Audytor wewnętrzny ISO/IEC 27001 (SZBI) (kod: ISO-27001-AUDYT)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Opis i cel szkolenia

Od nowelizacji ustawy o KSC system zarządzania bezpieczeństwem informacji (SZBI) muszą mieć podmioty kluczowe i ważne – a najczęściej buduje się go w oparciu o normę ISO/IEC 27001. Na tym szkoleniu przygotowujemy do roli audytora wewnętrznego SZBI. Pierwszy dzień poświęcamy wymaganiom normy, zabezpieczeniom z załącznika A i szacowaniu ryzyka na przykładzie modelowej instytucji. Drugi dzień to audyt wewnętrzny według wytycznych ISO 19011: od planu i list kontrolnych, przez rozmowy i dowody, po zapis niezgodności.

Po szkoleniu:

- zrozumiesz, czego norma ISO/IEC 27001 wymaga od organizacji i jak czytać te wymagania w praktyce,
- poznasz układ 93 zabezpieczeń z załącznika A i zobaczysz, czym jest deklaracja stosowania (SoA),
- przejdziesz przez szacowanie ryzyka – od aktywów, przez zagrożenia i podatności, po ocenę ryzyka,
- przygotujesz plan audytu i listę kontrolną pod kątem ISO/IEC 27001,
- przećwiczysz wywiad audytowy, a ustalenia zapiszesz jako niezgodności lub obserwacje,
- przygotujesz się do prowadzenia audytów wewnętrznych SZBI w swojej organizacji.

Normę omawiamy w wydaniu ISO/IEC 27001:2022 (w Polsce PN-EN ISO/IEC 27001:2023), z odniesieniami do polskich przepisów: Krajowych Ram Interoperacyjności i ustawy o KSC. Szkolenie prowadzą praktycy cyberbezpieczeństwa – jednym z nich jest **audytor wiodący SZBI wg ISO/IEC 27001** – więc obok zgodności z normą rozmawiamy też o tym, czy zabezpieczenia działają naprawdę. To podejście wynika z naszej oferty: od lat prowadzimy szkolenia z cyberbezpieczeństwa i sieci komputerowych dla administratorów, specjalistów IT i kadry zarządzającej. Zajęcia kończy test wiedzy. To autorskie szkolenie ALX: uczestnicy otrzymują certyfikat ukończenia szkolenia z listą omówionych tematów.

Jeśli szukasz corocznego szkolenia dla zarządu z art. 8e ustawy o KSC, zobacz KSC i NIS2 – obowiązki kierownika podmiotu.

Szkolenie przyda się przyszłym i obecnym audytorom wewnętrznym, pełnomocnikom i administratorom bezpieczeństwa informacji, inspektorom ochrony danych, pracownikom działów bezpieczeństwa, IT, compliance, zarządzania ryzykiem i audytu wewnętrznego, kierownikom komórek objętych SZBI, a także osobom, które przygotowują organizację do certyfikacji albo do wymogów ustawy o KSC – w firmach i w administracji publicznej.

Czas trwania

2 dni

Program

1. Wprowadzenie do systemu zarządzania bezpieczeństwem informacji (SZBI)
   - podstawowe pojęcia (poufność, integralność, dostępność) oraz kontekst prawny (m.in. KRI w administracji publicznej, ustawa o KSC / NIS2)
   - struktura normy ISO/IEC 27001:2022 (Harmonized Structure)

2. Interpretacja wymagań normy (rozdziały 4–10)
   — kontekst organizacji, strony zainteresowane i określenie zakresu SZBI (rozdz. 4)
   — przywództwo, polityka bezpieczeństwa, role i odpowiedzialności (rozdz. 5)
   — planowanie: cele SZBI i podejście oparte na ryzyku (rozdz. 6)
   — wsparcie i działania operacyjne: kompetencje, świadomość, komunikacja, nadzór nad udokumentowanymi informacjami (rozdz. 7–8)
   — monitorowanie, pomiary, przegląd zarządzania i ciągłe doskonalenie (rozdz. 9–10)
3. Przegląd zabezpieczeń z załącznika A (wg edycji 2022)
   — podział na 4 obszary tematyczne: zabezpieczenia organizacyjne, osobowe, fizyczne i technologiczne (93 zabezpieczenia) oraz deklaracja stosowania (SoA)
4. Warsztat praktyczny: szacowanie ryzyka
   — identyfikacja aktywów, zagrożeń i podatności oraz szacowanie ryzyka bezpieczeństwa informacji na przykładzie modelowej instytucji
5. Audytowanie wewnętrzne SZBI wg wytycznych normy ISO 19011 – zasady i rodzaje audytów
   — audyt pierwszej, drugiej i trzeciej strony
   — kompetencje i etyka audytora wewnętrznego
6. Planowanie i przygotowanie audytu SZBI
   — program audytów a plan audytu
   — przegląd dokumentacji i przygotowanie list kontrolnych (check-list) pod kątem ISO 27001
7. Przebieg audytu w praktyce
   — spotkanie otwierające, techniki prowadzenia wywiadów
   — zbieranie i weryfikacja dowodów audytowych
   — radzenie sobie z trudnymi sytuacjami
8. Dokumentowanie wyników i działania poaudytowe
   — klasyfikacja ustaleń (niezgodności, obserwacje), formułowanie kart niezgodności
   — ocena skuteczności działań korygujących
9. Warsztat praktyczny: scenki audytowe
   — symulacja wywiadu audytowego
   — identyfikacja niezgodności na podstawie opisów sytuacji
   — egzamin końcowy (test wiedzy)

Dla grup na zamówienie szkolenie możemy połączyć z audytem ciągłości działania wg ISO 22301. Obie normy mają wspólną strukturę (rozdziały 4–10) i tę samą metodykę audytu wg ISO 19011, dlatego oba tematy mieszczą się w trzech dniach zamiast czterech: dzień wspólny, dzień ISO/IEC 27001 i dzień ISO 22301. Przykłady i ćwiczenia możemy oprzeć na realiach organizacji zamawiającego.

Przeznaczenie i wymagania

Szkolenie przede wszystkim dla:
— kandydatów na audytorów wewnętrznych SZBI i osób, które już takie audyty prowadzą,
— pełnomocników, koordynatorów i administratorów bezpieczeństwa informacji oraz inspektorów ochrony danych,
— pracowników działów bezpieczeństwa, IT, compliance, zarządzania ryzykiem i audytu wewnętrznego,
— kierowników komórek objętych systemem zarządzania bezpieczeństwem informacji,

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

— osób przygotowujących organizację do certyfikacji ISO/IEC 27001 lub do wymogów ustawy o KSC.

Od uczestników oczekujemy ogólnej orientacji w tym, jak działa ich organizacja, i podstawowych pojęć z bezpieczeństwa informacji. Wcześniejsza znajomość normy ISO/IEC 27001 nie jest konieczna – wymagania omawiamy od początku. Doświadczenie z audytami innych systemów (np. ISO 9001) będzie mile widziane, ale nie jest wymagane.

Tekst normy nie jest częścią materiałów szkoleniowych. Kto ma do niej dostęp w swojej organizacji, może z niej korzystać na zajęciach.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

1640 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.