszenia certyfikacji określa ISOCERT i nie może być on dłuższy niż 6 miesięcy.
O terminie zawieszenia certyfikacji ISOCERT zawiadamia Organizację pisemnie.
Wznowienie ważności certyfikacji może nastąpić w przypadku przekazania przez organizację, której certyfikacja uległa zawieszeniu, informacji o spełnieniu warunków towarzyszących decyzji o zawieszeniu.

9. COFNIĘCIE CERTYFIKACJI

Cofnięcie certyfikacji następuje w przypadku nie rozwiązania przez organizację w ustalonym przez ISOCERT terminie przyczyn, które spowodowały zawieszenie certyfikacji. Po unieważnieniu certyfikacji organizacja nie może powoływać się na certyfikację.
Po podjęciu decyzji o cofnięciu certyfikacji ISOCERT rozwiązuje umowę i unieważnia certyfikację.
O terminie cofnięcia certyfikacji ISOCERT zawiadamia Organizację pisemnie.

10. OGRANICZENIE ZAKRESU CERTYFIKACJI

ISOCERT ogranicza zakres certyfikacji organizacji w celu wyłączenia tych części, które nie spełniają wymagań. Ma to miejsce w przypadku stałego lub poważnego stopnia nie spełnienia wymagań certyfikacyjnych w pewnym zakresie certyfikacji.
Ograniczenie zakresu certyfikacji może nastąpić:

- w wyniku auditu, w trakcie którego stwierdzono brak możliwości prowadzenia działalności w pełnym zakresie udzielonej certyfikacji,
- gdy organizacja nie wykonała w uzgodnionym terminie działań korekcyjnych i korygujących wynikających z niezgodności ujawnionych podczas auditów,
- na wniosek organizacji.

O terminie ograniczenia certyfikacji ISOCERT zawiadamia Organizację pisemnie.

11. PRZENIESIENIE PRAW

Przeniesienie praw z umowy następuje na wniosek organizacji w wyniku zmiany jej statusu prawnego.
W przypadku, gdy z dokumentów, które uległy zmianie wynika (np. dokumenty rejestracyjne firmy, regulaminy, procedury...), że zmianie uległ jedynie status prawny organizacji ISOCERT może podjąć decyzję o przeniesieniu praw z umowy bez przeprowadzenia auditu.
Jeżeli z przedstawionych dokumentów wynika, że oprócz zmiany statusu prawnego zaszły inne zmiany, decyzja o przeniesienie praw może być podjęta po przeprowadzeniu auditu.

12. INFORMOWANIE O ZMIANACH W ORGANIZACJI

Organizacja powinna bezzwłocznie informować ISOCERT o istotnych zmianach, które wpływają na zdolność systemu zarządzania do spełniania wymagań normy stanowiącej podstawą certyfikacji.
Zmiany te mogą dotyczyć np.:

- statusu prawnego, handlowego, organizacyjnego lub własnościowego,
- struktury organizacyjnej i zarządzania (kluczowego personelu zarządzającego, podejmującego decyzje lub technicznego),
- adresu do kontaktów i miejsc prowadzenia działalności,
- zakresu działania objętego certyfikowanym systemem zarządzania,
- głównych zmian w systemie zarządzania i procesach.

13. ZMIANY W WYMAGANIACH CERTYFIKACYJNYCH

ISOCERT pisemnie informuje organizacje o zmianach w wymaganiach certyfikacyjnych z odpowiednim wyprzedzeniem, umożliwiającym wprowadzenie zmian w organizacjach. Zmiany w wymaganiach certyfikacyjnych mogą dotyczyć np. zmiany w normach systemu zarządzania lub zmian w wymaganiach akredytacyjnych. Sprawdzenie wdrożonych zmian ISOCERT może przeprowadzać poprzez ankiety, rozmowy, wizje lokalne lub audity.

14. WYMAGANIA DLA ORGANIZACJI WIELOODZIAŁOWYCH

Organizacja wielooddziałowa powinna spełniać następujące warunki:

- w całej organizacji funkcjonuje pojedynczy system zarządzania
- Organizacja powinna zidentyfikować swoją funkcję centralną. Funkcja centralna jest częścią organizacji i nie powinna być podzlecana organizacji zewnętrznej.
- funkcja centralna powinna mieć uprawnienia organizacyjne do zdefiniowania, ustanowienia i utrzymywania pojedynczego systemu zarządzania.
- pojedynczy system zarządzania organizacji powinien podlegać scentralizowanemu przeglądowi zarządzania.
- wszystkie oddziały powinny podlegać programowi auditów wewnętrznych organizacji.
- Funkcja centralna powinna być odpowiedzialna za zapewnienie gromadzenia i analizowania danych ze wszystkich oddziałów i powinna być w stanie wykazać swoje uprawnienia i zdolność do inicjowania zmian organizacyjnych koniecznych między innymi, ale nie wyłącznie, w kontekście:
  - dokumentacji systemu i zmian w systemie;
  - przeglądów zarządzania;
  - skarg;
  - oceny działań korygujących;
  - planowania auditów wewnętrznych i oceny ich wyników;

- wymagań przepisów prawnych i regulacyjnych dotyczących obowiązującej(-ych) normy(norm).

15. ZASADY REALIZACJA PROCESÓW CERTYFIKACJI W SYTUACJI NADZWYCZAJNEJ

Jeżeli w wyniku sytuacji nadzwyczajnej wytyczne w danym sektorze wydane przez uprawnione urzędy lub przepisy wewnętrzne organizacji ograniczają możliwość przeprowadzenia auditu „na miejscu" lub w wyniku sytuacji nadzwyczajnej istnieje ryzyko dla zdrowia/bezpieczeństwa klienta lub auditora, ISOCERT rozpatruje alternatywne metody oceny organizacji w celu weryfikacji skuteczności systemu zarządzania certyfikowanej organizacji.

ISOCERT:

• ocenia ryzyko w zakresie możliwości przeprowadzenia auditu oraz kontunuowania certyfikacji

• analizuje możliwości zastosowania alternatywnych metod pozwalających w sposób wiarygodny potwierdzić zgodność systemu zarządzania z wymaganiami kryterialnymi, identyfikowane są alternatywne miejsca i sposoby pobierania próbek

• ustala tryb postępowania w zależności od posiadanych i pozyskanych informacji stanowiących podstawę do podjęcia decyzji w sprawie certyfikacji.

• określa zasady komunikacji z certyfikowaną organizacją (jeśli nie można nawiązać kontaktu, lub dokonać niezbędnych ustaleń z organizacją, uruchamia proces zawieszenia, cofnięcia lub wygaszenia certyfikacji),

• wyznacza tryb postępowania w zależności od rodzaju auditu

• opracowuje program auditu uwzględniający terminy i wszelkie informacje w zakresie nadzorowania organizacji,

Dopuszcza się :

- odroczenie auditu
- przeprowadzenie auditu zdalnego pełnego
- przeprowadzenie auditu zdalnego częściowego

16. REKLAMACJE, ODWOŁANIA, SKARGI

16.1 Reklamacje na działania ISOCERT

Organizacja może złożyć do ISOCERT reklamację związaną ze sposobem przeprowadzenia procesu certyfikacji systemu zarządzania, w tym zastrzeżenia na temat pracy auditorów.

Osoba rozpatrująca reklamację nie może być zaangażowana w przedmiot reklamacji.

ISOCERT rozpatruje reklamację w terminie do 30 dni od daty wpłynięcia reklamacji.

Decyzję o uznaniu lub nie uznaniu reklamacji podejmuje osoba z kierownictwa ISOCERT nie zaangażowana w jej przedmiot.

ISOCERT określa, jakie działania mają być podjęte w reakcji na złożoną reklamację i pisemnie informuje o nich osobę zgłaszającą reklamację.

16.2 Odwołania

Odwołania mogą dotyczyć: decyzji w procesie certyfikacji, nadzoru nad certyfikacją w tym zawieszeń oraz cofania certyfikacji. Złożenie odwołania przez organizację nie skutkuje żadnymi działaniami dyskryminującymi przeciwko składającemu odwołanie.

Odwołania rozpatruje zespół odwoławczy powoływany przez isocert. W skład zespołu wchodzą:

- kompetentny auditor ISOCERT (przy zachowaniu warunku, że auditor powołany do zespołu odwoławczego nie brał udziału w certyfikacji/weryfikacji/audycie w obszarze gospodarki odpadami organizacji składającej odwołanie)
- Komitet Nadzorujący bezstronność ISOCERT z wykluczeniem Dyrektora ds. certyfikacji (ze względu, że Dyrektor ds. certyfikacji jest jedną ze stron w Komitecie Nadzorującym)

Dyrektor ds. certyfikacji przekazuje odwołania do zespołu odwoławczego oraz wszystkie niezbędne dokumenty i procedury ISOCERT niezbędne do rozpatrzenia odwołania.

Odwołanie powinno być rozpatrzone w terminie 60 dni od dnia jego doręczenia do ISOCERT.

16.3 Skargi

Skargi mogą dotyczyć działalności ISOCERT (mogą dotyczyć działalności Organizacji obsługiwanych przez ISOCERT lub bezpośrednio działalność ISOCERT), w tym naruszenia poufności i bezpieczeństwa informacji.

Skargi na działalność ISOCERT mogą być składane do Polskiego Centrum Akredytacji.

W przypadku skargi na działalność organizacji obsługiwanej przez ISOCERT, ISOCERT pisemnie informuje organizację, której skarga dotyczy. ISOCERT wymaga od organizacji, na którą wpłynęła skarga, żeby w odpowiedzi ustaliła i – kiedy jest to właściwe – raportowała przyczynę skargi. ISOCERT analizuje problem i weryfikuje zebrane informacje. Jeżeli dla rozpatrzenia skargi wymagana jest wizyta w organizacji, to prowadzący sprawę po uzgodnieniu terminu, dokonuje wyjaśnień na miejscu (w organizacji) opracowując protokół z ustaleń.

Decyzję o uznaniu lub nie uznaniu skargi podejmuje osoba z kierownictwa ISOCERT, która nie była zaangażowana w przedmiot skargi.

W przypadku skargi na działalność ISOCERT, zgłaszający skargę informowany jest o decyzji i działaniach podjętych w reakcji na skargę w sposób pisemny.

W przypadku skargi na działalność organizacji obsługiwanej , ISOCERT pisemnie informuje zgłaszającego skargę i organizację, której skarga dotyczy, o swojej decyzji i działaniach podjętych w reakcji na skargę.

17. INFORMACJE PUBLICZNE

ISOCERT utrzymuje i udostępnia publicznie, bez żądania we wszystkich obszarach geograficznych, w których działa informacje dotyczące:

- procesów auditowania - INFORMATOR ISOCERT „Certyfikacja systemów zarządzania”, umieszczony na www.isocert.org.pl (zakładka „certyfikacja”)
- procesów udzielania, odmowy, utrzymywania, przedłużania, zawieszania, wznowienia lub cofnięcia certyfikacji, lub rozszerzenia albo ograniczenia zakresu certyfikacji -INFORMATOR ISOCERT „Certyfikacja systemów zarządzania”, umieszczony na www.isocert.org.pl (zakładka „certyfikacja”)
- rodzajów systemów zarządzania i programów certyfikacji, w których prowadzi działalność – informacje na www.isocert.org.pl (zakładka „certyfikacja”)
- stosowania nazwy ISOCERT oraz znaku certyfikacji – dokument „Specyfikacja oraz użytkowanie znaku certyfikacji” umieszczony na www.isocert.org.pl (zakładka „certyfikacja”)
- procesów postępowania z żądaniami o informację, skargami i odwołaniami -INFORMATOR ISOCERT „Certyfikacja systemów zarządzania”, umieszczony na www.isocert.org.pl (zakładka „certyfikacja”)
- polityki bezstronności – Deklaracja bezstronności, informacje na www.isocert.org.pl (zakładka „certyfikacja”)

Ponadto na żądanie ISOCERT udziela informacje o:

- obszarach geograficznych, w jakich prowadzi działalność,
- statusie danej certyfikacji,
- nazwie, związanym dokumencie normatywnym, zakresie i geograficznej lokalizacji określonego certyfikowanego klienta.

Pozostałe informacje o organizacjach, którym udzielono certyfikacji są poufne.

Dostęp do informacji o organizacji przez stronę trzecią jest możliwy jedynie za pisemną zgodą organizacji.

W każdym przypadku wymaganego przez prawo udostępnienia informacji stronie trzeciej, organizacja jest informowana o treści ujawnionej informacji (chyba, że prawo stanowi inaczej).

-Koniec-