SZCZEGÓŁY OFERTY

Szkolenie komórki ds. bezpieczeństwa – Zadania komórki ds. ryzyka ICT, pomiar ryzyka ICT, raportowanie ryzyka ICT wg przepisów DORA

I. ADRESACI:

1. Członkowie Zarządu nadzorujący IT
2. Pracownicy pełniący funkcję Inspektora Ochrony Danych
3. Pracownicy pełniący obowiązki Administratora/Stanowiska ds. bezpieczeństwa
4. Pracownicy banku odpowiedzialni za ryzyko braku zgodności (compliance)
5. Pracownicy komórek ds. kontroli wewnętrznej

II. WYMAGANIA WSTĘPNE DLA UCZESTNIKÓW:

1. Ogólna znajomość przepisów w zakresie ochrony informacji, w tym DORA
2. Ogólna znajomość przepisów dot. ochrony danych osobowych
3. Ogólna znajomość praktyki działania banku spółdzielczego

III. CEL SEMINARIUM:

1. Pozyskać informacje o zasadach wdrożenia Rekomendacji D i doskonaleniu jej stosowania w typowym banku spółdzielczym, posiadającym niewielką komórkę ds. informatyki lub zewnętrzną obsługę
2. Uzyskać przykłady regulacji wewnętrznych oraz sprawozdań

IV. KORZYŚCI Z UCZESTNICTWA W SEMINARIUM:

1. Uzyskanie wiedzy o nowych wymaganiach związanych z zadaniami swojego stanowiska pracy/służbowego
2. Uzyskanie przykładowych regulacji wewnętrznych i wzorów sprawozdań do wykorzystania w Banku – po przeglądzie

Po szkoleniu otrzymujecie Państwo:

1. Strategia operacyjnej odporności cyfrowej Zgodna z DORA
2. Polityka bezpieczeństwa informacji, w tym załączniki dotyczące zadań komórki ds. bezpieczeństwa – 2025 Zgodna z DORA oraz RTS dot. ryzyka ICT
3. Zasady/instrukcja użytkowania systemów – dla użytkowników systemów – 2025 Przegląd obejmujący wymagania DORA
4. Zasady/instrukcja w zakresie zarządzania architekturą i jakością danych 2025 – (przepisy nadal obowiązują – Rekomendacja 4.14, są też nowe w ramach
DORA) Przegląd obejmujący wymagania Rekomendacji M KNF, DORA
5. Przykładowa analiza ryzyka ICT Obejmujące wymagania DORA
6. Przykładowy raport komórki ds. bezpieczeństwa (komórki ds. ryzyka ICT) Obejmujące wymagania DORA

Program szkolenia

1. Bezpieczeństwo informacji w banku, a ryzyko ICT
2. Struktura organizacyjna w zakresie nadzoru nad bezpieczeństwem informacji / ryzykiem ICT
1) Umiejscowienie komórki ds. bezpieczeństwa (komórki ds. ryzyka ICT) w strukturze organizacyjnej wg przepisów bankowych
2) Ryzyko konfliktu interesów – jakie komórki mogą pełnić funkcję ds. bezpieczeństwa (komórki ds. ryzyka ICT)?
3. Rola i zadania komórki ds. bezpieczeństwa (komórki ds. ryzyka ICT)
1) Zadania komórki wg DORA
2) Zadania komórki wg Rekomendacji KNF dot. ryzyka transakcji płatniczych w internecie
4. Ramy (system) zarządzania ryzykiem ICT
5. Proces zarządzania ryzykiem ICT wg DORA i dobrych praktyk (ISO 27001, ISO 27005)
1) Metodyka identyfikacji i szacowania ryzyka
2) Akceptacja ryzyka
3) Plany postępowania z ryzykiem
4) Raportowanie ryzyka
6. Nadzór komórki ds. bezpieczeństwa nad przestrzeganiem polityki bezpieczeństwa
1) Klasyfikacja i dokumentowanie zasobów danych, zasobów ICT (systemów i infrastruktury)
2) Nadzór nad wdrożeniami i zarządzanie zmianami w systemach
3) Nadzór nad analizą ryzyka i podatnościami, wdrażaniem poprawek
4) Nadzór nad przestrzeganiem zasad czystego biurka, ekranu, kosza, drukarki
5) Przegląd uprawnień
6) Nadzór nad działaniem użytkowników uprzywilejowanych
7. Rozwój i wdrażanie systemów i zapewnienie bezpieczeństwa informacji
1) Przepisy DORA
2) Przepisy RODO
3) Typowe błędy i zaniechania
8. Szkolenia i budowanie świadomości ryzyka ICT
1) Program zwiększania świadomości w zakresie bezpieczeństwa ICT
2) Częstotliwość i zakres szkoleń
9. Reakcja na incydenty bezpieczeństwa
1) Zdarzenie, a incydent
2) Identyfikacja zdarzeń dotyczących ryzyka ICT
3) Identyfikacja incydentów związanych z ryzykiem ICT lub bezpieczeństwem
4) Reakcja na incydenty bezpieczeństwa
5) Naruszenia ochrony danych osobowych i zgłaszanie do PUODO
10. Zarządzanie architekturą i jakością danych (Rekomendacja M 4.14 KNF)
11. Przeglądy i testowanie bezpieczeństwa
1) Program Testowania Operacyjnej Odporności Cyfrowej Banku
2) Rodzaje działań w ramach programu testowania operacyjnej odporności cyfrowej
12. Nadzór nad zewnętrznymi dostawcami usług ICT
13. Obszary i zakres raportowania komórki ds. bezpieczeństwa (komórki ds. ryzyka IsCT)
VI. METODYKA:
1) Wykład
2) Prezentacja przykładów do wykorzystania w Banku
3) Rozwiązanie problemów i odpowiedzi na pytania
4) Odpowiedzi na wątpliwości uczestników przez wykładowcę po szkoleniu

Warunki uczestnictwa i regulamin

> Warunki uczestnictwa
>
> po otrzymaniu zgłoszenia prześlemy potwierdzenie przyjęcia zgłoszenia, a na około 2 dni przed terminem szkolenia zostaną wysłane wiadomości organizacyjne wraz z linkiem do

szkolenia oraz materiałami szkoleniowymi. Płatności po szkoleniu, zwykle w tym samym dniu po szkoleniu prześlemy do Państwa faktury do zapłaty wraz z zaświadczeniem drogą mailową.

Regulamin

rezygnację przyjmujemy najpóźniej na 3 dni przed szkoleniem w formie pisemnej. Rezygnacja w późniejszym terminie wiąże się z koniecznością pokrycia kosztów w 100%. Nieobecność na szkoleniu nie zwalnia z dokonania opłaty. W przypadku braku możliwości wzięcia udziału w danym terminie jest możliwość przesłania nagrania ze szkolenia online.

Promocja

390 + VAT
za każdą kolejną osobę z firmy

490 + VAT | za osobę

NADCHODZĄCE TERMINY