



Podstawy zarządzania bezpieczeństwem informacji. Wymagania normy ISO/IEC 27001:2022. Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) - szkolenie

1 291,50 PLN brutto
1 050,00 PLN netto
184,50 PLN brutto/h
150,00 PLN netto/h

CENTRUM
ZARZĄDZANIA
JAKOŚCIĄ INFOX
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

Numer usługi 2024/06/12/120241/2180727



📍 Bochnia / stacjonarna
🏠 Usługa szkoleniowa
🕒 7 h
📅 12.08.2024 do 12.08.2024

Informacje podstawowe

Kategoria

Biznes / Zarządzanie przedsiębiorstwem

Sposób dofinansowania

wsparcie dla osób indywidualnych
wsparcie dla pracodawców i ich pracowników

Grupa docelowa usługi

Usługa rozwojowa „**Podstawy zarządzania bezpieczeństwem informacji. Wymagania normy ISO/IEC 27001:2022. Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) - szkolenie**” adresowana jest do:

- przedstawicieli kierownictwa odpowiedzialnych za:
 - zgodność SZBI z wymaganiami ISO/IEC 27001:2022,
 - przedstawianie sprawozdań dla najwyższego kierownictwa w zakresie funkcjonowania SZBI,
 - utrzymanie integralności SZBI podczas planowania i wprowadzania zmian,
- audytorów wewnętrznych przewidzianych do realizacji audytów w ramach SZBI,
- menedżerów IT, menedżerów systemów informatycznych, Inspektorów Ochrony Danych,
- wszystkich organizacji, które przechowują, przetwarzają lub udostępniają poufne informacje - szczególnie ważne jest to dla organizacji z sektorów finansowego, medycznego, IT oraz dla tych, które obsługują duże ilości danych osobowych,
- wszystkich osób zainteresowanych tematyką SZBI i uzyskaniem nowych, przyszłościowych kompetencji zawodowych,

Minimalna liczba uczestników

6

Maksymalna liczba uczestników

20

Data zakończenia rekrutacji	05-08-2024
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	7
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

Usługa rozwojowa przygotowuje do samodzielnego określania kontekstu organizacji, zakresu SZBI, ryzyk i szans dla SZBI oraz działań w odpowiedzi na te ryzyka i szanse, szacowania ryzyka i postępowania z ryzykiem w bezpieczeństwie informacji oraz stosowania zabezpieczeń i zabezpieczeń zawartych w załączniku A do ISO/IEC 27001:2022, monitorowania SZBI oraz jego doskonalenia a także do stosowania wymagań ISO/IEC 27001:2022.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Omawia podstawy zarządzania bezpieczeństwem informacji w organizacji.	Omawia zasady stosowania i strukturę norm międzynarodowych serii ISO/IEC 27000.	Test teoretyczny
	Omawia zasady certyfikacji systemów zarządzania bezpieczeństwem informacji (SZBI) z zastosowaniem wymagań ISO/IEC 27001:2022.	Test teoretyczny
	Omawia zasady korzystania z wytycznych zawartych w normach ISO/IEC 27000.	Test teoretyczny
	Omawia podstawową terminologię stosowaną w normach ISO/IEC 27000.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przystosowuje system zarządzania bezpieczeństwem informacji (SZBI) do organizacji.	Określa kontekst organizacji.	Test teoretyczny
	Przedstawia potrzeby i oczekiwania stron zainteresowanych.	Test teoretyczny
	Określa zakres systemu zarządzania bezpieczeństwem informacji (SZBI).	Test teoretyczny
	Identyfikuje procesy systemu zarządzania bezpieczeństwem informacji (SZBI).	Analiza dowodów i deklaracji
	Omawia wymagania w zakresie określania polityki bezpieczeństwa.	Test teoretyczny
Określa rolę kierownictwa i personelu w systemie zarządzania bezpieczeństwem informacji (SZBI).	Omawia przewodnią rolę kierownictwa organizacji oraz ich zobowiązania.	Test teoretyczny
	Charakteryzuje role, odpowiedzialności i uprawnienia w ramach systemu zarządzania bezpieczeństwem informacji (SZBI).	Test teoretyczny
	Omawia kompetencje i świadomość personelu organizacji.	Test teoretyczny
	Przedstawia jak ważna jest komunikacja wewnętrzna i zewnętrzna związana z systemem zarządzania bezpieczeństwem informacji (SZBI).	Test teoretyczny
Określa ryzyka, szanse, cele i zasoby systemu zarządzania bezpieczeństwem informacji (SZBI).	Określa ryzyka i szanse odnośnie systemu zarządzania bezpieczeństwem informacji (SZBI), dokonuje ich oceny oraz określa działania odnoszące się do nich.	Test teoretyczny
	Wdraża działania i ocenia ich skuteczność.	Analiza dowodów i deklaracji
	Planuje cele bezpieczeństwa informacji oraz sposoby ich realizacji.	Analiza dowodów i deklaracji
	Określa niezbędne zasoby do wdrożenia, utrzymywania i doskonalenia systemu zarządzania bezpieczeństwem informacji (SZBI).	Test teoretyczny
	Szacuje ryzyko w bezpieczeństwie informacji oraz sposoby postępowania z tym ryzykiem.	Analiza dowodów i deklaracji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przygotowuje dokumentację związaną z systemem zarządzania bezpieczeństwem informacji (SZBI).	Wskazuje wymaganą dokumentację systemu zarządzania bezpieczeństwem informacji (SZBI).	Test teoretyczny
	Przygotowuje materiały wejściowe do okresowych przeglądów zarządzania.	Analiza dowodów i deklaracji
	Dokumentuje wyniki okresowych przeglądów zarządzania.	Analiza dowodów i deklaracji
Kontroluje system zarządzania bezpieczeństwem informacji (SZBI) w organizacji.	Planuje i nadzoruje działania operacyjne w kontekście bezpieczeństwa informacji.	Analiza dowodów i deklaracji
	Monitoruje system zarządzania bezpieczeństwem informacji (SZBI).	Analiza dowodów i deklaracji
	Przeprowadza audyt wewnętrzny bezpieczeństwa informacji – planuje, przeprowadza, dokumentuje i komunikuje wyniki audytów.	Analiza dowodów i deklaracji
	Planuje i nadzoruje realizację działań w odpowiedzi na audyty wewnętrzne bezpieczeństwa informacji.	Analiza dowodów i deklaracji
	Wdraża działania korekcyjne i korygujące oraz monitoruje skuteczność ich wdrożenia.	Analiza dowodów i deklaracji
	Ciągle doskonalą system zarządzania bezpieczeństwem informacji (SZBI).	Analiza dowodów i deklaracji
	Buduje pozytywną atmosferę bezpieczeństwa i zaufania w kontakcie z innymi ludźmi.	Obserwacja w warunkach rzeczywistych
Rozwija kompetencje społeczne.	Rozwija umiejętności komunikacyjne tj. słucha, zbiera informacje, zadaje pytania, udziela odpowiedzi, bierze udział w dyskusji.	Obserwacja w warunkach rzeczywistych
	Dostrzega, analizuje i rozwiązuje problemy.	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Efekty uczenia się umieszczone są na zaświadczeniu potwierdzającym, że uczestnik ukończył usługę rozwojową.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Na zaświadczeniu potwierdzającym, że uczestnik ukończył usługę rozwojową umieszczone są efekty uczenia się wraz z kryteriami ich weryfikacji oraz przypisaną do każdego kryterium weryfikacji metodą walidacji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Na zaświadczeniu potwierdzającym, że uczestnik ukończył usługę rozwojową znajduje się adnotacja dotycząca:

a. Osoby prowadzącej usługę – imię, nazwisko

b. Osoby walidującej usługę – imię, nazwisko

Program

PROGRAM USŁUGI:

1. Podstawy zarządzania bezpieczeństwem informacji w organizacji.
2. Zasady stosowania i struktura norm międzynarodowych serii ISO/IEC 27000.
3. Zasady certyfikacji systemów zarządzania bezpieczeństwem informacji z zastosowaniem wymagań ISO/IEC 27001:2022.
4. Zasady korzystania z wytycznych zawartych w normach ISO/IEC 27000.
5. Podstawowa terminologia stosowana w normach ISO/IEC 27000.
6. Zrozumienie i określenie kontekstu organizacji.
7. Zrozumienie potrzeb i oczekiwań stron zainteresowanych.
8. Określenie zakresu systemu zarządzania bezpieczeństwem informacji.
9. Procesy systemu zarządzania bezpieczeństwem informacji.
10. Przewodnia rola kierownictwa organizacji oraz ich zobowiązania.
11. Wymagania w zakresie określania polityki bezpieczeństwa.
12. Role, odpowiedzialności i uprawnienia w ramach systemu zarządzania bezpieczeństwem informacji.
13. Określenie ryzyk i szans odnośnie SZBI, ich ocena oraz określenie działań odnoszących się do nich. Wdrożenie tych działań i ocena ich skuteczności.
14. Planowanie celów bezpieczeństwa informacji oraz sposobu ich realizacji.
15. Niezbędne zasoby do wdrożenia, utrzymywania i doskonalenia SZBI.
16. Kompetencje i świadomość personelu organizacji.
17. Komunikacja wewnętrzna i zewnętrzna związana z SZBI.
18. Wymagana dokumentacja SZBI.
19. Planowanie i nadzór nad działaniami operacyjnymi w kontekście bezpieczeństwa informacji.
20. Szacowanie ryzyka w bezpieczeństwie informacji oraz postępowanie z tym ryzykiem.
21. Monitorowanie SZBI.
22. Audyt wewnętrzny bezpieczeństwa informacji – planowanie, przeprowadzanie, dokumentowanie i komunikowanie wyników audytów.
23. Planowanie i nadzór nad realizacją działań w odpowiedzi na audyty.
24. Przygotowanie materiałów wejściowych do okresowych przeglądów zarządzania.
25. Dokumentowanie wyników okresowych przeglądów zarządzania.
26. Realizacja działań korekcyjnych i korygujących i monitorowanie skuteczności ich wdrożenia.
27. Ciągłe doskonalenie SZBI.

Sposób weryfikacji efektów uczenia się:

Efekty uczenia się, osiągnięte dzięki udziałowi uczestników w usłudze rozwojowej „**Podstawy zarządzania bezpieczeństwem informacji. Wymagania normy ISO/IEC 27001:2022. Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) - szkolenie**” zostaną zweryfikowane poprzez:

- **WIEDZA** - przeprowadzenie przez Osobę prowadzącą usługę testu wśród uczestników. Test zostanie przeprowadzony w pierwszym dniu usługi rozwojowej (PRE TEST) w celu sprawdzenia poziomu wiedzy uczestników przed udziałem w usłudze rozwojowej. W dniu zakończenia usługi rozwojowej, jako jej podsumowanie zostanie przeprowadzony test (POST TEST) mający na celu sprawdzenie poziomu wiedzy uczestników po zakończeniu udziału w usłudze rozwojowej.

Dowód: PRE TEST + POST TEST

Przygotowanie, przeprowadzenie testu: Osoba prowadząca usługę

Walidacja: Osoba walidująca usługę

- **UMIĘJĘTNOŚCI** – analiza dowodów przez Osobę walidującą usługę. Osoba walidująca usługę na podstawie stworzonego przez Osobę prowadzącą usługę case study (studium przypadku) ocenia umiejętności uczestników w rzeczywistych sytuacjach, które mogą wystąpić.

Dowód: case study

Przygotowanie, przeprowadzenie case study: Osoba prowadząca usługę

Walidacja: Osoba walidująca usługę

- **KOMPETENCJE SPOŁECZNE** – obserwacja uczestników przez Osobę prowadzącą usługę oraz Osobę walidującą w warunkach rzeczywistych tj. podczas usługi rozwojowej. Analiza działań uczestników w zakresie kryteriów weryfikacji określonych w efekcie uczenia się „*Rozwija kompetencje społeczne*” w warunkach rzeczywistych, tj. podczas usługi rozwojowej.

Dodatkowo: wywiad Osoby walidującej usługę z Osobą prowadzącą usługę

Dowód: protokół z obserwacji i wywiadu

Walidacja: Osoba walidująca usługę

- Dodatkowo, osiągnięcie efektów uczenia się, w tym kryteriów weryfikacji zostanie zweryfikowane poprzez ankietę ewaluacyjną po zakończeniu usługi rozwojowej, mającą na celu indywidualne potwierdzenie przez każdego uczestnika usługi rozwojowej stopnia osiągnięcia przez niego danego efektu uczenia się w tym kryteriów weryfikacji.

Dowód: ankieta ewaluacyjna

Przeprowadzenie ankiety: Osoba prowadząca usługę

Walidacja: Osoba walidująca usługę

Warunki organizacyjne:

Usługa rozwojowa „**Podstawy zarządzania bezpieczeństwem informacji. Wymagania normy ISO/IEC 27001:2022. Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) - szkolenie**” realizowana będzie bez podziału na grupy. Usługa rozwojowa nie wymaga dostępu do indywidualnych stanowisk komputerowych. Sala w której będzie realizowana usługa rozwojowa będzie wyposażona w rzutnik, ekran do projektora. Na sali będzie dostęp do Internetu.

Czas trwania:

Usługa rozwojowa „**Podstawy zarządzania bezpieczeństwem informacji. Wymagania normy ISO/IEC 27001:2022. Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) - szkolenie**” trwa 7 godzin zegarowych, gdzie 1 godzina szkolenia trwa 60 minut.

Przerwy podczas usługi rozwojowej:

Dzień 1: 12.08.2024 r.

Przerwa nr 1: 11:00 – 11:15

Przerwa nr 2: 14:15 – 14:30

Informacje dodatkowe:

Usługa rozwojowa „**Podstawy zarządzania bezpieczeństwem informacji. Wymagania normy ISO/IEC 27001:2022. Wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) - szkolenie**”:

- może zostać przeprowadzona w formie zdalnej w czasie rzeczywistym,
- może zostać przeprowadzona dla zamkniętej grupy uczestników – szkolenie indywidualne, zamknięte,
- może zostać zrealizowana w innym, dogodnym terminie,

W celu ustalenia szczegółów realizacji zapraszamy do kontaktu mailowego.

Harmonogram

Liczba przedmiotów/zajęć: 14

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>1 z 14 Podstawy zarządzania bezpieczeństwem informacji w organizacji. Zasady stosowania i struktura norm międzynarodowych serii ISO/IEC 27000.</p>	Eligiusz Myśliwy	12-08-2024	08:00	08:30	00:30
<p>2 z 14 Zasady certyfikacji systemów zarządzania bezpieczeństwem informacji z zastosowaniem wymagań ISO/IEC 27001:2022. Zasady korzystania z wytycznych zawartych w normach ISO/IEC 27000.</p>	Eligiusz Myśliwy	12-08-2024	08:30	09:00	00:30
<p>3 z 14 Podstawowa terminologia stosowana w normach ISO/IEC 27000. Zrozumienie i określenie kontekstu organizacji. Zrozumienie potrzeb i oczekiwań stron zainteresowanych.</p>	Eligiusz Myśliwy	12-08-2024	09:00	09:30	00:30
<p>4 z 14 Określenie zakresu systemu zarządzania bezpieczeństwem informacji. Procesy systemu zarządzania bezpieczeństwem informacji.</p>	Eligiusz Myśliwy	12-08-2024	09:30	10:00	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>5 z 14 Przewodnia rola kierownictwa organizacji oraz ich zobowiązania. Wymagania w zakresie określania polityki bezpieczeństwa.</p>	Eligiusz Myśliwy	12-08-2024	10:00	10:30	00:30
<p>6 z 14 Role, odpowiedzialności i uprawnienia w ramach systemu zarządzania bezpieczeństwem informacji.</p>	Eligiusz Myśliwy	12-08-2024	10:30	11:00	00:30
<p>7 z 14 Określenie ryzyk i szans odnośnie SZBI, ich ocena oraz określenie działań odnoszących się do nich. Wdrożenie tych działań i ocena ich skuteczności.</p>	Eligiusz Myśliwy	12-08-2024	11:15	11:45	00:30
<p>8 z 14 Planowanie celów bezpieczeństwa informacji oraz sposobu ich realizacji. Niezbędne zasoby do wdrożenia, utrzymywania i doskonalenia SZBI.</p>	Eligiusz Myśliwy	12-08-2024	11:45	12:15	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>9 z 14 Kompetencje i świadomość personelu organizacji. Komunikacja wewnętrzna i zewnętrzna związana z SZBI. Wymagana dokumentacja SZBI.</p>	Eligiusz Myśliwy	12-08-2024	12:15	12:45	00:30
<p>10 z 14 Planowanie i nadzór nad działaniami operacyjnymi w kontekście bezpieczeństwa informacji. Szacowanie ryzyka w bezpieczeństwie informacji oraz postępowanie z tym ryzykiem. Monitorowanie SZBI.</p>	Eligiusz Myśliwy	12-08-2024	12:45	13:15	00:30
<p>11 z 14 Audyt wewnętrzny bezpieczeństwa informacji – planowanie, przeprowadzanie, dokumentowanie i komunikowanie wyników audytów.</p>	Eligiusz Myśliwy	12-08-2024	13:15	13:45	00:30
<p>12 z 14 Planowanie i nadzór nad realizacją działań w odpowiedzi na audyty.</p>	Eligiusz Myśliwy	12-08-2024	13:45	14:15	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>13 z 14</p> Przygotowanie materiałów wejściowych do okresowych przeglądów zarządzania. Dokumentowanie wyników okresowych przeglądów zarządzania.	Eligiusz Myśliwy	12-08-2024	14:30	15:00	00:30
<p>14 z 14</p> Realizacja działań korekcyjnych i korygujących i monitorowanie skuteczności ich wdrożenia. Ciągłe doskonalenie SZBI.	Eligiusz Myśliwy	12-08-2024	15:00	15:30	00:30

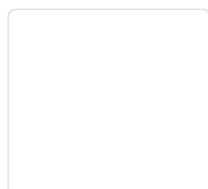
Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 291,50 PLN
Koszt przypadający na 1 uczestnika netto	1 050,00 PLN
Koszt osobogodziny brutto	184,50 PLN
Koszt osobogodziny netto	150,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Eligiusz Myśliwy

Certyfikowany Audytor Wewnętrzny (CIA – Certified Internal Auditor), Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji.

Ekspert w dziedzinie Zarządzania Jakością, trener, konsultant i pełnomocnik ds. jakości, specjalista w zakresie zarządzania ciągłością działania.

Doświadczony trener i wykładowca realizujący szkolenia i doradztwo z zakresu systemów zarządzania jakością w organizacjach.

Prowadzi konsultacje i szkolenia w dziedzinie ochrony danych osobowych, zarządzania ryzykiem, bezpieczeństwem informacji. Planuje audyty wewnętrzne w organizacjach klientów oraz realizuje zadania audytowe. Wdraża i doskonali Systemy Zarządzania Jakością w samorządach lokalnych, prywatnych przedsiębiorstwach.

Wdrożył systemy zarządzania w ponad 1,5 tys. przedsiębiorstw. Przeszkolił ponad 3 tysiące osób.

Posiada 20-letnie doświadczenie we wdrażaniu i doskonaleniu Systemów Zarządzania.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników otrzymuje komplet materiałów w wersji papierowej i/lub elektronicznej.

Każdy z uczestników otrzymuje prezentację multimedialną w wersji papierowej i/lub elektronicznej i/lub konspekt w wersji papierowej i/lub elektronicznej.

Dodatkowo, uczestnicy usługi rozwojowej otrzymają wykaz materiałów (książek, artykułów, stron internetowych, czasopism, rejestrów, ogólnodostępnych prezentacji ppt., materiałów audiovideo, e-podręczników, e-booków, itp.) umożliwiających utrwalenie efektów uczenia się, zdobytych w trakcie udziału w usłudze rozwojowej oraz umożliwiających samokształcenie się po zakończeniu usługi rozwojowej.

Uczestnicy otrzymają certyfikat i zaświadczenie, potwierdzające, że ukończyli usługę rozwojową.

Informacje dodatkowe

Usługa rozwojowa, która dla uczestnika ma charakter usługi kształcenia zawodowego / przekwalifikowania zawodowego i jest finansowana ze środków publicznych w co najmniej 70% jest zwolniona z podatku VAT na podstawie §3 ust.1 pkt 14 rozporządzenia Ministra Finansów z dn. 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U.2018.701)).

Cena usługi rozwojowej dla 1 uczestnika, który uzyskał dofinansowanie w co najmniej 70% wynosi **1 050,00 zł netto/brutto**.

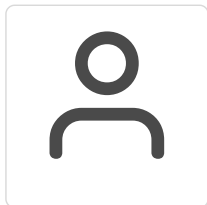
Cena usługi rozwojowej dla uczestników, którzy uzyskali dofinansowanie ze środków publicznych poniżej 70% oraz dla uczestników, którzy nie uzyskali takiego dofinansowania lub usługa rozwojowa nie ma charakteru usługi kształcenia zawodowego / przekwalifikowania zawodowego jest powiększona o podatek VAT (23%).

Cena usługi rozwojowej dla pozostałych (wyżej opisanych) uczestników to **1 050,00 zł netto + 241,50 zł 23%VAT = 1 291,50 zł/osoba brutto**.

Adres

ul. Brzeska 95
32-700 Bochnia
woj. małopolskie

Kontakt



Magdalena Polek

E-mail sekretariat@czj-infox.pl

Telefon (+48) 518 925 841