Tytuł szkolenia: Normy ISO/IEC 2700x w praktyce zarządzania bezpieczeństwem IT

Kod szkolenia: INFRA-BEZP-ISO-IEC

Wprowadzenie

Zapoznanie z wytycznymi dotyczącymi planowania, wdrożenia, utrzymania, oceny i zarządzania bezpieczeństwem systemów teleinformatycznych. Przybliżenie zagadnień związanych z pojęciami dotyczącymi bezpieczeństwa systemów teleinformatycznych, wskazanie elementów wchodzących w skład zarządzania bezpieczeństwem. Przedstawienie elementów niezbędnych do przygotowania i przeprowadzenia audytu wewnętrznego niezbędnego do oceny bezpieczeństwa teleinformatycznego.

Adresaci szkolenia

Szkolenie adresowane jest do administratorów bezpieczeństwa, oficerów bezpieczeństwa, a także do osób na co dzień zajmujących się problematyką bezpieczeństwa i zarządzania bezpieczeństwem systemów teleinformatycznych. Szkolenie jest również przeznaczone dla osób uczestniczących w pracach przygotowujących systemy teleinformatyczne do wdrożenia rozwiązań z obszaru ISO/IEC 2700x.

Cel szkolenia

Celem szkolenia jest przekazanie wiedzy na temat wymagań normy międzynarodowej**ISO/IEC 27001** w obszarze zarządzania bezpieczeństwem systemów teleinformatycznych. Wskazanie najważniejszych elementów wymaganych obligatoryjnie przez zapisy normy oraz sposoby rozwiązania, projektowania elementów bezpieczeństwa odpowiadających tym wymaganiom. W ramach szkolenia omawiana jest ponadto dokumentacja systemu, stanowiąca integralną i nierozłączną cześć działania elementów zabezpieczeń w systemach IT.

Czas i forma szkolenia

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

Plan szkolenia

1. Bezpieczeństwo systemów IT – wymagania wynikające z „rodziny” norm ISO/IEC – 2700x.
    a. Dlaczego bezpieczeństwo informacji jest kluczowe.
2. Podstawowe pojęcia związane z bezpieczeństwem systemów teleinformatycznych.
    a. Pojęcia związane z bezpieczeństwem, zarządzaniem bezpieczeństwem zarządzaniem ryzykiem dla systemów przetwarzających informacje
3. Zarządzanie bezpieczeństwem w systemach teleinformatycznych .
    a. Zarzadzanie ryzykiem w systemach IT – ISO/IEC 27005, ISO/IEC 31000
    b. Zarządzanie incydentami bezpieczeństwa informacji na bazie ISO/IEC 27035.
4. Planowanie, wdrożenie, zarządzanie i utrzymanie systemu bezpieczeństwa IT.
    a. Planowanie i jego elementy składowe.
    b. Przygotowanie do wdrożenia
    c. Utrzymanie i kontrola rozwiązań zabezpieczeń
    d. Audyt wewnętrzny i ocena skuteczności zastosowanych
5. Ocena bezpieczeństwa teleinformatycznego – ISO/IEC 27003
    a. Przygotowanie do przeprowadzenia kontroli
    b. Bieżące elementy nadzoru skuteczności systemu
6. Przygotowanie i przeprowadzenie audytu wewnętrznego dla oceny bezpieczeństwa teleinformatycznego.
7. Audyt certyfikacyjny