# Tytuł szkolenia: Przygotowanie i realizacja audytu bezpieczeństwa IT

## Kod szkolenia: INFRA-BEZP-AUDYT

## Wprowadzenie

Szkolenia jest ukierunkowane na zapoznanie się z obecnymi wymaganiami dla systemów teleinformatycznych oraz wskazuje elementy oceny poprawności wdrożenia i skuteczności zabezpieczeń. Na szkoleniu uczestnicy dowiedzą się w oparciu o jakie normy i wytyczne można przygotować audyt teleinformatyczny oraz jak przygotować raport po audytowy.

## Adresaci szkolenia

Szkolenie adresowane jest do audytorów wewnętrznych, administratorów bezpieczeństwa informacji, a także do osób na co dzień zajmujących się problematyką bezpieczeństwa i zarządzania bezpieczeństwem systemów teleinformatycznych, odpowiedzialnych za kontrolę systemów informatycznych.

## Cel szkolenia

Celem szkolenia jest przedstawienie zakresu wiedzy na temat wymagań norm międzynarodowych będących wytycznymi do przeprowadzenia audytu w systemach teleinformatycznych. Ponadto omówienie zakresu normy ISO/IEC 27001 i wymagań z nią związanych, które podlegają ocenie i kontroli w ramach prowadzonych działań audytowych. W ramach szkolenia omawiana jest dokumentacja systemu IT, stanowiąca integralną i nierozłączną cześć działania elementów zabezpieczeń w tych systemach oraz dokumentacja audytora.

## Czas i forma szkolenia

- 14 godzin (2 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

## Plan szkolenia

1. Aktualne tendencje rozwoju zagrożeń oraz zabezpieczanie systemów teleinformatycznych
2. Analiza ryzyka i zarządzanie ryzkiem dla systemów IT – ISO/IEC 27005 i ISO/IEC 31000
    a. Przedstawienie wybranych metodologii szacowania ryzyka
3. Audyt obszarów organizacyjnych i technicznych w oparciu o wybrane normy i metodyki międynarodwe
4. Zgodność systemów teleinformatycznych z przepisami prawnymi
    a. Analiza wymagań prawnych
    b. Analiza wymagań wynikających ze standardów
    c. Analiza wymagań wewnętrznych związanych z politykami, procedurami
5. Przygotowanie do audytu teleinformatycznego i przeprowadzenie audytu
    a. Plan audytu
    b. Etap 1 – elementy działań podejmowane z audytowana jednostką
    c. Etap 2 – plan działań w jednostce audytowanej
    d. Dowody audytowe
    e. Zakończenie audytu i draft raportu końcowego
    f. Audytor wiodący, audytorzy, zadania i wymagania
6. Ocena zastosowanych elementów bezpieczeństwa w postępowaniu audytowym
7. Raport końcowy po przeprowadzonym audycie i zalecenia końcowe
8. Audyt certyfikacyjny i audyt następczy