P16 P01 Program certyfikacji Audytor Wiodący ISO/IEC 27001:2022

1. Tytuł

Certyfikacja na:
Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001:2022.

2. Zakres certyfikacji

Certyfikacja osób w celu potwierdzenia ich kompetencji jako:

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001:2022.

Uzyskanie Certyfikatu umożliwia przeprowadzenie audytów na zgodność z normą ISO/IEC 27001:2022 oraz pełnienie funkcji Audytora Wiodącego zarządzającego zespołem audytowym.

3. Przystąpienie do certyfikacji początkowej

Warunki wstępne i kryteria kwalifikacyjne

Przystępujący do certyfikacji musi spełniać następujące warunki wstępne:

Warunki prawne:	Warunki techniczne:
Ukończone 18 lat, Nie jest pozbawiona zdolności do czynności prawnych. Nie ma ograniczonej zdolności do czynności prawnych.	Posługuje się płynnie językiem w jakim jest przeprowadzany egzamin, Posiada komputer z kamerą, mikrofonem i możliwością podłączenia do Internetu, Posiada stabilne łącze internetowe, Jest w stanie posługiwać się przeglądarką internetową i komunikować przez internet za pomocą komunikatorów, Posiada pomieszczenie, w którym znajduje się tylko i wyłącznie osoba egzaminowana.

Wymagane kompetencje uprawniające do udziału w egzaminie i do wydania certyfikatu

Przystępujący do certyfikacji powinien spełnić kryteria dotyczące edukacji i doświadczenia zawodowego zgodnie z poniższymi tabelami.

Edukacja
Przystępujący do certyfikacji musi posiadać wykształcenie średnie lub wyższe oraz edukację z zakresu zarządzania bezpieczeństwem informacji jako jeden z poniższych warunków:

Warunek	Potwierdzenie
Wykształcenie Ukończona szkoła średnia lub studia wyższe obejmujące swym zakresem bezpieczeństwo informacji lub cyberbezpieczeństwo.	Świadectwo ukończenia szkoły lub dyplom ukończenia studiów.
Szkolenie Ukończone szkolenie z zakresu bezpieczeństwa informacji dedykowane dla osób audytujących systemy bezpieczeństwa informacji obejmujące zagadnienia prawne i normatywne z zakresu bezpieczeństwa informacji i obejmującą wymagania normy ISO/IEC 27001 i ISO 19011 - potwierdzane dokumentem zawierającym informacje pozwalające potwierdzić zakres szkolenia.	Dokument zawierający informacje pozwalające potwierdzić zakres szkolenia.
Uprawnienia Pozytywnie zdany egzamin eksternistyczny w zakresie wymagań normy ISO/IEC 27001:2022 oraz technik audytowania systemów zarządzania bezpieczeństwem informacji.	Dokument potwierdzający zdanie egzaminu, uwzględniający uprawnienia audytorskie.
Eksternistycznie Dla osób samodzielnie przygotowujących się istnieje możliwość przystąpienia „z wolnej stopy”.	W takiej sytuacji kandydat do egzaminu zobowiązany jest do złożenia oświadczenia o znajomości wymagań normy ISO/IEC 27001 i technik audytowania systemów bezpieczeństwa informacji oraz wymagań określonych w niniejszym programie certyfikacji, niezbędnych do przystąpienia do egzaminu.

Doświadczenie zawodowe (w obszarze bezpieczeństwa informacji jako spełnienie jednego z warunków)	
Personel służby mundurowej	• minimum 6 miesięcy służby potwierdzane dokumentem zawierającym datę rozpoczęcia służby oraz • wykonanie co najmniej jednego audytu, kontroli lub inspekcji lub dopuszczenie do przetwarzania informacji niejawnych
Osoby z wykształceniem średnim lub wyższym (Cywile)	• minimum 12 miesięcy pracy, w tym wykonanie co najmniej 3 audytów, kontroli lub inspekcji potwierdzenie dokumentem potwierdzającym datę rozpoczęcia pracy • oświadczeniem o przeprowadzeniu audytów

Przystąpienie do certyfikacji i organizacja certyfikacji odbywa się zgodnie z P16 000 Procedura certyfikacji personelu.

4. Przystąpienie do certyfikacji ponownej

Warunki wstępne i kryteria kwalifikacyjne

Przystępujący do certyfikacji ponownej musi posiadać Certyfikat Audytora Wiodącego Bezpieczeństwa Informacji ISO/IEC 27001:2022 - ważny co najmniej 1 miesiąc wystawiony przez akredytowaną jednostkę certyfikującą.

Wymagane kompetencje uprawniające do udziału w egzaminie i do wydania certyfikatu

Osoba ubiegająca się o ponowną certyfikację musi wykazać:

- przeprowadzenie w każdym roku co najmniej 1 audytu bezpieczeństwa informacji zgodnie z normą ISO/IEC 27001:2022 lub
- 4 audyty w okresie ważności certyfikatu.

Jeśli osoba certyfikowana nie jest w stanie wykazać wymogu przeprowadzenia audytów, może przystąpić w toku certyfikacji początkowej.

5. Kodeks postępowania

Osoba certyfikowana zgodnie z Programem Certyfikacji zobowiązuje się do wykazywania profesjonalnego postępowania podczas wykonywania swoich działań, co obejmuje:

- Działanie w sposób uczciwy, rzetelny, wiarygodny, prawdomówny i odpowiedzialny.
- Umiejętność delikatnego i wyważonego podejścia w kontaktach międzyludzkich.
- Skoncentrowane obserwowanie otoczenia, warunków fizycznych oraz zachowań ludzi.
- Świadomość bieżących okoliczności i umiejętność ich właściwej interpretacji.
- Umiejętność szybkiego i sprawnego dostosowania się do zmieniających się warunków.
- Niezachwiane dążenie do realizacji wyznaczonych celów mimo przeszkód.
- Umiejętność podejmowania trafnych decyzji we właściwym czasie, na podstawie logicznej analizy.
- Zdolność do samodzielnego działania przy jednoczesnym efektywnym współdziałaniu z innymi.
- Gotowość do doskonalenia wiedzy i umiejętności, rozwoju osobistego i nieustannego podnoszenia jakości działań.
- Szacunek dla różnorodności kulturowej oraz przestrzeganie norm i zwyczajów partnerów współpracy.
- Efektywne współdziałanie z innymi osobami, takimi jak eksperci, audytorzy czy członkowie zespołu.

Ponadto, osoba certyfikowana jest zobowiązana do deklarowania, że jest certyfikowana wyłącznie w zakresie, na jaki udzielono jej certyfikacji oraz niewykorzystywania certyfikacji w sposób mogący zdyskredytować CertCom lub składać mylące/nieuprawnione oświadczenia.

Osoba certyfikowana jest zobowiązana do niewykorzystywania certyfikatu w sposób mogący wprowadzić w błąd.

W przypadku zawieszenia lub cofnięcia certyfikacji, osoba certyfikowana zaprzestaje stosowania wszelkich deklaracji powołujących się na jednostkę certyfikującą lub certyfikację oraz zwraca wszelkie wydane certyfikaty w formie papierowej i usuwa trwale z nośników wszystkie wersje elektroniczne, a także zaprzestaje wykorzystywania certyfikatu, aby nie wprowadzać w błąd.

Musi również bezzwłocznie informować jednostkę certyfikującą o sprawach, które mogłyby mieć wpływ na zdolność do spełniania wymagań certyfikacyjnych.

Osoba przystępująca do certyfikacji składa oświadczenia woli co do swojego stanu prawnego, co wymaga od niej postawy etycznej w celu potwierdzenia stanu zgodnego z stanem faktycznym.

6. Opis przeprowadzania egzaminów

Egzamin odbywa się za pomocą łącza wideo za pomocą wyznaczonego podczas organizacji linku do spotkania. Gdy w trakcie zdawania egzaminu Egzaminator utraci wizję lub fonię od zdającego na czas dłuższy niż 15 sekund, egzamin jest przerywany i powtarzany od nowa.

Zdający nie może przerwać lub zawiesić rozpoczętego egzaminu.

Przed rozpoczęciem egzaminu kwalifikacyjnego egzaminator legitymuje uczestnika egzaminu (okazanie dowodu osobistego lub innego dokumentu ze zdjęciem potwierdzającego tożsamość do kamery internetowej).

Podczas egzaminu:

- Dopuszcza się korzystanie z normy ISO/IEC 27001:2022 (lub równoważnej PN-EN ISO/IEC 27001:2023) w formie elektronicznej lub papierowej
- Nie dopuszcza się korzystania z pomocy innych niż norma..
- Nie dopuszcza się kontaktowania z „osobami trzecimi" (jedna osoba certyfikowana w jednym pomieszczeniu).
- Telefony komórkowe należy wyłączyć i schować, nie dopuszcza się trzymania telefonów komórkowych na stolikach
- W przypadku niezastosowania się osoby zdającej egzamin do powyższych wymagań Egzaminator ma prawo przerwać egzamin z wynikiem negatywnym.

Egzamin składa się z dwóch części:

Część teoretyczna - test wielokrotnego wyboru:

Odbywa się za pomocą aplikacji internetowej pracującej w trybie online i składa się z testu wielokrotnego wyboru:

- zawierającego 20 pytań z 1 do 4 prawidłowych odpowiedzi
- pytania są losowo wybierane przez aplikację z bazy pytań
- pytania dotyczą wymagań normy ISO/IEC 27001:2022 wraz z załącznikiem A
- czas na rozwiązanie testu:20 minut od momentu kliknięcia w przycisk "start" i rozpoczęcia odliczania na stronie egzaminu
- istnieje możliwość przewinięcia pytania i przejścia do następnego lub powrotu do poprzednich pytań
- po zakończeniu egzaminu (kliknięciu w przycisk "zakończ lub finish" algorytm aplikacji dokonuje oceny poprawności udzielonych odpowiedzi i generuje wynik.
- wynik jest pozytywny w momencie uzyskania minimum 55%

Po zakończeniu części teoretycznej Osoba Certyfikowana zgłasza Egzaminatorowi gotowość do części praktycznej egzaminu.

Część praktyczna - "case study":

Osoba certyfikowana losuje 3 numery z puli zagadnień "case study"

- w trakcie egzaminu oceniane są umiejętności praktyczne oraz umiejętności rozwiązywania zadań
- jako odpowiedź na każde z 3 zagadnień osoba certyfikowana powinna przeanalizować podane sytuacje audytowe, a następnie:
  - określić czy istnieją obiektywne dowody zgodności lub niezgodności
  - odnieść się do właściwego punktu normy ISO/IEC 27001:2022
  - podać uzasadnienie swojej odpowiedzi
- czas odpowiedzi na każde z zagadnień: 5 minut
- odpowiedź zostanie oceniona w P16 F03 Protokół z egzaminu zgodnie z metodyką oceny
- wynik jest pozytywny w momencie uzyskania minimum 55%

Za pozytywny wynik całości egzaminu uważa się, gdy zostanie osiągnięty minimum 55% punktów z każdej części egzaminu. Ocena obu części egzaminu w P16 F03 Protokół z egzaminu, decyzja o certyfikacji i wystawienie Certyfikatu Audytora Wiodącego

bezpieczeństwa Informacji ISO/IEC 27001:2022 odbywa się zgodnie z P16 000 Procedura certyfikacji personelu.

Jeśli wynik jest niższy niż 55% z jednej części egzaminu, osoba certyfikowana może powtórzyć niezdaną część egzaminu, składając wniosek o certyfikację, zaznaczając opcję egzamin ponowny zgodnie z cennikiem.

7. Kryteria certyfikacji początkowej i ponownej certyfikacji

Certyfikacja początkowa

Osoba poddana certyfikacji początkowej po podpisaniu umowy i dokonaniu opłaty, przystępuje do egzaminu, który zdaje łącząc się w ustalonym terminie z Egzaminatorem za pomocą uzgodnionego łącza wideo.

Część teoretyczna - test wielokrotnego wyboru:

W celu przystąpienia do egzaminu zdający musi zalogować się do aplikacji EXAM po czym wybrać egzamin i przystąpić do niego. Zdawanie egzaminu odbywa się pod nadzorem Egzaminatora, który obserwuje zdającego za pomocą komunikatora (Google Meet lub Microsoft Teams). Jeżeli zdający podczas zdawania egzaminu zacznie zadawać pytania dotyczące egzaminu innej osobie lub będzie ściągał, Egzaminator zamyka egzamin i przyznaje zero punktów zdającemu.
Po odpowiedzeniu na wszystkie pytania przez zdającego lub upływie 20 minut, egzamin jest automatycznie zamykany.

Część praktyczna - “case study”:

Następnie Egzaminator zadaje 3 zagadnienia, wylosowane przez zdającego z puli pytań, po czym notuje odpowiedzi w protokole egzaminacyjnym P16 F03 Protokół z egzaminu. Pytania dotyczą praktycznego zrozumienia wymagań standardu, którego dotyczy egzamin.
Po zakończeniu egzaminu ustnego odpowiedzi kandydata poddawane są ocenie w P16 F03 Protokół z egzaminu i na tej podstawie jest wydawana decyzja o certyfikacji osoby.

Certyfikat jest wystawiany po pozytywnym zdaniu egzaminu oraz pozytywnej decyzji o certyfikacji osoby na 3 lata.

Certyfikacja ponowna

Osoba poddana certyfikacji ponownej musi przystąpić do certyfikacji ponownej minimum na 1 miesiąc przed upływem daty ważności certyfikatu. Po upłynięciu daty ważności certyfikatu osoba może ubiegać się zgodnie z tokiem postępowania certyfikacji początkowej.

Przystępując do certyfikacji ponownej.osoba certyfikowana musi wykazać się przeprowadzeniem w każdym roku co najmniej 1 audytu bezpieczeństwa informacji zgodnie z normą ISO/IEC 27001:2022.
i lub 4 w okresie ważnego certyfikatu. Jeśli osoba certyfikowana nie jest w stanie wykazać wymogu przeprowadzenia audytów, może przystąpić w toku certyfikacji początkowej.

Osoba certyfikowana powinna złożyć P16 F01 Certyfikacja osoby | WNIOSEK | PL zaznaczając opcję “Certyfikacja ponowna”.

Po pozytywnej decyzji certyfikacji osoby Certyfikat jest wydawany na okres kolejnych 3 lat zgodnie z cennikiem.

8. Metody oceny podczas certyfikacji początkowej i ponownej certyfikacji

Certyfikacja początkowa

Ocena formalna wstępna jest prowadzona na podstawie oceny spełnienia wymagań punktu 3 niniejszego Programu Certyfikacji zgodnie P16 000 Procedura certyfikacji personelu.

Ocena podczas egzaminu składa się z:

- oceny egzaminu teoretycznego - testu wielokrotnego wyboru oraz
- oceny egzaminu praktycznego "case study"

Wynik uznaje się za pozytywny, gdy z każdej części zostanie osiągnięty próg minimum 55%. Jeśli wynik jest niższy niż 55% z jednej części egzaminu, osoba certyfikowana może ją powtórzyć niezdaną część egzaminu, składając wniosek o certyfikację, zaznaczając opcję egzamin ponowny zgodnie z cennikiem.

Egzamin teoretyczny - test wielokrotnego wyboru:

- 20 pytań losowanych automatycznie z bazy pytań
- każde pytanie zawiera cztery odpowiedzi w pytaniu, z czego poprawna jest od 1 do 4 odpowiedzi
- wymagane jest zaznaczenie tylko poprawnych odpowiedzi w pytaniu
- czas na rozwiązanie 20 minut licząc od rozpoczęcia przyciskiem start
- minimum 55% poprawnych odpowiedzi - wynik pozytywny
- punktacja:
  - za każdą prawidłową odpowiedź (odpowiednia liczba zakreśleń na właściwym miejscu) otrzymuje się 1 punkt
  - za brak odpowiedzi lub odpowiedź niepełną - zero punktów
  - nie przyznaje się punktów ułamkowych
  - maksymalna ilość punktów: 20
  - minimalna ilość punktów do zaliczenia testu: 11 co stanowi próg zdawalności 55%
- wynik egzaminu jest wyliczany przez aplikację Exam i podawany po zakończeniu testu przyciskiem "zakończ/finish" lub automatycznym zakończeniu po upływie 20 minut

Egzamin praktyczny - ustny "case study" - sprawdzenie wiedzy merytorycznej oraz umiejętności oceny symulowanych sytuacji audytowych

- 3 pytania zawierające opis sytuacji audytowych
- w odpowiedzi na każde z 3 zagadnień osoba certyfikowana powinna:
  - przeanalizować podane sytuacje audytowe
  - określić czy istnieją obiektywne dowody zgodności lub niezgodności
  - odnieść się do właściwego punktu normy ISO/IEC 27001:2022
  - podać uzasadnienie swojej odpowiedzi
- czas na odpowiedź: 5 minut na pytanie, łącznie 15 minut
- minimum 55% poprawnych odpowiedzi - wynik pozytywny
- punktacja:

- za każdą poprawną odpowiedź na pytanie zdający otrzymuje maksymalnie 3 punkty wg kryteriów:
  - klasyfikacja dowodów jako zgodności lub niezgodności - 1 pkt
  - określenie wymagań normy - 1 pkt,
  - uzasadnienie odpowiedzi - 1 pkt
- maksymalna ilość punktów: 9
- minimalna ilość punktów do zaliczenia testu: 5, co stanowi próg 55%

Z egzaminu na podstawie zapisów w P16 F03 Protokół z egzaminu jest podejmowana decyzja o certyfikacji osoby. W przypadku pozytywnej decyzji certyfikacyjnej jest wystawiany Certyfikat.

Certyfikacja ponowna

Ocena jest prowadzona na podstawie oceny spełnienia wymagań punktu 4 niniejszego Programu Certyfikacji zgodnie P16 000 Procedura certyfikacji personelu.

Kryterium oceny ponownej certyfikacji jest spełnienie warunków:

- posiadanie ważnego co najmniej 1 m-c Certyfikatu Audytora Wiodącego ISO/IEC 27001:2022 wystawionego przez akredytowaną jednostkę certyfikującą
- Spełnienie wymogu przeprowadzenia audytów bezpieczeństwa zgodnie z wymaganiami normy ISO/IEC 27001:2022 w ilości: audyty po jednym w każdym roku lub 4 audyty w okresie ważności obecnie posiadanego Certyfikatu

Po ocenie następuje podjęcie decyzji o certyfikacji a w przypadku pozytywnej decyzji, wystawienie Certyfikatu.

9. Metody i kryteria nadzoru przebiegu egzaminów

Do nadzorowania przebiegu egzaminu stosowana jest obserwacja w formie połączenia audio-wideo W tym celu używana jest jedna z aplikacji (co jest ustalane wcześniej ze zdającym):

- Google Meet
- Microsoft Teams

za pomocą, której zdający łączą się z Egzaminatorem w ustalonym terminie, udostępniając mu obraz oraz dźwięk, dzięki czemu Egzaminator:

- potwierdza tożsamość osoby zdającej na podstawie okazanego do kamery dokumentu tożsamości ze zdjęciem i numerem dokumentu
- widzi, czy zdający korzysta z niedozwolonej pomocy przy zdawaniu egzaminu

Podczas egzaminu:

- Dopuszcza się korzystanie z normy ISO/IEC 27001:2022 (lub równoważnej PN-EN ISO/IEC 27001:2023) w formie elektronicznej lub papierowej
- Nie dopuszcza się korzystania z niedozwolonych pomocy.
- Nie dopuszcza się kontaktowania z „osobami trzecimi” (jedna osoba certyfikowana w jednym pomieszczeniu).
- Telefony komórkowe należy wyłączyć i schować, nie dopuszcza się trzymania telefonów komórkowych na stolikach

W przypadku braku potwierdzenia tożsamości osoby zdającej egzamin Egzaminator ma prawo przerwać egzamin z wynikiem negatywnym.

W celu zapobiegania używania niedozwolonych pomocy, zdający ma cały czas włączoną kamerę i mikrofon, skierowane na siebie i pomieszczenie, w którym się znajduje.
W przypadku niezastosowania się osoby zdającej egzamin do powyższych wymagań Egzaminator ma prawo przerwać egzamin z wynikiem negatywnym.

Gdy w trakcie zdawania egzaminu Egzaminator utraci wizję lub fonię od zdającego na czas dłuższy niż 15 sekund, egzamin jest przerywany i powtarzany od nowa.

Dopuszcza się możliwość udziału niezależnego Obserwatora oraz możliwość nagrania egzaminu po uzyskaniu zgody wszystkich osób uczestniczących.

10. Kryteria zawieszania i cofania certyfikacji

Zawieszenie certyfikacji może nastąpić:

- na skutek niespełnienia warunków, gdy osoba certyfikowana:
  - poda nieprawdziwe informacje i oświadczenia podczas przystąpienia do certyfikacji, które nie były znane CertCom
  - nie wniesie opłaty za certyfikację początkową lub ponowną
  - wykorzystuje certyfikat niezgodnie z jego przeznaczeniem
  - wykorzystuje certyfikację w sposób mogący zdyskredytować CertCom i składa oświadczenia związane z certyfikacją, które CertCom może uznać za mylące lub nieuprawnione
  - wykorzystuje certyfikat w sposób mogący wprowadzić w błąd
  - używa certyfikat wyłącznie w zakresie innym niż na jaki udzielono certyfikacji
  - wykorzystuje certyfikat w sposób niedozwolony lub niezgodnie z przeznaczeniem
  - wykorzystuje certyfikat w sposób mogący wprowadzić w błąd w zakresie zasad prezentowania certyfikatów i znaków graficznych CerCom
  - nie prowadzi czynnej działalności w certyfikowanym obszarze
- na skutek odnotowania skarg wnoszonych skarg wobec certyfikowanej osoby w zakresie udzielonej certyfikacji
- w przypadku wycofania standardu międzynarodowego opublikowanym przez ISO.ORG lub standardu krajowego opublikowanego przez PKN.PL lub przepisu krajowego, którego dotyczy certyfikat.

Jeśli na podstawie powyższych przesłanek CertCom podejmie decyzję o cofnięciu certyfikatu informuje osobę certyfikowaną pisemnie o przyczynach oraz o wynikających z tego skutkach, a równocześnie daje możliwość zajęcia stanowiska w tej sprawie w wyznaczonym terminie. Jeżeli przyczyn nie można usunąć, CertCom cofa certyfikat i informuje pisemnie w wiadomości e-mail lub drogą pocztową wraz z podaniem uzasadnienia wycofania. W piśmie osoba certyfikowana jest wzywana do zwrócenia certyfikatu w formie papierowej do CertCom i usunięcia wszystkich kopii elektronicznych certyfikatu. Pismo zawiera również pouczenie o możliwości wniesienia odwołania od decyzji. Zawieszenie lub wycofanie certyfikatu zapisywane jest w P16 R01 000 CRM DCP CertCom.
Jeżeli osoba, której cofnięto certyfikat nie zastosuje się do wezwania, to CertCom nalicza opłaty administracyjne zgodnie z cennikiem certyfikacji.

Wygaśnięcie certyfikatu

Certyfikat jest wydawany na 3 lata licząc od daty decyzji o certyfikacji.

Certyfikat wygasa w przypadku upływu terminu ważności certyfikatu lub jego wycofania.

11. Kryteria zmiany zakresu lub poziomu certyfikacji

Zmiana zakresu lub poziomu certyfikacji nie ma zastosowania w niniejszym Programie Certyfikacji, ponieważ w przypadku nowego wydania normy powstanie nowy Program Certyfikacji.