Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
27 maja 2024 r.

WPROWADZENIE DO WYKONYWANIA AUDYTÓW BEZPIECZEŃSTWA INFORMACJI I CYBERBEZPIECZEŃSTWA W JST

WAŻNE INFORMACJE O SZKOLENIU:

- Czy wdrażane przez jst zabezpieczenia w procesach ochrony informacji (w tym danych osobowych), wdrażane polityki i procedury bezpieczeństwa oraz liczne zabezpieczenia techniczne faktycznie działają? Czy są skuteczne?
- Czy kadra zarządzająca zdaje sobie sprawę ze swojej roli w procesie ochrony informacji? Czy pracownicy wiedzą, jak zgłaszać incydenty i dlaczego to jest tak ważne? Czy znają procedury? Czy w ogóle takie procedury są wdrożone?
- Czy wewnętrzne polityki i procedury oraz same systemy IT są aktualizowane, aby odpowiadały bieżącym wymaganiom i przeciwstawiały się realnym zagrożeniom?

W dobie coraz większej informatyzacji podmiotów i usług, a w konsekwencji coraz częściej występujących cyberataków - kradzieży lub wycieków danych należy na bieżąco analizować procesy w swoich jednostkach. Podstawowym narzędziem w tym zakresie jest audyt bezpieczeństwa informacji i cyberbezpieczeństwa, który odpowiada między innymi na te pytania i jest obiektywną formą weryfikacji, sprawdzenia czy i na ile wdrożone zabezpieczenia działają. Konieczność audytowania jst w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa wynika z przepisów (RODO, KRI, KSC) oraz dobrych praktyk, ponieważ nie ma lepszej drogi do sprawdzenia czy nasze zabezpieczenia działają jak ich weryfikacja.

Podczas proponowanego szkolenia krok po kroku omówimy przydatne narzędzia w zapewnieniu skutecznego przeprowadzenia audytu bezpieczeństwa. Przedstawimy praktyczne aspekty prowadzenia audytu oraz bycia audytowanym. Wyjaśnimy na czym polegają najczęstsze błędy popełniane przez jst w zakresie cyberbezpieczeństwa, które „widać" i „słychać" podczas audytów. Zaprezentujemy na przykładach jak przeprowadzić audyt wewnętrzny zgodnie z wymaganiami KRI.

CELE I KORZYŚCI:

- Zdobędziesz, uzupełnisz i uporządkujesz wiedzę związaną z ochroną informacji (w tym danych osobowych) oraz cyberbezpieczeństwem w jednostkach publicznych w kontekście prowadzenia audytów (wewnętrznych i zewnętrznych) oraz testów bezpieczeństwa.
- Poznasz zasady przygotowania i wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w jst.
- Dowiesz się jakie są podstawowe zasady przygotowania i prowadzenia audytów bezpieczeństwa zgodnie z Krajowymi Ramami Interoperacyjności (KRI).
- Poznasz dobre praktyki dotyczące prowadzenia audytów bezpieczeństwa.
- Zapoznasz się z praktycznymi zasadami dotyczącymi analizy ryzyka w bezpieczeństwie informacji.
- Dowiesz się jakie są najczęściej popełniane błędy i nieprawidłowości w zakresie bezpieczeństwa przetwarzania informacji i cyberbezpieczeństwa w jednostkach oraz poznasz sposoby postępowania mające na celu ich eliminację.
- Uzyskasz odpowiedzi na pojawiające się pytania i wątpliwości związane z przedmiotem zajęć m.in.
  - Czy warto robić testy bezpieczeństwa?
  - Jak się prawidłowo przygotować do testów bezpieczeństwa?
  - Czy o planowanych testach socjotechniczne warto informować pracowników? A jeśli tak, to jak to zrobić?
- Dowiesz się jak samodzielnie i bez dodatkowych kosztów przeprowadzić audyty KRI i KSC.
- Zapoznasz się ze sposobami przygotowania ewidencji zasobów (aktywów) oraz podatności i zagrożeń.

PROGRAM:

1. **Przegląd aktów prawnych dotyczących bezpieczeństwa informacji i cyberbezpieczeństwa:**
   - Ogólne Rozporządzenie o ochronie danych (RODO).
   - Rozporządzenie Krajowe Ramy Interoperacyjności (KRI).
   - Ustawa Krajowy System Cyberbezpieczeństwa (KSC).
2. **Nowa Dyrektywa NIS2:**
   - Obowiązki dla podmiotów publicznych.
   - Na co już teraz należy się przygotować?
3. **Budowa kultury ochrony informacji w jst:**
   - Wyzwanie dla każdej organizacji.
   - Szanse i zagrożenia.
4. **Przegląd norm serii ISO 27xxx.:**
   - Czy warto mieć normy ISO 27xxx w jst?
   - Dlaczego warto korzystać z dobrych praktyk zawartych w normach?
5. **System Zarządzania Bezpieczeństwem Informacji (SZBI) w jst:**
   - Jak zbudować skuteczny SZBI w jst? Od czego zacząć?
   - Jak się przygotować do wdrożenia SZBI?
   - Ciągłe doskonalenie.
6. **Zasoby, podatności i zagrożenia:**
   - Ewidencja zasobów IT i innych aktywów informacyjnych.
   - Sposoby identyfikacji na potrzeby szacowania ryzyka.
7. Szacowanie ryzyka w bezpieczeństwie informacji. Przykłady metodyk.
8. **Testy i audyty bezpieczeństwa:**
   - Rodzaje testów bezpieczeństwa.
   - Rodzaje audytów.
   - Korzyści dla jst z wykonania testów i audytów.
9. **Wybrane wnioski z kontroli NIK** dotyczących bezpieczeństwa informacji (danych osobowych).
10. **Wnioski z przeprowadzonych „Diagnoz cyberbezpieczeństwa”** oraz wykonanych „Ankiet dojrzałości cyberbezpieczeństwa” – przykłady z jst
11. **Audyty KRI:**
    - Główne obszary audytowania.
    - Przebieg audytu.
    - Dobre praktyki audytowania.
12. **Jak samodzielnie przeprowadzić audyt bezpieczeństwa informacji zgodnie z KRI i KSC?:**
    - Jak przygotować ankietę?
    - Jak przygotować raport z audytu?
13. **Przegląd przykładowych działań** zapobiegawczych, korygujących i doskonalących po audytach KRI.
14. **Pytania / Odpowiedzi / Dyskusja.**

ADRESACI:

- Osoby koordynujące i nadzorujące pracę audytorów wewnętrznych.
- Osoby koordynujące i nadzorujące pracę zespołów IT.
- Pracownicy komórek audytu i kontroli.
- Zespoły IT.
- Inspektorzy Ochrony Danych.

PROWADZĄCY:

Audytor, trener, doradca i kierownik projektów. Specjalista w dziedzinie bezpieczeństwa informacji i cyberbezpieczeństwa. Audytor wiodący normy ISO/IEC 27001. Członek Polskiego Towarzystwa Informatycznego. Prowadzi audyty bezpieczeństwa informacji oraz szkolenia z zakresu bezpieczeństwa informacji, przygotowania polityk bezpieczeństwa, cyberbezpieczeństwa i budowania kultury ochrony informacji.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Wprowadzenie do wykonywania audytów bezpieczeństwa informacji i cyberbezpieczeństwa w jst

Szkolenie będziemy realizowali **w formie webinarium on line**.

27 maja 2024 r. **Szkolenie w godzinach 10:00-14:00**

Cena: 435 PLN netto/os. **Przy zgłoszeniu do 26 kwietnia 2024 cena wynosi 399 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 OR w Gdańsku Targ Drzewny 3/7, 80-886 Gdańsk tel. 733 932 334 biuro.gdansk@frdl.org.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 ☐

Dokonanie zgłoszenia na szkolenie jest równoznaczne z zapoznaniem się i zaakceptowaniem regulaminu szkoleń Fundacji Rozwoju Demokracji Lokalnej zamieszczonym na stronie Organizatora **www.gdansk.frdl.pl** oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać na zgloszenia.gdansk@frdl.org.pl do 21 maja 2024 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 _____