Kluczowe Aspekty Cyberbezpieczeństwa w Bankach Spółdzielczych: Praktyczne Wdrożenie DORA i NIS2

SZKOLENIE ONLINE wykład na żywo
z możliwością zadawania pytań przez chat

Cel Szkolenia: Celem szkolenia jest wyposażenie uczestników w niezbędną wiedzę i umiejętności do skutecznego wdrożenia regulacji DORA (Digital Operational Resilience Act) i NIS2 (Network and Information Security Directive) w bankach spółdzielczych. Szkolenie koncentruje się na zrozumieniu wymagań dotyczących bezpieczeństwa cyfrowego, zarządzania ryzykiem oraz ochrony infrastruktury krytycznej, co jest kluczowe dla zapewnienia ciągłości działania i odporności operacyjnej.
Korzyści dla Uczestników:
• Dogłębne Zrozumienie Regulacji: Uczestnicy zdobędą wiedzę na temat wymagań DORA i NIS2 oraz ich praktycznego zastosowania w bankach spółdzielczych.
• Wzrost Odporności Cyfrowej: Szkolenie dostarczy narzędzi do skutecznego zarządzania ryzykiem cybernetycznym i zapewnienia ciągłości operacyjnej w obliczu zagrożeń cyfrowych.
• Skuteczne Zarządzanie Incydentami: Uczestnicy nauczą się, jak efektywnie zarządzać incydentami cyberbezpieczeństwa oraz testować odporność systemów.
• Praktyczne Podejście do Wdrożenia: Szkolenie pomoże w opracowaniu praktycznych strategii wdrożenia regulacji, w tym współpracy z dostawcami usług IT i partnerami zewnętrznymi.
• Podniesienie Kompetencji Zarządu: Uczestnicy dowiedzą się, jak skutecznie zarządzać ryzykiem na poziomie zarządu i przygotować organizację do audytów wewnętrznych oraz zewnętrznych.
• Zwiększenie Zgodności z Regulacjami: Szkolenie pomoże w opracowaniu strategii monitorowania zgodności z DORA i NIS2, minimalizując ryzyko sankcji i naruszeń.

PROGRAM:

Wprowadzenie do Szkolenia
1. Powitanie uczestników.
2. Omówienie celu szkolenia i kluczowych zagadnień.
3. Znaczenie DORA i NIS2 w bankach spółdzielczych.

Panel 1: Wymagania Prawne i Organizacyjne
1. Definicja cyberbezpieczeństwa w kontekście prawnym.
2. Przegląd kluczowych regulacji DORA i NIS2.
3. Obowiązki banków spółdzielczych wynikające z DORA i NIS2.
4. Omówienie zasady proporcjonalności w implementacji regulacji.
5. Organizacja i zarządzanie ryzykiem w systemach ICT.
6. Rola departamentu compliance w zarządzaniu ryzykiem.
7. Ramy zarządzania incydentami związanymi z ICT.
8. Audyty wewnętrzne i zewnętrzne w kontekście regulacji.

Panel 2: Zarządzanie Ryzykiem ICT i Odporność Operacyjna
1. Tworzenie ram zarządzania ryzykiem związanym z ICT.
2. Testowanie operacyjnej odporności cyfrowej: TLPT i inne narzędzia.
3. Zarządzanie incydentami – klasyfikacja, raportowanie i reagowanie.

4. Wymogi dotyczące zewnętrznych dostawców ICT.
5. Strategie reagowania na kryzysy i przywracania systemów.
6. Praktyczne przykłady implementacji w bankach spółdzielczych.
7. Rekomendacje dotyczące współpracy z dostawcami IT.
8. Wdrażanie planów ciągłości działania (BCP) z uwzględnieniem specyfiki sektora finansowego.

Panel 3: Praktyczne Wdrożenie DORA i NIS2
1. Harmonizacja przepisów i różnice między DORA a NIS2.
2. Wdrożenie polityk bezpieczeństwa w bankach spółdzielczych.
3. Zarządzanie ryzykiem cybernetycznym: narzędzia i praktyki stosowane w bankach.
4. Wdrażanie mechanizmów monitorowania bezpieczeństwa ICT.
5. Strategie skutecznej komunikacji z interesariuszami podczas incydentów.
6. Praktyczne aspekty przygotowania do audytów operacyjnych i zewnętrznych.
7. Kluczowe wskaźniki efektywności (KPI) i ich monitorowanie.
8. Case studies: sukcesy i wyzwania przy wdrożeniu DORA i NIS2.

• Otwarta dyskusja z uczestnikami.
• Wyjaśnienie wątpliwości.
• Podsumowanie i rekomendacje dla dalszych działań.

INFORMACJE ORGANIZACYJNE:

Szczegółowych informacji udziela:
Monika Cicha
tel.: 22 207 22 58
E-mail: biuro@crf.pl

Data i miejsce zajęć:
16 stycznia 2025 r. Online

Godziny zajęć: 10.00-13.30

Cena obejmuje: Uczestnictwo w wideoszkoleniu dla 1 osoby, możliwość zadawania pytań przez chat podczas szkolenia, autorskie materiały szkoleniowe przygotowane przez trenera, zaświadczenie

PROMOCJA:
Każda kolejna osoba z firmy 490zł +23 % VAT

Koszt szkolenia:
od jednej osoby - **590** zł + VAT*

* cena bez VAT dla opłacających szkolenie w co najmniej 70% ze środków publicznych

Płatności prosimy dokonać po otrzymaniu potwierdzenia na konto:
ING BANK ŚLĄSKI
70 1050 1025 1000 0097 0816 2640
Uprzejmie prosimy na przelewie umieścić temat, datę szkolenia oraz nazwiska uczestników.

Zgłoszenia prosimy nadsyłać mailem biuro@crf.pl lub faksem na nr 22 207 22 58.