SZCZEGÓŁY OFERTY

Testowanie odporności cyfrowej zgodnie z przepisami DORA oraz Rozp. 2024/1774, a także nową ankietą KRI IT

I. ADRESACI:

1. Członkowie Zarządu nadzorujący ryzyko ICT
2. Pracownicy pełniący obowiązki Administratora / Stanowiska ds. bezpieczeństwa / Komórki ds. ryzyka ICT
3. Pracownicy banku odpowiedzialni za ryzyko braku zgodności (compliance)
4. Pracownicy komórek ds. kontroli wewnętrznej

II. WYMAGANIA WSTĘPNE DLA UCZESTNIKÓW:

5. Ogólna znajomość przepisów w zakresie ochrony informacji, w tym DORA
6. Ogólna znajomość praktyki działania banku spółdzielczego

III. CEL SEMINARIUM:

1. Zrozumienie obowiązków wynikających z DORA i Rozporządzenia 2024/1774.
2. Poznanie metod testowania odporności cyfrowej proporcjonalnych do skali banku spółdzielczego.
3. Wyposażenie uczestników w wiedzę praktyczną o bezpieczeństwie fizycznym i środowiskowym jako filarze odporności operacyjnej

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 dostosowaniu do specyfiki działania danej instytucji.

Po szkoleniu otrzymujecie Państwo:

1. Program testowania odporności cyfrowej Zgodny z DORA
2. Roczny plan testowania odporności cyfrowej Zgodny z DORA
3. Plan audytu zewnętrznych dostawców usług Obejmujący wymagania DORA oraz pytania audytu wewnetrznego
3. Wzory scenariuszy testów odporności i wzory dokumentacji testów Zgodne z DORA
4. Plan PUCD i plany awaryjne Obejmujący wymagania DORA
5. Plan testowania PUCD i planów awaryjnych Obejmujący wymagania DORA oraz spójność z programem testowania odporności cyfrowej
6. Raport z realizacji programu testowania odporności cyfrowej Obejmujący wymagania DORA

Program szkolenia

1. Wprowadzenie do DORA i Rozp. 2024/1774, nowa ankieta KRI IT
1) Zakres przepisów DORA, a przepisy wykonawcze (RTS/ITS).
2) Rozporządzenie 2024/1774 – przepisy dotyczące ryzyka ICT, w tym bezpieczeństwa fizycznego i środowiskowego.
3) Powiązania z systemem ciągłości działania banku (BCP/DRP).
4) Nowa ankieta KRI IT – pytania o testowania odporności, w tym bezpieczeństwo fizyczne
2. Ramy testowania odporności cyfrowej w banku spółdzielczym
1) Program testowania odporności cyfrowej w Banku
2) Obowiązkowe rodzaje testów zgodnie z DORA (bez TLPT).
3) Współpraca z zewnętrznymi dostawcami ICT i outsourcerami.
3. Bezpieczeństwo fizyczne i środowiskowe wg 2024/1774
1) Bezpieczeństwo fizyczne i środowiskowe wg DORA i Rozp. 2024/1774
2) Wymogi dla budynków i pomieszczeń krytycznych (serwerownie, archiwa, centrale).
3) Kontrola dostępu fizycznego (strefy, monitoring, rejestry wejść).
4) Ochrona przed zagrożeniami środowiskowymi:
a) pożar (systemy detekcji i gaszenia),
b) powódź i zalania,
c) wahania temperatury i wilgotności,
d) dostępność energii (UPS, generatory).
5) Rola testów weryfikujących odporność fizyczną i środowiskową:
a) test procedury po awarii zasilania,
b) test reakcji na fałszywy alarm pożarowy
c) test reakcji na naruszenie polityki czystego biurka i ekranu
d) test wejścia przez osoby nieupoważnione
e) test ewakuacji.
4. Organizacja i dokumentowanie testów odporności cyfrowej
1) Jak opracować program testowania odporności cyfrowej i plany oraz scenariusze testów (uwzględniając ICT i aspekty fizyczno-środowiskowe)
2) Dokumentowanie przebiegu i wyników testów
3) Raportowanie do Zarządu i Rady Nadzorczej
5. Scenariusze praktyczne testów dla banku spółdzielczego
1) odtworzenie danych z backupu,
2) symulacja awarii zasilania w centrali,
3) test reakcji na incydent phishingowy,
4) test reakcji na poważny incydent i gotowość do zgłoszenia do KNF
5) test dostępu do serwerowni i innych stref (kontrola procedur wejścia).
5. Działania następcze i doskonalenie
1) Analiza wyników testów i tworzenie planów działań korygujących.
2) Utrwalanie kultury bezpieczeństwa.

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