

Zarządzanie projektem wdrożenia i doskonalenia SZBI zgodnego z ISO/IEC 27001

Szkolenie buduje kompetencje prowadzenia wdrożenia i doskonalenia systemu zarządzania bezpieczeństwem informacji (SZBI) zgodnego z ISO/IEC 27001 jako dobrze zarządzanego projektu - od analizy luk i uzasadnienia biznesowego, przez harmonogram, rejestr ryzyka i współpracę z interesariuszami, po audyt certyfikacyjny i przekazanie systemu do utrzymania.

Program osadza dobre praktyki zarządzania projektami według PMBOK® Guide i ISO 21502 w realiach przedsięwzięć dostosowawczych wynikających m.in. z dyrektywy NIS2 i ustawy o krajowym systemie cyberbezpieczeństwa (KSC 2.0).

Po szkoleniu będziesz w stanie zaplanować projekt wdrożenia SZBI od celu po harmonogram z kamieniami milowymi audytów, zbudować rejestr ryzyka projektu oraz przygotować organizację do audytu certyfikacyjnego i przekazania systemu do doskonalenia.



Odbiorcy szkolenia

- Pełnomocnicy i koordynatorzy SZBI odpowiedzialni za wdrożenie lub doskonalenie systemu zgodnego z ISO/IEC 27001
- Specjaliści bezpieczeństwa informacji i cyberbezpieczeństwa prowadzący projekty dostosowawcze do wymagań NIS2 i KSC 2.0
- Specjaliści compliance i audytu wewnętrznego uczestniczący w projektach z obszaru bezpieczeństwa informacji

- Menedżerowie i specjaliści IT odpowiedzialni za wdrażanie zabezpieczeń i współpracę z obszarem bezpieczeństwa
- Kierownicy projektów, którym powierzono prowadzenie wdrożenia SZBI
- Osoby przygotowujące organizację do certyfikacji ISO/IEC 27001



Korzyści

- Zaplanujesz projekt wdrożenia SZBI od wymogu regulacyjnego lub potrzeby biznesowej po kompletną kartę projektu z celami, zakresem i kryteriami sukcesu
- Zbudujesz strukturę podziału pracy (WBS) i harmonogram wdrożenia z kamieniami milowymi: deklaracją stosowania, audytem wewnętrznym, przeglądem zarządzania i audytem certyfikacyjnym
- Rozróżnisz ryzyko projektowe od ryzyka bezpieczeństwa informacji i poprowadzisz oba procesy zgodnie z ISO 31000 oraz ISO/IEC 27005
- Zmapujesz interesariuszy projektu – od zarządu i właścicieli ryzyka po dostawców i jednostkę certyfikującą – i dobierzesz strategię ich angażowania
- Przygotujesz raport statusowy projektu i poprowadzisz komunikację wspierającą decyzje sponsora i komitetu sterującego
- Zastosujesz wymagania dyrektywy NIS2 i ustawy KSC 2.0 jako źródło zakresu i priorytetów projektu dostosowawczego
- Przygotujesz organizację do audytu certyfikacyjnego oraz zaplanujesz postępowanie z niezgodnościami i obserwacjami
- Przekażesz SZBI do utrzymania i doskonalenia w cyklu PDCA, domykając projekt bez utraty wypracowanych rezultatów



Program szkolenia

1. Wdrożenie SZBI jako projekt – kontekst normy i regulacji
 - Wymagania ISO/IEC 27001 z perspektywy przedsięwzięcia organizacyjnego: co trzeba wytworzyć, wdrożyć i utrzymać
 - Otoczenie regulacyjne jako motor projektów: dyrektywa NIS2, ustawa o krajowym systemie cyberbezpieczeństwa (KSC 2.0), wymagania sektorowe
 - Projekt a system zarządzania: wdrożenie SZBI kończy się, system trwa – konsekwencje dla planowania
 - Cykl życia projektu według PMBOK® Guide i ISO 21502 na przykładzie wdrożenia SZBI
 - Ćwiczenie praktyczne: mapa przedsięwzięcia – produkty projektu wdrożenia SZBI i ich odbiorcy
2. Od analizy luk do uzasadnienia biznesowego i karty projektu
 - Analiza luk względem ISO/IEC 27001 jako punkt startu i źródło zakresu projektu

- Uzasadnienie biznesowe projektu: koszty, korzyści, konsekwencje zaniechania (sankcje, incydenty, utrata kontraktów)
 - Karta projektu wdrożenia SZBI: cele, zakres systemu, produkty, kryteria sukcesu, założenia i ograniczenia
 - Role w projekcie: sponsor, kierownik projektu, pełnomocnik SZBI, właściciele ryzyk, komitet sterujący
 - *Ćwiczenie praktyczne: karta projektu wdrożenia SZBI dla studium przypadku*
3. Interesariusze projektu wdrożenia SZBI
- Identyfikacja interesariuszy: zarząd, kierownicy obszarów, IT, HR, dostawcy, jednostka certyfikująca, regulatorzy
 - Mapa wpływu i nastawienia oraz strategie angażowania interesariuszy
 - Budowanie poparcia dla zmian wynikających z wdrożenia zabezpieczeń – opór organizacyjny i sposoby pracy z nim
 - *Ćwiczenie praktyczne: mapa interesariuszy i plan ich angażowania dla studium przypadku*
4. Planowanie zakresu i harmonogramu wdrożenia
- Struktura podziału pracy (WBS) projektu wdrożenia SZBI: od kontekstu organizacji, przez szacowanie ryzyka i deklarację stosowania, po wdrożenie zabezpieczeń, szkolenia i audyty
 - Kamienie milowe projektu: deklaracja stosowania, wdrożenie zabezpieczeń, audyt wewnętrzny, przegląd zarządzania, audyt certyfikacyjny (etap 1 i 2)
 - Sekwencja zadań, zależności, ścieżka krytyczna i rezerwy w harmonogramie
 - *Ćwiczenie praktyczne: WBS i harmonogram wdrożenia SZBI z kamieniami milowymi dla studium przypadku*
5. Ryzyko w projekcie wdrożenia SZBI – dwa poziomy zarządzania
- Ryzyko projektowe a ryzyko bezpieczeństwa informacji: rozróżnienie, powiązania i typowe pomyłki
 - Zarządzanie ryzykiem projektu według ISO 31000 i dobrych praktyk PMBOK® Guide: identyfikacja, ocena, reakcje
 - Szacowanie ryzyka bezpieczeństwa informacji według ISO/IEC 27005 jako zadanie w harmonogramie projektu
 - Rejestr ryzyka projektu, macierz prawdopodobieństwa i wpływu, właściciele ryzyk
 - *Ćwiczenie praktyczne: rejestr i macierz ryzyka projektu wdrożenia SZBI dla studium przypadku*
6. Realizacja projektu – zabezpieczenia, dostawcy, komunikacja
- Wdrażanie zabezpieczeń z Załącznika A: praca z właścicielami obszarów i priorytetyzacja działań
 - Współpraca z dostawcami i podwykonawcami: wymagania bezpieczeństwa w umowach, nadzór nad realizacją
 - Monitorowanie postępu prac, zarządzanie zmianą zakresu i harmonogramu
 - Raport statusowy projektu: postęp, ryzyka, decyzje do podjęcia; raportowanie do sponsora i komitetu sterującego
 - *Ćwiczenie praktyczne: raport statusowy i symulacja spotkania komitetu sterującego*
7. Droga do certyfikacji – audyty jako kamienie milowe projektu
- Audyt wewnętrzny i przegląd zarządzania: planowanie w harmonogramie, przygotowanie organizacji i dokumentacji

- Audyt certyfikacyjny etap 1 i 2: przebieg, typowe niezgodności i obserwacje, rola zespołu projektowego
 - Postępowanie z niezgodnościami: działania korygujące jako element planu projektu
 - *Ćwiczenie praktyczne: plan przygotowania organizacji do audytu certyfikacyjnego dla studium przypadku*
8. Zamknięcie projektu i przejście do doskonalenia SZBI
- Przekazanie SZBI do utrzymania: role, procesy, kompetencje po stronie organizacji
 - Formalne zamknięcie projektu, rozliczenie z interesariuszami i lessons learned
 - Doskonalenie SZBI w cyklu PDCA: skąd będą pochodzić kolejne projekty i inicjatywy
 - *Ćwiczenie praktyczne: plan przekazania systemu do utrzymania oraz retrospektywa – indywidualny plan przeniesienia dobrych praktyk do własnego projektu*



Oczekiwane przygotowanie uczestnika

- Znasz podstawowe pojęcia z obszaru bezpieczeństwa informacji lub compliance
- Masz doświadczenie w pracy w projektach lub przedsięwzięciach organizacyjnych – w dowolnej roli
- Znasz wymagania ISO/IEC 27001 (mile widziane)
- Znajomość formalnych metodyk zarządzania projektami nie jest wymagana



Czas trwania

2 dni / 16 godzin

Język

- Szkolenie: polski
- Materiały: polski