

## **AUDYTY BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA**

### **WAŻNE INFORMACJE:**

Przedmiotem proponowanego szkolenia jest omówienie zagadnień związanych z audytem bezpieczeństwa informacji i cyberbezpieczeństwa, a w szczególności w zakresie:

- przydatnych narzędzi organizacyjnych w zapewnieniu skutecznego przeprowadzenia audytu bezpieczeństwa,
- praktycznych elementów prowadzenia audytu i bycia audytowanym,
- najczęstszych błędów popełnianych przez urzędy w zakresie cyberbezpieczeństwa, które są najczęściej widoczne podczas audytów.

### **CELE I KORZYŚCI ZE SZKOLENIA:**

- Omówienie zagadnień związanych z ochroną informacji, danych osobowych oraz cyberbezpieczeństwem w jednostkach publicznych w kontekście prowadzenia audytów (wewnętrznych i zewnętrznych).
- Zapoznanie się z zasadami przygotowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji.
- Przedstawienie podstawowych zasad przygotowania i prowadzenia audytów bezpieczeństwa.
- Przegląd dobrych praktyk dotyczących audytów KRI.
- Przedstawienie praktycznych zasad dotyczących analizy ryzyka w bezpieczeństwie informacji.
- Poznanie odpowiedzi na najczęściej pojawiające się pytania i wątpliwości związane z tematem zajęć.

### **PROGRAM:**

1. Przegląd aktów prawnych dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa: RODO, KRI, KSC.
2. Dyrektywa NIS2 – obowiązki dla podmiotów publicznych.
3. Budowa kultury ochrony informacji jako wyzwanie dla każdej organizacji - szanse i zagrożenia.
4. Przegląd norm serii ISO 2700x.
5. System Zarządzania Bezpieczeństwem Informacji – jak zbudować? Od czego zacząć?
6. Testy i audyty bezpieczeństwa – rodzaje i korzyści.
7. Audyt to nie kontrola.
8. Przygotowanie audytora do przeprowadzenia audytu.
9. Komunikacja podczas audytów i inne predyspozycje audytora.
10. Audyty KRI – założenia, główne obszary, przebieg, dobre praktyki.
11. Przegląd przekładowych działań korygujących i doskonalących po audytach KRI.
12. Analiza ryzyka w bezpieczeństwie informacji, przykładowe metodyki.
13. Zasoby, podatności i zagrożenia – sposoby identyfikacji na potrzeby szacowania ryzyka.

### **ADRESACI:**

Osoby koordynujące i nadzorujące pracę audytorów wewnętrznych i zespołów IT, pracownicy komórek audytu i kontroli, zespoły IT, Inspektorzy Ochrony Danych.

### **PROWADZĄCY:**

Trener, doradca i kierownik projektów. Specjalista w dziedzinie bezpieczeństwa informacji i cyberzagrożeń. Audytor wiodący normy ISO/IEC 27001:2017. Członek Polskiego Towarzystwa Informatycznego. Prowadzi audyty bezpieczeństwa oraz szkolenia i konsultacje m.in. z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa oraz budowania kultury ochrony informacji.

## Audyty bezpieczeństwa informacji i cyberbezpieczeństwa



Szkolenie będziemy realizowali w formie webinarium on line.



**28 kwietnia 2023 r.**      Szkolenie w godzinach 10:00-14:00



**Cena: 395 PLN netto/os.** Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

### CENA zawiera:

udział w profesjonalnym szkoleniu on-line z możliwością zadawania pytań,  
materiały szkoleniowe w wersji elektronicznej,  
certyfikat ukończenia szkolenia.

### DANE DO KONTAKTU:

Fundacja Rozwoju Demokracji Lokalnej Podkarpacki Ośrodek Samorządu Terytorialnego  
ul. Kolejowa 1, 35 – 073 Rzeszów  
tel. 17 862 69 64 [post@frdl.rzeszow.pl](mailto:post@frdl.rzeszow.pl)

## DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

Nazwa i adres nabywcy  
(dane do faktury)

Nazwa i adres odbiorcy

NIP

Telefon

1. Imię i nazwisko uczestnika, stanowisko,  
E-MAIL i TEL. DO KONTAKTU

2. Imię i nazwisko uczestnika, stanowisko,  
E-MAIL i TEL. DO KONTAKTU

Oświadczam, że szkolenie dla ww. pracowników jest kształceniem zawodowym finansowanym w całości lub co najmniej 70% ze środków publicznych (proszę zaznaczyć właściwe)      TAK   
NIE

Proszę o przesłanie faktury na adres mailowy: .....

Proszę o przesłanie certyfikatu na adres mailowy: .....

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora [www.frdl.rzeszow.pl](http://www.frdl.rzeszow.pl) oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

**Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na [www.frdl.rzeszow.pl](http://www.frdl.rzeszow.pl) do 24 kwietnia 2023 r.**

**UWAGA!** Liczba miejsc ograniczona. O udziale w szkoleniu decyduje kolejność zgłoszeń. Zgłoszenie na szkolenie musi zostać potwierdzone przesłaniem do Ośrodka karty zgłoszenia. Brak pisemnej rezygnacji ze szkolenia najpóźniej na trzy dni robocze przed terminem jest równoznaczny z obciążeniem Państwa należnością za szkolenie niezależnie od przyczyny rezygnacji. Płatność należy uregulować przelewem na podstawie wystawionej i przesłanej FV.

Podpis osoby upoważnionej \_\_\_\_\_