Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

SZKOLENIE ON LINE
16 kwietnia 2026 r.

JAK WYGLĄDA AUDYT KLUCZOWYCH WSKAŹNIKÓW RYZYKA (KRI) W PRAKTYCE – PODEJŚCIE ISO 27001, DOWODY, USTALENIA I RAPORT

WAŻNE INFORMACJE O SZKOLENIU:

- Szkolenie pokazuje audyt wymagań KRI i uKSC z perspektywy dowodów, ustaleń audytowych i realnej logiki pracy audytora. Uczestnicy zobaczą, jak wymagania organizacyjne i techniczne „materializują się" w dokumentach, konfiguracjach, logach, rejestrach i decyzjach kierownictwa.
- Program oparty jest na praktycznym podejściu zgodnym z metodyką ISO/IEC 27001 – nie jako kurs audytora, lecz jako uporządkowana rama rozumienia: jak planuje się audyt, jak buduje łańcuch dowodowy oraz kiedy mamy do czynienia z niezgodnością (NC), a kiedy z obserwacją (OBS).
- Szkolenie ma charakter warsztatowy i analityczny – uczestnicy pracują na przykładach kart niezgodności, dowodów i uzasadnień. Dzięki temu lepiej przygotują się do audytu zewnętrznego, kontroli lub audytu wewnętrznego, a także będą potrafili samodzielnie ocenić, czy ich organizacja rzeczywiście spełnia wymagania KRI, czy jedynie „posiada dokument".
- To szkolenie jest szczególnie istotne dla jednostek sektora publicznego, w których wymagania KRI przenikają się z obowiązkami wynikającymi z Ustawa o Krajowym Systemie Cyberbezpieczeństwa – zwłaszcza w obszarze zarządzania ryzykiem, incydentów, logowania i monitoringu.
- Udział w szkoleniu pozwala uporządkować system zarządzania bezpieczeństwem informacji, ograniczyć ryzyko niezgodności podczas kontroli oraz świadomie budować dowody zgodności – zamiast reagować dopiero na ustalenia audytowe, a praca będzie opierała się na przykładach kart niezgodności (NC) obserwacji (OBS), ustaleń audytowych (DOW).

CELE I KORZYŚCI:

Udział w szkoleniu daje uczestnikowi tzw. świadomość audytową tzn. pozna:

- jakie są obszary wymagań KRI i uKSC (SZBI) i jak one w praktyce „materializują się" w organizacji,
- jak audytor planuje i wykonuje audyt zgodności (metodyka z ISO/IEC 27001 jako rama pracy, nie kurs audytora),
- jakie dowody są uznawane (dokumenty, rejestry, konfiguracje, logi, zapisy z systemów, testy),
- jak odróżnia się: ustalenia audytowe (UD) vs obserwację (OBS) vs niezgodność (NC) i jak buduje się uzasadnienie oraz działania korygujące.

PROGRAM:

1. **Jak przeprowadzany jest audyt wskaźników KRI:**
   a. Kryteria audytu (KRI jako reżim: zakres, próbka, scenariusze, lista żądanych dowodów (evidence request list),
   b. Techniki: przegląd dokumentów, wywiad, oględziny, testy, weryfikacja zapisów systemowych,
   c. Zasada: procedura ≠ działanie (jak audytor to weryfikuje).
2. **Jak wygląda „dowód zgodności" i jak ocenić jego jakość:**
   a. Typy dowodów (pierwotne vs wtórne; systemowe vs deklaratywne),
   b. Minimalne cechy dobrego dowodu: identyfikowalność, aktualność, integralność, możliwość odtworzenia,
   c. Jak dokumentuje się dowód (karta dow/ud) – co powinno się znaleźć, żeby dowód „obronił się" w audycie.
3. **Obszary audytu KRI – co powinno być audytowane i „po czym widać zgodność":**
   a. **Inwentaryzacja aktywów i zarządzanie zmianą (sprzęt, oprogramowanie, statusy):**
      - elementy audytowane: aktualność, kompletność, cykl życia, „wyzwalacze" aktualizacji, spójność z zakupami/likwidacją/naprawą,
      - dowody: rejestr aktywów + statusy, protokoły, potwierdzenia przekazań, raporty z narzędzi it, zgodność z konfiguracją,
      - typowe obs/nc: brak aktualizacji „na bieżąco", brak statusów/wycofania, niespójności między rejestrem a stanem faktycznym.
   b. **Ocena ryzyka i zarządzanie podatnościami (cyberbezpieczeństwo w praktyce):**
      - elementy audytowane: czy ryzyko jest liczone, akceptowane, redukowane i przeglądane; jak organizacja reaguje na podatności (patching),
      - dowody: rejestr ryzyk, decyzje i plany postępowania, harmonogramy aktualizacji, raporty podatności, wyjątki i ich akceptacje, testy po wdrożeniach,
      - typowe nc: ryzyko „opisane ogólnie", bez cyklu przeglądu; brak śladu decyzji kierownictwa; brak procesu podatności.
   c. **Nadawanie uprawnień, konta uprzywilejowane, kontrola dostępu:**

a. elementy audytowane: nadawanie/odbieranie, adekwatność, rozdział ról, recertyfikacje, admin/root, mfa, zasady wyjątków,
b. dowody: wnioski i akceptacje, rejestr uprawnień, raporty kont uprzywilejowanych, logi działań admina, wyniki przeglądów okresowych.

d. Praca zdalna i mobilna + ochrona danych na urządzeniach:
- elementy audytowane: zasady dostępu zdalnego, bezpieczeństwo stacji, urządzenia przenośne, szyfrowanie, mdm/vpn, reakcja na utratę sprzętu,
- dowody: „krok po kroku", konfiguracje (vpn/mfa), rejestr sprzętu, protokoły powierzenia, logi dostępu.

e. Dostawcy i usługi zewnętrzne (relacje, umowy, odpowiedzialności):
- elementy audytowane: czy wymagania bezpieczeństwa są „wpisane w relację", jak wygląda nadzór, offboarding, dostęp dostawców, logowanie, kopie, sla,
- dowody: umowy/załączniki bezpieczeństwa, rejestr dostawców, protokoły dostępów, raporty serwisowe, wyniki przeglądów.

f. Bezpieczeństwo fizyczne i środowiskowe (jako warunek ciągłości i ochrony):
- elementy audytowane: kontrola dostępu do stref, serwerowni/szaf, przechowywanie nośników, polityka kluczy, monitoring,
- dowody: ewidencja wejść/kluczy, uprawnienia, protokoły, oględziny, zapisy monitoringu (jeśli dotyczy).

g. Incydenty, działania korygujące i audyty wewnętrzne (cykl doskonalenia):
- elementy audytowane: czy incydenty są zgłaszane, analizowane i zamykane; czy są działania korygujące; czy audyt wewnętrzny działa realnie,
- dowody: rejestr incydentów, raporty i decyzje, capa (działania + terminy + odpowiedzialni + weryfikacja skuteczności), raporty z audytów.

h. Logi (co logować, jak długo i jak wykazać odtwarzalność):
- elementy audytowane: zakres logowania (w tym admin), retencja, ochrona logów, możliwość pozyskania logów z okresu retencji, centralizacja,
- dowody: konfiguracje logowania, polityka retencji, repozytoria logów, uprawnienia do logów, test „retrievability".

4. Kiedy stwierdzamy obserwację (OBS), a kiedy niezgodność (NC) – zasady dokumentowania ustaleń oraz przygotowania kart niezgodności:
a. Logika kwalifikacji: niespełnienie wymagania (NC) vs usprawnienie/dojrzałość (OBS),
b. Co powinna zawierać: fakt → dowód → kryterium → skutek/ryzyko → zalecenie → kryterium zamknięcia,
c. Jak przypisać odpowiedzialnego i jak ustawić weryfikację skuteczności.
d. Ćwiczenie na karcie NC dot. Ról/kompetencji i konfliktu interesów [np. IOD] (bardzo typowy problem w jednostkach).

5. Synergia wymagań: KRI, ISO/IEC 27001 oraz Ustawa o KSC w procesie audytu:
a. Krajowe Ramy Interoperacyjności (KRI) jako fundament SZBI i zasad logowania w administracji publicznej.
b. Metodyka ISO/IEC 27001 – jak wykorzystać standard do budowy spójnego systemu (kontekst, ryzyko, kontrole, audyt, zapisy, doskonalenie).
c. Krajowy System Cyberbezpieczeństwa (uKSC) – audyt w obliczu równoległych reżimów prawnych.
d. Punkty styku w praktyce: Jak efektywnie połączyć audyt ryzyka, incydentów i monitorowania logów według trzech standardów jednocześnie.

ADRESACI:

Szkolenie jest skierowane do kadry kierowniczej jednostek samorządu terytorialnego - **sekretarzy, dyrektorów wydziałów, kierowników jednostek organizacyjnych**, a także do osób odpowiedzialnych za system zarządzania bezpieczeństwem informacji (SZBI), kierowników i pracowników działów IT, administratorów systemów i sieci, inspektorów ochrony danych, audytorów wewnętrznych oraz pracowników komórek kontroli.
Adresatami są w szczególności osoby, które odpowiadają za przygotowanie jednostki do audytu wymagań KRI, gromadzenie i dokumentowanie dowodów zgodności, zarządzanie ryzykiem, incydentami oraz działaniami korygującymi – a także te, które podejmują decyzje w zakresie zgodności z wymaganiami KRI oraz obowiązkami wynikającymi z Ustawa o Krajowym Systemie Cyberbezpieczeństwa.

PROWADZĄCY:

nieetatowy współpracownik Wyższej Szkoły Nauk Pedagogicznych w Warszawie, audytor w zakresie realizacji wymagań zgodnych z KRI oraz audytor wiodący ISO 27001, obecnie zatrudniony jako inspektor ochrony danych w jednostkach samorządu terytorialnego, prelegent z wieloletnim doświadczeniem na szkoleniach z zakresu ochrony danych osobowych w jednostkach sektora publicznego. Wykładowca ceniony i polecany przez członków Forum Ochrony Danych działającego przy FRDL.

audytor wewnętrzny bezpieczeństwa informacji normy IOS27001, absolwent studiów podyplomowych na kierunku Inspektor Ochrony Danych. Aktywny członek stowarzyszenia inspektorów ochrony danych (SABI). Posiada doświadczenie w zakresie współpracy z administracją publiczną pełniąc funkcję inspektora ochrony danych oraz obsługując naruszenia ochrony danych. Prowadzi audyty ochrony danych osobowych, audyty bezpieczeństwa systemów informatycznych oraz szkolenia dla pracowników, których tematyka związana jest z danymi osobowymi, prywatnością a także bezpieczeństwem informacji.

Fundacja Rozwoju Demokracji Lokalnej
im. Jerzego Regulskiego

INFORMACJE ORGANIZACYJNE I KARTA ZGŁOSZENIA

Jak wygląda audyt kluczowych wskaźników ryzyka (KRI) w praktyce – podejście ISO 27001, dowody, ustalenia i raport

Szkolenie będziemy realizowali **w formie webinarium online**.

16 kwietnia 2026 r. **Szkolenie w godzinach 9.00-13.30**

Cena: 479 zł netto/os. Przy zgłoszeniu do 30 marca 2026 r. cena wynosi 449 zł. Udział w szkoleniu zwolniony z VAT w przypadku finansowania szkolenia ze środków publicznych.

CENA zawiera:	udział w profesjonalnym szkoleniu online z możliwością zadawania pytań, materiały szkoleniowe w wersji elektronicznej, certyfikat ukończenia szkolenia.
DANE DO KONTAKTU:	Fundacja Rozwoju Demokracji Lokalnej im. Jerzego Regulskiego Centrum Szkoleniowe FRDL ul. Księcia Witolda 7-9, po.102, 71-063 Szczecin; tel. +48 725 302 313, centrum@frdl.szczecin.p

DANE UCZESTNIKA ZGŁASZANEGO NA SZKOLENIE

(dane do faktury)
Nazwa i adres nabywcy
NIP Nabywcy
Nazwa i adres odbiorcy
NIP Odbiorcy

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 ☐

Faktura zostanie wystawiona jako faktura ustrukturyzowana w Krajowym Systemie e-Faktur (KSeF).
Uwagi: ……

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.szczecin.pl oraz zawartej w nim Polityce prywatności i ochrony danych osobowych.

Wypełnioną kartę zgłoszenia należy przesłać poprzez formularz zgłoszenia na www.frdl.szczecin.pl do 13 kwietnia 2026 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 faktury w KSeF.

Podpis osoby upoważnionej _____