kod szkolenia: ZP-BIZP / PL DL 2d

Bezpieczeństwo informacji w zarządzaniu projektami

Szkolenie buduje kompetencje uwzględniania bezpieczeństwa informacji w codziennym zarządzaniu projektami - od wymagań bezpieczeństwa w zakresie i harmonogramie, przez ryzyka i umowy z dostawcami, po obsługę incydentu i odbiory z testami oraz audytami bezpieczeństwa. Program łączy dobre praktyki PMBOK® Guide i ISO 21502 z wymaganiami ISO/IEC 27001 oraz obowiązkami wynikającymi z dyrektywy NIS2 i ustawy o krajowym systemie cyberbezpieczeństwa (KSC 2.0) - w tym z ich konsekwencjami dla dostawców i podwykonawców w łańcuchu dostaw. Po szkoleniu będziesz w stanie włączyć wymagania bezpieczeństwa do planu projektu w cyklu tradycyjnym i zwinnym, prowadzić rejestr ryzyka obejmujący ryzyka bezpieczeństwa informacji oraz sformułować wymagania wobec dostawców i zasady pracy zespołu z informacjami wrażliwymi.

Odbiorcy szkolenia

- Kierownicy projektów prowadzący projekty IT i biznesowe w organizacjach o podwyższonych wymaganiach bezpieczeństwa
- Specjaliści i menedżerowie PMO odpowiedzialni za standardy prowadzenia projektów w organizacji
- Kierownicy projektów u dostawców i podwykonawców podmiotów objętych wymaganiami NIS2 i KSC 2.0
- Product Ownerzy i liderzy zespołów wytwórczych pracujący z informacjami wrażliwymi
- Analitycy biznesowi i systemowi formułujący wymagania dla rozwiązań IT
- Osoby przygotowujące się do prowadzenia projektów w środowisku regulowanym

Korzyści

- Włączysz wymagania bezpieczeństwa informacji do zakresu, harmonogramu i budżetu projektu – od karty projektu po kryteria odbioru
- Zastosujesz zasadę security by design w cyklu tradycyjnym i zwinnym: wymagania niefunkcjonalne, definition of done, kryteria akceptacji
- Zidentyfikujesz i ocenisz ryzyka bezpieczeństwa informacji w rejestrze ryzyka projektu zgodnie z ISO 31000 i ISO/IEC 27005
- Sformułujesz wymagania bezpieczeństwa wobec dostawców i podwykonawców na potrzeby umów oraz postępowań zakupowych
- Zorganizujesz pracę zespołu z informacjami wrażliwymi: klasyfikacja informacji, zasada wiedzy koniecznej, bezpieczne narzędzia pracy (w tym narzędzia AI)
- Rozpoznasz incydent bezpieczeństwa w trakcie projektu i poprowadzisz jego obsługę we współpracy z zespołem bezpieczeństwa, z uwzględnieniem obowiązków NIS2 i KSC 2.0
- Zaplanujesz testy, przeglądy i audyty bezpieczeństwa jako punkty kontrolne w harmonogramie i warunki odbioru produktów projektu
- Przełożysz wymagania ISO/IEC 27001 klienta lub własnej organizacji na konkretne działania i produkty w projekcie

Program szkolenia

1. Bezpieczeństwo informacji jako obowiązek kierownika projektu
   - Dlaczego bezpieczeństwo trafia do projektów: wymagania klientów, certyfikacja ISO/IEC 27001, dyrektywa NIS2 i ustawa KSC 2.0, odpowiedzialność w łańcuchu dostaw
   - Informacje w projekcie: klasyfikacja, dane osobowe (RODO), tajemnica przedsiębiorstwa, informacje prawnie chronione
   - Podział ról: kierownik projektu, zespół bezpieczeństwa, inspektor ochrony danych, właściciele informacji
   - *Ćwiczenie praktyczne: mapa informacji w projekcie – co przetwarzamy, skąd pochodzi, kto ma dostęp*
2. Wymagania bezpieczeństwa w zakresie projektu
   - Security by design: wymagania bezpieczeństwa jako wymagania niefunkcjonalne od pierwszego dnia projektu
   - Wymagania w cyklu tradycyjnym: karta projektu, specyfikacja, kryteria odbioru
   - Wymagania w cyklu zwinnym: definition of done, kryteria akceptacji, historyjki dotyczące bezpieczeństwa
   - Typowe źródła wymagań: ISO/IEC 27001 i Załącznik A, polityki organizacji, wymagania kontraktowe klienta

- *Ćwiczenie praktyczne: wymagania bezpieczeństwa dla studium przypadku – wersja tradycyjna i zwinna*

3. Bezpieczeństwo w harmonogramie i budżecie
   - Działania bezpieczeństwa jako zadania w WBS: analizy, testy, przeglądy kodu, testy penetracyjne, audyty
   - Punkty kontrolne i kamienie milowe związane z bezpieczeństwem oraz ich wpływ na ścieżkę krytyczną
   - Koszt zabezpieczeń i rezerwy budżetowe na działania bezpieczeństwa
   - *Ćwiczenie praktyczne: uzupełnienie WBS i harmonogramu studium przypadku o działania bezpieczeństwa*
4. Ryzyka bezpieczeństwa informacji w rejestrze ryzyka projektu
   - Ryzyko projektowe a ryzyko bezpieczeństwa informacji – wspólny rejestr, różne perspektywy
   - Identyfikacja i ocena ryzyk zgodnie z ISO 31000, z wykorzystaniem podejścia ISO/IEC 27005
   - Typowe ryzyka: wyciek danych, dostęp osób nieuprawnionych, podatności rozwiązania, błędy dostawców
   - Strategie reakcji i właściciele ryzyk – współpraca kierownika projektu z zespołem bezpieczeństwa
   - *Ćwiczenie praktyczne: rejestr ryzyka studium przypadku rozszerzony o ryzyka bezpieczeństwa informacji*
5. Dostawcy i podwykonawcy – bezpieczeństwo w łańcuchu dostaw
   - Wymagania NIS2 i KSC 2.0 wobec łańcucha dostaw i ich konsekwencje dla projektów
   - Wymagania bezpieczeństwa w postępowaniach zakupowych i umowach: NDA, powierzenie przetwarzania danych, prawo do audytu
   - Weryfikacja dostawcy przed umową i nadzór nad dostawcą w trakcie realizacji
   - *Ćwiczenie praktyczne: zestaw wymagań bezpieczeństwa do umowy z dostawcą dla studium przypadku*
6. Codzienna praca zespołu z informacjami wrażliwymi
   - Zasada wiedzy koniecznej i zarządzanie dostępami w cyklu życia projektu – od onboardingu po odejście członka zespołu
   - Bezpieczne narzędzia pracy projektowej: repozytoria, komunikatory, przestrzenie współdzielone, praca zdalna
   - Narzędzia AI w pracy projektowej: co wolno, czego nie wolno, jak ustalić zasady w zespole
   - *Ćwiczenie praktyczne: zasady pracy z informacją dla zespołu studium przypadku*
7. Incydent bezpieczeństwa w trakcie projektu
   - Rozpoznanie incydentu i pierwsze decyzje kierownika projektu
   - Zgłaszanie incydentów: ścieżki wewnętrzne oraz obowiązki raportowe według NIS2 i KSC 2.0
   - Wpływ incydentu na projekt: zakres, harmonogram, komunikacja z interesariuszami i klientem
   - *Ćwiczenie praktyczne: symulacja decyzyjna – incydent bezpieczeństwa w trakcie realizacji studium przypadku*
8. Odbiory, zamknięcie projektu i przekazanie do utrzymania
   - Testy i audyty bezpieczeństwa jako warunek odbioru produktów projektu
   - Dokumentacja bezpieczeństwa przekazywana do utrzymania i wsparcia

- Zamknięcie projektu: odebranie dostępów, archiwizacja, lessons learned z obszaru bezpieczeństwa
- *Ćwiczenie praktyczne: lista kontrolna bezpieczeństwa dla odbioru i zamknięcia projektu oraz retrospektywa – indywidualny plan zastosowania dobrych praktyk we własnym projekcie*

Oczekiwane przygotowanie uczestnika

- Masz doświadczenie w prowadzeniu projektów lub pracy w zespole projektowym
- Znasz podstawowe produkty zarządcze, np. kartę projektu, harmonogram, rejestr ryzyka lub backlog
- Wiedza z obszaru bezpieczeństwa informacji nie jest wymagana

Czas trwania

2 dni / 16 godzin

Język

- Szkolenie: polski
- Materiały: polski