Możliwość dofinansowania

Audytor wewnętrzny/ Pełnomocnik ISO/IEC 27001 (S_52147)

Numer usługi 2026/03/07/7629/3388050

2 324,70 PLN brutto
1 890,00 PLN netto
136,75 PLN brutto/h
111,18 PLN netto/h
261,33 PLN cena rynkowa

ASSECO DATA SYSTEMS SPÓŁKA AKCYJNA

4,4 / 5

156 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
17:00 h
15.06.2026 do 16.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	• Audytorzy wewnętrzni Systemu Zarządzania Bezpieczeństwem Informacji, w szczególności opartego o normę ISO/IEC 27001 • Pełnomocnicy ds. cyberbezpieczeństwa odpowiedzialni za utrzymanie i doskonalenie SZBI • Kadra kierownicza nadzorująca bezpieczeństwo informacji oraz zarządzanie ryzykiem cyberbezpieczeństwa • Audytorzy innych systemów zarządzania chcących rozszerzyć kompetencje o obszar bezpieczeństwa informacji • Osoby zaangażowane w projekty wdrożenia lub doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	08-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	17
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie uczestników do rozumienia wymagań normy ISO/IEC 27001 oraz do planowania i prowadzenia audytów wewnętrznych Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Uczestnicy poznają zasady funkcjonowania SZBI, zarządzania ryzykiem cyberbezpieczeństwa oraz rolę audytu w ocenie skuteczności systemu i doskonaleniu bezpieczeństwa informacji w organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik charakteryzuje zasady funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji zgodnego z normą ISO/IEC 27001.	Omawia podstawowe elementy SZBI Wyjaśnia rolę polityki bezpieczeństwa informacji Wskazuje kluczowe obszary SZBI	Test teoretyczny
WIEDZA: Uczestnik wyjaśnia wymagania normy ISO/IEC 27001 oraz znaczenie mechanizmów zabezpieczeń w ochronie informacji.	Opisuje strukturę normy ISO/IEC 27001 Wskazuje przykłady zabezpieczeń organizacyjnych i technicznych Wyjaśnia rolę zarządzania ryzykiem w SZBI	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik planuje audyt wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji.	Przygotowuje program audytu Opracowuje plan audytu dla wybranego obszaru SZBI Określa zakres i cele audytu	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik przygotowuje wnioski i raport z audytu wewnętrznego.	Formułuje wnioski audytowe na podstawie dowodów Proponuje działania korygujące lub usprawniające Przygotowuje raport z audytu zgodnie z przyjętą strukturą	Test teoretyczny
KOMPETECJE SPOŁECZNE: Uczestnik stosuje zasady bezstronności i obiektywizmu w pracy audytora wewnętrznego.	Formułuje oceny audytowe w oparciu o dowody Unika subiektywnych ocen podczas analizy sytuacji audytowej Respektuje zasadę niezależności audytu	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KOMPETECJE SPOŁECZNE: Uczestnik dostrzega znaczenie audytu jako narzędzia doskonalenia systemu bezpieczeństwa informacji w organizacji.	Wskazuje korzyści wynikające z audytów wewnętrznych Identyfikuje rolę audytu w procesie ciągłego doskonalenia SZBI Proponuje działania wspierające poprawę bezpieczeństwa informacji w organizacji	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

- Wprowadzenie do szkolenia
- Norma ISO/IEC 27001:2023 – wymagania Systemu Zarządzania Bezpieczeństwem Informacji
- Norma ISO/IEC 27001:2023 – wymagania Systemu Zabezpieczeń
- Cele i ramy działania audytu wewnętrznego
- Program audytów (warsztat)
- Planowanie audytu Systemu Zarządzania (warsztat)
- Planowanie audytu skuteczności zabezpieczeń (warsztat)
- Przebieg audytu Systemu Zarządzania (ćwiczenia w zespołach)
- Przebieg audytu skuteczności zabezpieczeń – 2 obszary zabezpieczeń (ćwiczenia w zespołach)
- Raport z audytu i dalsze postępowanie (warsztat)
- Podsumowanie szkolenia

Szkolenie trwa **3 dni**. Łącznie realizowanych jest **26 godzin dydaktycznych** (45 min) wraz z przerwami.

Każdego dnia jest przewidziana 1 dłuższa przerwa na lunch (30 minut) oraz 2 krótsze przerwy kawowe (po 15 minut każda). Przerwy zostały wliczone w harmonogramie usługi.

Ramowy program szkolenia

- Wprowadzenie do szkolenia
- Norma ISO/IEC 27001:2023 – wymagania Systemu Zarządzania Bezpieczeństwem Informacji
- Norma ISO/IEC 27001:2023 – wymagania Systemu Zabezpieczeń
- Cele i ramy działania audytu wewnętrznego
- Program audytów (warsztat)
- Planowanie audytu Systemu Zarządzania (warsztat)
- Planowanie audytu skuteczności zabezpieczeń (warsztat)
- Przebieg audytu Systemu Zarządzania (ćwiczenia w zespołach)
- Przebieg audytu skuteczności zabezpieczeń – 2 obszary zabezpieczeń (ćwiczenia w zespołach)
- Raport z audytu i dalsze postępowanie (warsztat)
- Podsumowanie szkolenia

Wszystkie punkty agendy obejmują zarówno zagadnienia teoretyczne, jak i praktyczne. **Łącznie w szkoleniu przewidziano 3 godziny dydaktyczne na część praktyczną. Część teoretyczna obejmuje 23 godziny dydaktyczne.**

Szkolenie rozpoczyna się i kończy odpowiednio pre- i post-testem walidującym efekty kształcenia. Jest to test teoretyczny z wynikiem generowanym automatycznie.Szkolenie trwa **2 dni**. Łącznie realizowanych jest **17 godzin dydaktycznych** (45 min) wraz z przerwami.

Każdego dnia jest przewidziana 1 dłuższa przerwa na lunch (30 minut) oraz 2 krótsze przerwy kawowe (po 15 minut każda). Przerwy zostały wliczone w harmonogramie usługi.

Ramowy program szkolenia

- Wprowadzenie do szkolenia
- Norma ISO/IEC 27001:2023 – wymagania Systemu Zarządzania Bezpieczeństwem Informacji
- Norma ISO/IEC 27001:2023 – wymagania Systemu Zabezpieczeń
- Cele i ramy działania audytu wewnętrznego
- Program audytów (warsztat)
- Planowanie audytu Systemu Zarządzania (warsztat)
- Planowanie audytu skuteczności zabezpieczeń (warsztat)
- Przebieg audytu Systemu Zarządzania (ćwiczenia w zespołach)
- Przebieg audytu skuteczności zabezpieczeń – 2 obszary zabezpieczeń (ćwiczenia w zespołach)
- Raport z audytu i dalsze postępowanie (warsztat)
- Podsumowanie szkolenia

Wszystkie punkty agendy obejmują zarówno zagadnienia teoretyczne, jak i praktyczne. **Łącznie w szkoleniu przewidziano 3 godziny dydaktyczne na część praktyczną. Część teoretyczna obejmuje 14 godziny dydaktyczne.**

Szkolenie rozpoczyna się i kończy odpowiednio pre- i post-testem walidującym efekty kształcenia. Jest to test teoretyczny z wynikiem generowanym automatycznie.

Harmonogram

Liczba pozycji harmonogramu: 18

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 18 Pre-test	-	15-06-2026	09:00	09:15	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 18 Norma ISO/IEC 27001:2023 – wymagania Systemu Zarządzania Bezpieczeństwem Informacji	-	15-06-2026	09:15	10:15	01:00
3 z 18 Przerwa kawowa	-	15-06-2026	10:15	10:30	00:15
4 z 18 Norma ISO/IEC 27001:2023 – wymagania Systemu Zabezpieczeń	-	15-06-2026	10:30	11:30	01:00
5 z 18 Cele i ramy działania audytu wewnętrznego	-	15-06-2026	11:30	12:30	01:00
6 z 18 Przerwa na lunch	-	15-06-2026	12:30	13:00	00:30
7 z 18 Program audytów + warsztat	-	15-06-2026	13:00	14:00	01:00
8 z 18 Przerwa kawowa	-	15-06-2026	14:00	14:15	00:15
9 z 18 Planowanie audytu Systemu Zarządzania + warsztat	-	15-06-2026	14:15	15:30	01:15
10 z 18 Planowanie audytu skuteczności zabezpieczeń + warsztat	-	16-06-2026	09:00	10:15	01:15
11 z 18 Przerwa kawowa	-	16-06-2026	10:15	10:30	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 18 Przebieg audytu Systemu Zarządzania + ćwiczenia w zespołach	-	16-06-2026	10:30	11:30	01:00
13 z 18 Przebieg audytu skuteczności zabezpieczeń: 2 obszary zabezpieczeń + ćwiczenia w zespołach	-	16-06-2026	11:30	12:30	01:00
14 z 18 Przerwa na lunch	-	16-06-2026	12:30	13:00	00:30
15 z 18 Raport z audytu i dalsze postępowanie + warsztat	-	16-06-2026	13:00	14:00	01:00
16 z 18 Przerwa kawowa	-	16-06-2026	14:00	14:15	00:15
17 z 18 Podsumowanie szkolenia	-	16-06-2026	14:15	15:15	01:00
18 z 18 Post-test (walidacja efektów kształcenia)	-	16-06-2026	15:15	15:30	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 324,70 PLN
Koszt przypadający na 1 uczestnika netto	1 890,00 PLN
Koszt osobogodziny brutto	136,75 PLN

Koszt osobogodziny netto	111,18 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W cenie uczestnik otrzymuje

- Udział w 3-dniowym szkoleniu #cyberSecurity Foundation prowadzonym zdalnie w czasie na żywo przez trenera eksperta ds. cyberbezpieczeństwa
- Komplet materiałów szkoleniowych #cyberSecurity Foundation w wersji elektronicznej
- Zaświadczenie Asseco Academy o ukończeniu szkolenia.

Język

- Język szkolenia: polski
- Język materiałów: polski

Metody interaktywne i aktywizujące prowadzenia usługi m.in.: dyskusje, quizy, odpowiadanie na pytania testowe, praca z tablicą interaktywną, ćwiczenia do samodzielnego wykonania lub w grupach 3-4 osobowych.

Link do szkolenia: https://academy.asseco.pl/szkolenie/audytor-wewnetrzny-pelnomocnik-iso-iec-270012023/

Warunki uczestnictwa

Warunki organizacyjne: Szkolenie realizowane jest w formie zdalnej w czasie rzeczywistym. Uczestnik powinien posiadać dostęp do komputera z kamerą i mikrofonem, spełniające minimalne wymagania opisane w sekcji: Warunki techniczne. Uczestnik bierze udział w szkoleniu wraz z całą grupą szkoleniową, zarówno w części teoretycznej, jak i praktycznej, zgodnie z programem.

Wymagana frekwencja: min. 80%. Podstawą weryfikacji są listy obecności tworzona na podstawie rzeczywistego czasu zalogowania w sesji szkoleniowej. Brak wymaganej frekwencji skutkuje nieuznaniem usługi za zrealizowaną i brakiem możliwości rozliczenia dofinansowania w systemie BUR.

Informacje dodatkowe

Dla usług z dofinansowaniem powyżej 70% istnieje możliwość wystawienia faktury ZW VAT. Prosimy o kontakt z Biurem Asseco Academy academy@assecods.pl Natomiast w przypadku dofinansowania usługi poniżej 70% ze środków publicznych, usługa nie jest zwolniona z podatku VAT. Należy wówczas doliczyć do usługi szkoleniowej należny VAT w wysokości 23%. Podstawa prawna zwolnienia z VAT: art. 43 ust. 1 pkt. 29 lit. c ustawy o podatku od towarów i usług z dnia 11 marca 2004r. (Dz.U. Nr 54, poz. 535 ze zm.) oraz zgodnie z § 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U. z 2015, poz. 736 ze zm.).

Warunki techniczne

Szkolenie prowadzone jest w formie zdalnej na żywo za pośrednictwem aplikacji Webex Meeting. Aby wziąć udział, konieczne jest posiadanie urządzenia takiego jak komputer stacjonarny lub laptop wyposażonego w stabilne połączenie internetowe oraz mikrofon i kamerę. Przed rozpoczęciem szkolenia uczestnicy będą mieli możliwość przetestowania swojego sprzętu podczas sesji próbnej, aby upewnić się, że połączenie internetowe, mikrofon i kamera/słuchawki działają poprawnie.

Minimalne wymagania sprzętowo-systemowe

- Komputer PC z systemem Windows 7 lub nowszym, Max OX 10.13 lub nowszym. Istnieje możliwość korzystania z innych systemów, w tym Linux. Szczegółowe informacje można uzyskać pod adresem: https://help.webex.com/en-us/nki3xrq/Webex-Meetings-Suite-SystemRequirements.
- Przeglądarka internetowa (zalecamy korzystanie z Chrome lub Firefox).
- Karta LAN: min. 100 MBPS lub stabilne połączenie WiFi (zalecamy połączenie do sieci „kablem"). Nie dopuszcza się udziału w szkoleniu za pośrednictwem łączy GSM/LTE. Zalecane pasmo, to przynajmniej 2 MB/s (download i upload). W przypadku spadku przepustowości łącza poniżej 1,2 MB/s należy liczyć się z istotnym obniżeniem jakości połączenia.
- Mikrofon i głośniki (zalecamy korzystanie z zestawu typu headset).
- Kamera internetowa.

Przed szkoleniem każdy uczestnik otrzyma na podany adres email link do platformy, gdzie odbędzie się szkolenie. Uczestnictwo w szkoleniu umożliwia aktywne uczestnictwo w zajęciach, w tym komunikację z trenerem oraz pozostałymi uczestnikami. Umożliwia to wymianę doświadczeń oraz aktywny kontakt zarówno z grupą, jak i prowadzącym. Dodatkowo, uczestnicy mają dostęp do funkcji czatu online, co jeszcze bardziej ułatwia interakcję.

Kontakt

Alicja Kozłowska

E-mail bur-szkolenia@assecods.pl
Telefon (+48) 801 303 030