Możliwość dofinansowania

REA Sp. z o.o.

Brak ocen dla tego dostawcy

"Wymagania normy ISO 27001"

Numer usługi 2024/12/02/162530/2444756

1 000,00 PLN brutto
1 000,00 PLN netto
100,00 PLN brutto/h
100,00 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
10 h
28.01.2025 do 28.01.2025

Informacje podstawowe

Kategoria	Prawo i administracja / Administracja publiczna
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie jest przeznaczone głównie dla osób związanych z zarządzaniem bezpieczeństwem informacji, audytami wewnętrznymi, oraz zarządzaniem ryzykiem. Jest to także kurs przydatny dla osób, które chcą wdrożyć lub doskonalić systemy zarządzania bezpieczeństwem informacji w swoich organizacjach oraz dla tych, którzy dążą do uzyskania certyfikacji ISO 27001.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	21-01-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	10
Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych

Cel

Cel edukacyjny

Celem edukacyjnym szkolenia jest zapoznanie uczestników z wymaganiami normy ISO 27001 oraz zrozumienie kluczowych zasad i procesów związanych z zarządzaniem bezpieczeństwem informacji. Uczestnicy zdobędą wiedzę na temat struktury normy, w tym wymagań dotyczących planowania, wdrażania, oceny ryzyka oraz audytów. Szkolenie ma na celu umożliwienie uczestnikom zrozumienia korzyści biznesowych z wdrożenia ISO 27001, takich jak minimalizacja ryzyka i zwiększenie zaufania klientów. Uczestnicy nauczą si

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Poznają historię, zasady i strukturę normy ISO 27001 oraz jej kluczowe elementy, takie jak zarządzanie ryzykiem i kontrole bezpieczeństwa.	Ocena praktyczna, sprawdzająca, czy uczestnicy rozumieją kluczowe zasady normy ISO 27001, strukturę normy oraz wymagania dotyczące dokumentacji i procesów zarządzania ryzykiem.	Wywiad swobodny
Nauczą się przeprowadzać analizę ryzyka i oceniać zagrożenia oraz podatności w organizacji zgodnie z wymaganiami ISO 27001.	Sprawdzanie umiejętności uczestników w przeprowadzaniu analizy ryzyka, identyfikowaniu zagrożeń i podatności, oraz stosowaniu metod oceny ryzyka zgodnie z ISO 27001.	Wywiad swobodny
Zdobędą wiedzę na temat wymaganej dokumentacji oraz procedur związanych z wdrażaniem Systemu Zarządzania Bezpieczeństwem Informacji (ISMS).	Studium przypadku: weryfikacja umiejętności wdrażania konkretnych kontroli bezpieczeństwa, takich jak zarządzanie aktywami czy kryptografia, poprzez rozwiązanie praktycznego zadania związane z normą ISO 27001	Wywiad swobodny
Nauczą się wdrażać kontrole bezpieczeństwa, takie jak zarządzanie aktywami i kryptografia	Ocena dokumentacji : analiza przygotowanej przez uczestników dokumentacji ISMS, aby sprawdzić, czy spełnia wymagania normy ISO 27001, w tym identyfikację zasobów i procesów	Wywiad swobodny
Zdobędą kompetencje do przeprowadzania audytów wewnętrznych oraz oceny skuteczności wdrożonych działań w ramach ISO 27001	Przeprowadzenie symulacji audytu wewnętrznego, w której uczestnicy ocenią zgodność z ISO 27001 oraz zidentyfikują obszary do poprawy w systemie zarządzania bezpieczeństwem informacji.	Wywiad swobodny

Cel biznesowy

Do końca Q2 2026, wdrożyć System Zarządzania Bezpieczeństwem Informacji (ISMS) zgodny z normą ISO 27001 w naszej organizacji, aby zwiększyć bezpieczeństwo danych, zredukować ryzyko incydentów o 30% i uzyskać certyfikat zgodności z ISO 27001, co umożliwi poprawę reputacji firmy oraz zaufania klientów.

SMART:
Szczegółowy: Wdrożenie ISMS zgodnie z normą ISO 27001, uzyskanie certyfikatu.
Mierzalny: Zredukowanie ryzyka incydentów o 30%.
Realistyczny: Umożliwiają to dostępne zasoby, procedury oraz plan działania.
Terminowy: Zakończenie do końca Q2 2025.

Efekt usługi

Efekty usługi szkoleniowej:

1. **Zwiększona wiedza uczestników na temat normy ISO 27001:** Uczestnicy zdobędą szczegółową wiedzę na temat struktury normy, zasad oraz wymagań dotyczących bezpieczeństwa informacji.
2. **Umiejętność przeprowadzania analizy ryzyka:** Uczestnicy będą potrafili identyfikować zagrożenia, podatności i oceniać ryzyko w kontekście bezpieczeństwa informacji.
3. **Umiejętność wdrażania kontroli bezpieczeństwa:** Uczestnicy będą w stanie wdrożyć podstawowe kontrole bezpieczeństwa w organizacji zgodnie z załącznikiem A normy ISO 27001.
4. **Przygotowanie do audytów zgodności:** Uczestnicy będą w stanie przeprowadzać audyty wewnętrzne w celu oceny zgodności z normą ISO 27001.
5. **Kompetencje w zakresie dokumentacji ISMS:** Uczestnicy będą umieli przygotować i zarządzać dokumentacją wymaganą do wdrożenia ISMS w organizacji.

Kryteria weryfikacji efektywności szkolenia:

1. **Wywiad swobodny:** Sprawdzanie, czy uczestnicy posiadają wiedzę na temat kluczowych zasad normy ISO 27001, jej struktury oraz procesu analizy ryzyka.
2. **Praca praktyczna:** Ocena umiejętności uczestników w przeprowadzaniu analizy ryzyka oraz wdrażaniu kontroli bezpieczeństwa w kontekście konkretnego przypadku lub studium przypadku.
3. **Ocena dokumentacji:** Przegląd przygotowanej przez uczestników dokumentacji ISMS, aby ocenić jej zgodność z wymaganiami normy ISO 27001.
4. **Symulacja audytu:** Przeprowadzenie symulacji audytu wewnętrznego, w celu oceny, czy uczestnicy potrafią przeprowadzić audyt zgodności z normą ISO 27001 oraz zidentyfikować obszary do poprawy.
5. **Ankieta oceny szkolenia:** Zbieranie opinii uczestników na temat jakości szkolenia, jego przydatności oraz zdolności do zastosowania nabytej wiedzy w praktyce.

Metoda potwierdzenia osiągnięcia efektu usługi

Ocena praktyczna z wykorzystaniem studium przypadku i symulacji audytu:

1. **Studium przypadku:** Uczestnicy otrzymują konkretne scenariusze związane z bezpieczeństwem informacji i normą ISO 27001. Ich zadaniem jest przeprowadzenie analizy ryzyka, identyfikacja zagrożeń oraz wdrożenie odpowiednich kontroli bezpieczeństwa zgodnie z wymaganiami normy. Wyniki ich pracy są oceniane pod kątem zgodności z normą ISO 27001 i umiejętności zastosowania nabytej wiedzy w praktyce.
2. **Symulacja audytu:** Uczestnicy przeprowadzają audyt wewnętrzny w symulowanej organizacji, oceniając zgodność z normą ISO 27001. Audyt ten obejmuje identyfikację niezgodności, ocenę wdrożonych kontroli oraz przygotowanie raportu z rekomendacjami. Wyniki audytu potwierdzają umiejętność przeprowadzania audytów zgodności i efektywność zastosowanej wiedzy.

Weryfikacja:

- **Ocena wyników:** Wyniki analizy ryzyka, wdrożenia kontroli bezpieczeństwa oraz raporty z audytu są oceniane przez prowadzącego pod kątem zgodności z normą ISO 27001 i realności wdrożenia w organizacji.
- **Sprzedaż wyników:** Każdy uczestnik otrzymuje szczegółową informację zwrotną dotyczącą osiągniętych efektów, a także rekomendacje dla dalszego rozwoju umiejętności.

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Tak, dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

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

Tak, dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Tak, dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

Program

PROGRAM SZKOLENIA:

1. Wprowadzenie do normy ISO 27001

• Historia i cel normy ISO 27001.

• Podstawowe pojęcia: System Zarządzania Bezpieczeństwem Informacji (ISMS).

• Kluczowe zasady normy: poufność, integralność, dostępność informacji.

2. Korzyści z wdrożenia ISO 27001

• Korzyści biznesowe i operacyjne.

• Minimalizacja ryzyka i zwiększenie zaufania klientów.

• Spełnianie wymogów prawnych i regulacyjnych.

3. Struktura normy ISO 27001

• Omówienie kluczowych rozdziałów normy:

• Kontekst organizacji.

• Przywództwo.

• Planowanie.

• Wsparcie.

• Działania operacyjne.

• Ocena wydajności.

• Doskonalenie.

4. Podstawy analizy ryzyka w ISO 27001

• Identyfikacja zasobów, zagrożeń i podatności.

• Metodyka oceny ryzyka

• Definiowanie poziomów akceptowalnego ryzyka.

5. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (ISMS)

• Planowanie wdrożenia ISMS.

• Identyfikacja i mapowanie interesariuszy.

• Dokumentacja wymagana przez normę.

6. Kontrole bezpieczeństwa (Załącznik A)

• Przegląd 14 obszarów kontrolnych (np. polityki bezpieczeństwa, zarządzanie aktywami, kryptografia, fizyczne i środowiskowe bezpieczeństwo).

• Przykłady wdrożenia wybranych kontroli w organizacji.

7. Audyty zgodności z ISO 27001

8. Doskonalenie ciągłe

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt usługi brutto	1 000,00 PLN
Koszt usługi netto	1 000,00 PLN
Koszt godziny brutto	100,00 PLN
Koszt godziny netto	100,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne będą mieć formę:

- papierową w formie skryptu oraz notatek
- prezentacji multimedialnej
- certyfikat ukończenia szkolenia

Warunki uczestnictwa

Warunkiem niezbędnym do spełnienia przez uczestników, aby realizacja usługi pozwoliła na osiągnięcie głównego celu jest aktywność oraz obecność na szkoleniu.

Warunki techniczne

Szkolenie prowadzone będzie na pltformie Clickmeeting. Prezenterzy oraz uczestnicy nie muszą tworzyć konta, aby dołączyć do szkolenia. Mogą zostać zaproszeni do wydarzenia poprzez e-mail z linkiem przekierowującym do pokoju edukacyjnego. Platforma oparta jest na przeglądarce, wymagane zatem jest korzystanie z Google Chrome, Mozilla Firefox, Safari, Edge (Chromium), Yandex lub Opera.Platforma współpracuje z wszystkimi wbudowanymi w laptopy kamerami oraz większością kamer internetowych.

Kontakt

Małgorzata Bucka

E-mail rea.biurozarzadu@gmail.com
Telefon (+48) 789 574 344