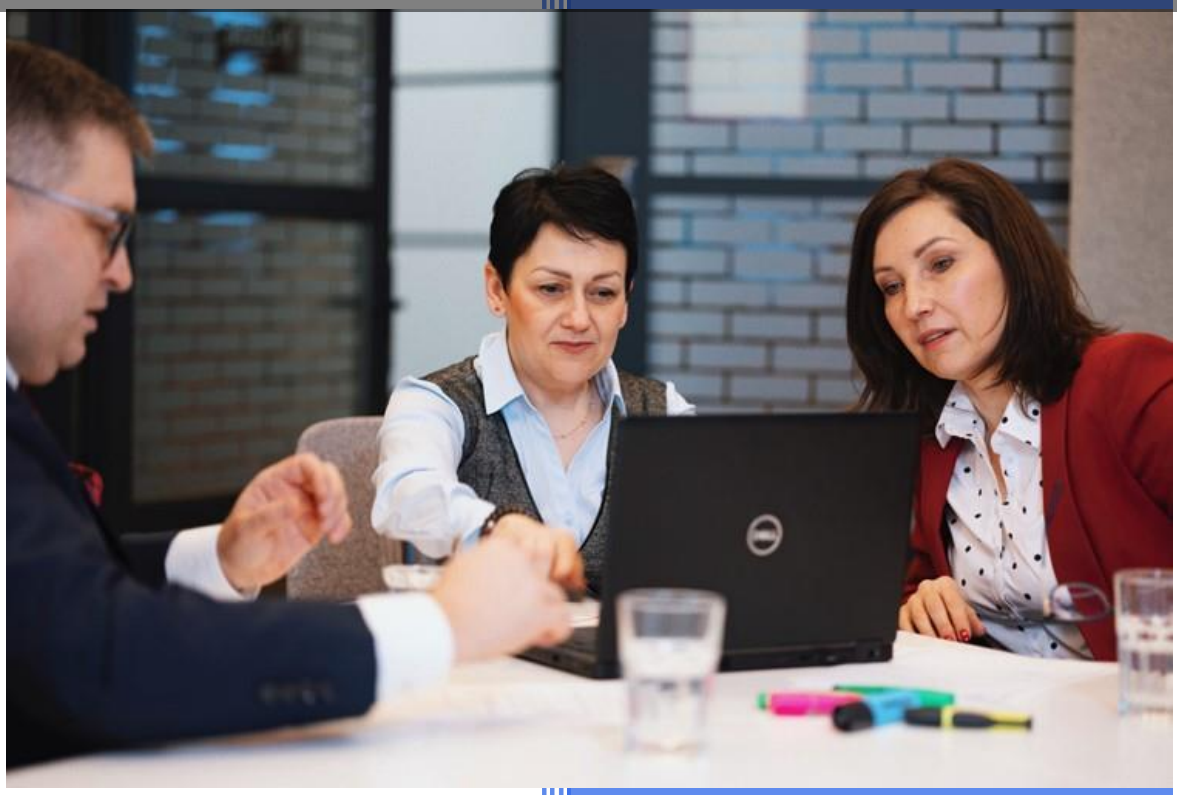
Kryteria kwalifikacyjne dla programu certyfikacji:

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001



Wydanie 4

z dnia 23.10.2023 r.

Niniejsze kryteria kwalifikacyjne stanowią wyciąg z wymagań z programu certyfikacji osób PCO-1 - Audytor Wiodący SZBI wg. normy PN-EN ISO/IEC 27001 i jest zbiorem wymagań, które muszą zostać spełnione przez osoby ubiegające się o zakwalifikowanie do egzaminu certyfikacji początkowej i ponownej na Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wg normy PN-EN ISO/IEC 27001:2023 – dalej zwanej PN-EN ISO/IEC 27001

KRYTERIA CERTYFIKACJI POCZĄTKOWEJ:

1. Kryterium wykształcenia

Kandydat powinien zapewnić, że posiada co najmniej wykształcenie średnie w rozumieniu Ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz.U. 2017 poz. 59 z późn. zm.)

Przykładowy dowód: dyplom, świadectwo ukończenia.

2. Kryterium doświadczenia zawodowego

Kandydat powinien zapewnić, że posiada udokumentowane doświadczenie zawodowe:

- co najmniej dwóch lat pracy w wymiarze pełnego etatu (w ostatnich 5 latach) w jednym z wymienionych obszarów:
  - bezpieczeństwo informacji,
  - ochrona danych osobowych,
  - technologii informacyjnych,

lub

- przeprowadził w ostatnich 5 latach audyty (pierwszej, drugiej lub trzeciej strony) Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami aktualnej normy PN-EN ISO/IEC 27001 w wymiarze minimum 20 audytorodni

Przykładowy dowód: Świadectwo pracy, umowa, referencje, lista audytów.

3. Kryterium przeszkolenia

Kandydat przed przystąpieniem do egzaminu musi ukończyć z sukcesem 40 godzinne szkolenie obejmujące swoim zakresem proces zarządzania audytem i audytowanie Systemu Zarządzania Bezpieczeństwem Informacji wg PN-EN ISO/IEC 27001. Szkolenie to musi obejmować zarówno część teoretyczną oraz ćwiczeniową w następujących zagadnieniach tematycznych:

- wymagania normy PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27006 i PN-EN ISO 19011;
- wzajemne relacje między normami PN-EN ISO/IEC 27001, PN-EN ISO/IEC 27002, PN-EN ISO/IEC 27006 i PN-EN ISO 19011;
- ustanowienie, rozwój i utrzymanie systemów informacyjnych;

- podstawowe pojęcia dotyczące urządzeń, systemów i sieci informacyjnych – analiza i ocena ryzyka;
- przygotowanie i planowanie działań audytowych;
- przeprowadzanie działań audytowych;
- metody i techniki audytowania;
- komunikowanie się podczas audytu;
- sprawozdawczość z audytu, działania wynikające z audytu, przygotowanie raportu z audytu;
- ustalenia audytowe, ocena wyników/ zgodności /niezgodności oraz zarządzanie niezgodnościami;

Przykładowy dowód: Zaświadczenie o ukończeniu szkolenia ze specyfikacją poruszanych zagadnień .

4. Przed egzaminem

Kandydat przed przystąpieniem do egzaminu wypełnia Wniosek o certyfikację osób, w którym listuje dowody potwierdzające spełnienie ww. kryteriów. Wniosek o certyfikację wysyła pocztą elektroniczną lub tradycyjną na adres biura CeCert wraz z dowodami (preferowana wersja elektroniczna) potwierdzającymi spełnienie kryteriów.

Warunkiem przystąpienia do egzaminu jest uregulowanie opłat zgodnych z przesłaną fakturą pro-forma.

W przypadku wyrażenia przez Kandydata zgody na realizację egzaminu w formie zdalnej, niezbędne jest posiadanie przez Kandydata dostępu do:

- pomieszczenia, w którym podczas trwania egzaminu panować będzie cisza i nie będą przebywać żadne osoby postronne.
- komputera, tabletu lub innego urządzenia z działającym mikrofonem i kamerą, o specyfikacji technicznej umożliwiającej korzystanie z najnowszej wersji oprogramowania Microsoft Teams, oprogramowania do edycji plików standardu Microsoft Word – format docx, a także przeglądarki internetowej np. Chrome, Firefox, Safari lub Edge – minimalne wymagania techniczne dostępne są na stronie internetowej producenta oprogramowania.
- internetu o przepustowości wystarczającej do prowadzenia połączenia audio i wideo za pośrednictwem Microsoft Teams.

5. Po egzaminie

Po zdanym egzaminie, zawierana jest z Kandydatem umowa o certyfikację osób, której następstwem jest wydanie ważnego na 3 lata certyfikatu.

Kandydat ma prawo do odwołania lub wniesienia skargi na podjętą przez CeCert decyzję w procesie certyfikacji, zgodnie z przyjętą przez jednostkę procedurą – dostępną na stronie internetowej cecert.pl

KRYTERIA PONOWNEJ CERTYFIKACJI:

W trzyletnim okresie ważności certyfikatu, osoba certyfikowana powinna zadbać o podnoszenie swoich kompetencji w zakresie, w którym otrzymała certyfikat.

Przy ponownej ocenie CeCert wymaga spełnienia następujących kryteriów:

1. Kryterium przeszkolenia:

Udział w min 1 szkoleniu / konferencji branżowej rocznie, związanej z szeroko pojętym Systemem Zarządzania Bezpieczeństwem Informacji zgodnym z aktualną normą PN-EN ISO/IEC 27001

Przykładowy dowód: zaświadczenie / certyfikat

2. Kryterium doświadczenia zawodowego:

Przeprowadzenie w 3 letnim okresie audytu/audytów (pierwszej, drugiej lub trzeciej strony) Systemu Zarządzania Bezpieczeństwem Informacji zgodnych z wymaganiami aktualnej normy PN-EN ISO/IEC 27001 o łącznym wymiarze czasu minimum 10 audytorodni.

Przykładowy dowód: lista zrealizowanych audytów

3. Przed egzaminem

Na 3 miesiące przed końcem ważności certyfikatu Kandydat wypełnia Wniosek o certyfikację osób, w którym listuje dowody potwierdzające spełnienie ww. kryteriów. Wniosek o certyfikację wysyła pocztą elektroniczną lub tradycyjną na adres biura CeCert wraz z dowodami (preferowana wersja elektroniczna) potwierdzającymi spełnienie kryteriów.

Warunkiem przystąpienia do egzaminu jest uregulowanie opłat zgodnych z przesłaną fakturą pro-forma.

W przypadku wyrażenia przez Kandydata zgodny na realizację egzaminu w formie zdalnej, niezbędne jest posiadanie przez Kandydata dostępu do:

- pomieszczenia, w którym podczas trwania egzaminu panować będzie cisza i nie będą przebywać żadne osoby postronne.
- komputera, tabletu lub innego urządzenia z działającym mikrofonem i kamerą, o specyfikacji technicznej umożliwiającej korzystanie z najnowszej wersji oprogramowania Microsoft Teams, oprogramowania do edycji plików standardu Microsoft Word – format docx, a także przeglądarki internetowej np. Chrome, Firefox, Safari lub Edge – minimalne wymagania techniczne dostępne są na stronie internetowej producenta oprogramowania.
- internetu o przepustowości wystarczającej do prowadzenia połączenia audio i wideo za pośrednictwem Microsoft Teams.

4. Po egzaminie:

Po zdanym egzaminie, zawierana jest z Kandydatem umowa o certyfikację osób, której następstwem jest wydanie ważnego na 3 lata certyfikatu.

Kandydat ma prawo do odwołania lub wniesienia skargi na podjętą przez CeCert decyzję w procesie certyfikacji, zgodnie z przyjętą przez jednostkę procedurą – dostępną na stronie internetowej cecert.pl

METODY OCENY PODCZAS CERTYFIKACJI POCZĄTKOWEJ I PONOWNEJ CERTYFIKACJI – WYMAGANIA EGZAMINACYJNE

Dla programu certyfikacji osób „Audytor Wiodący SZBI wg. normy PN-EN ISO/IEC 27001" przyjęto następujące metody oceny wiedzy i umiejętności Kandydatów dla procesów certyfikacji początkowej i audytorów do certyfikacji ponownej:

1. Test wiedzy – część teoretyczna – składająca się z 28 pytań jednokrotnego wyboru lub wielokrotnego wyboru, oraz 2 pytań otwartych. Za każde poprawnie rozwiązane pytanie Kandydat uzyskuje 1 punkt, tym samym łącznie można uzyskać 30 pkt. Czas trwania części teoretycznej to 45 minut.
2. Studia przypadku – część praktyczna – składające się z dwóch zagadnień problemowych do rozwiązania przez Kandydata w formie wypowiedzi ustnej. Na każde zagadnienie problemowe Kandydat ma 10 min, czyli w sumie 20 min. Po tym czasie Kandydat prezentuje swoje rozwiązanie egzaminatorowi. Maksymalny czas trwania egzaminu ustnego wynosi 20min na omówienie dwóch zagadnień. Łączny czas egzaminu części praktycznej wynosi 40min na jednego Kandydata. Za każde rozwiązane studium przypadku Kandydat uzyskuje do 5 punktów, czyli w sumie może uzyskać 10 pkt.

Wyniki oceny są przekazywane każdemu z uczestników indywidualnie wraz z punktacją otrzymaną w każdej sekcji. Wyniki oceny są poufne i nie będą przekazywane innym osobom niż Kandydat.

Warunkiem zaliczenia egzaminu jest uzyskanie minimalnego akceptowalnego poziomu dla potwierdzenia posiadanej wiedzy, umiejętności i kompetencji, który stanowi 51% każdej części egzaminu tj. testu wiedzy i studium przypadku.

W przypadku gdy Kandydat nie zaliczy części teoretycznej egzaminu tj. testu wiedzy, nie ma możliwości podejść do części praktycznej tj. studium przypadku. W takiej sytuacji Kandydat ma prawo do odpłatnego (z redukcją 50% ceny podstawowej) jednokrotnego przystąpienia do egzaminu poprawkowego, podczas której będzie miał możliwość ponownie podejść do części teoretycznej i po raz pierwszy części praktycznej.

W przypadku gdy Kandydat zaliczy część teoretyczną egzaminu tj. test wiedzy, a nie zaliczy części praktycznej tj. studium przypadku, wówczas Kandydat ma prawo do odpłatnego (z redukcją 50% ceny podstawowej) jednokrotnego przystąpienia do

egzaminu poprawkowego, podczas której będzie miał możliwość ponownie podejść do części praktycznej.

Kandydat ma prawo to jednej redukcji ceny podstawowej egzaminu, niezależnie czy dotyczy części teoretycznej czy praktycznej.

Datę egzaminu ustala się indywidualnie. Do egzaminu poprawkowego z redukcją 50% ceny podstawowej można przystąpić w ciągu roku od pierwszego podejścia.

KRYTERIA ZAWIESZANIA I COFANIA CERTYFIKACJI

Wydane przez Jednostkę certyfikaty są jej własnością i mogą zostać zawieszone w przypadku gdy:

- Klient wykorzystuje certyfikat w sposób mogący zdyskredytować jednostkę certyfikującą lub niezgodny z jego zakresem,
- ujawniono fakty, które nie były znane Jednostce w momencie podejmowania decyzji certyfikacyjnej,
- Klient dobrowolnie poprosił o zawieszenie certyfikatu.

W przypadku podjęcia przez Jednostkę decyzji o zawieszeniu certyfikatu, Klient zostaje poinformowany o przyczynach zawieszenia z jednoczesnym wyznaczeniem terminu usunięcia stwierdzonych uchybień oraz ze wskazaniem czasu na jaki zostanie zawieszona certyfikat/certyfikaty. Klient ma prawo do odwołania się od decyzji Jednostki, zgodnie z przyjętą procedurą.

Jednostka wznawia zawieszony certyfikat, jeśli przyczyny, które spowodowały zawieszenie, zostały rozwiązane. Nierozwiązanie, w czasie ustalonym przez Jednostkę, przyczyn, które spowodowały zawieszenie, skutkuje cofnięciem certyfikatu.

Zawieszenie nie może przekraczać okresu 6 miesięcy.

W okresie zawieszenia certyfikatu Klient ma obowiązek niezwłocznie zaprzestać używania certyfikatu, do czasu usunięcia przyczyny zawieszenia.

W przypadku cofnięcia certyfikatu rozwiązaniu ulega umowa o certyfikację osób, a certyfikat musi zostać odesłany do siedziby Jednostki (w przypadku wersji papierowej) albo trwale usunięty (w przypadku wersji elektronicznej).