kod szkolenia: DORA / PL DL 1d

Zapewnienie zgodności z DORA instytucji finansowej z wykorzystaniem Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO 27001

Co powinno być gotowe na 17 stycznia 2025 r.?

Jednodniowe szkolenie praktyczne dla instytucji finansowych, w trakcie którego zapoznamy uczestników z kluczowymi aspektami zapewnienia zgodności z wymaganiami Rozporządzenia DORA.

W obliczu nadchodzącego terminu obowiązywania Rozporządzenia (UE) 2022/2554 (DORA), instytucje finansowe stają przed wyzwaniem nie tylko dostosowania istniejących procesów ICT do nowych wymogów, ale także zintegrowania tych działań z istniejącym Systemem Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnym z ISO/IEC 27001:2022.

Udział w szkoleniu to inwestycja w zwiększenie zgodności regulacyjnej, odporności cyfrowej i dojrzałości operacyjnej organizacji.

Po ukończeniu szkolenia uczestnik będzie potrafił:

- interpretować kluczowe wymagania DORA i powiązać je z kontrolami ISO 27001,
- przeprowadzić analizę luk zgodności SZBI względem DORA,
- zidentyfikować brakujące mechanizmy nadzorcze i raportowe wymagane przez DORA,
- zaplanować działania dostosowujące SZBI do wymagań DORA w sposób zintegrowany,
- przygotować rejestr umów z dostawcami ICT i wymogi TLPT (threat-led penetration testing),

- opracować schematy audytów wewnętrznych w zakresie operacyjnej odporności cyfrowej.

DORA Compliance Checklist

Odbiorcy szkolenia

Szkolenie skierowane jest do osób zarówno bezpośrednio, jak i pośrednio odpowiedzialnych za:

- zgodność regulacyjną i audyt wewnętrzny w instytucjach finansowych,
- zarządzanie ryzykiem ICT i operacyjnym,
- bezpieczeństwo informacji i systemów informatycznych (CISO, ISO),
- projektowanie, wdrażanie i doskonalenie SZBI wg ISO 27001,
- przygotowanie organizacji do inspekcji KNF i raportowania zgodnie z DORA.

Szkolenie dostarcza zarówno wiedzy teoretycznej, jak i praktycznej, aby wspierać uczestników w dostosowaniu ich organizacji do wymagań regulacyjnych DORA w kontekście aktualnych standardów z zakresu cyberbezpieczeństwa.

Korzyści

Korzyści wynikające z ukończenia szkolenia:

1. Zrozumienie wymogów prawnych:
   - Poznanie Rozporządzenia DORA oraz powiązanych wytycznych KNF i EBA.
   - Jasne wskazówki, jak dostosować organizację do nowej regulacji.
2. Zdobycie praktycznej wiedzy nt. integracji DORA i ISO 27001.
3. Dostęp do szablonów analizy luk zgodności, rejestrów oraz przykładów dokumentacji (bazujących na materiałach NOREA, ENISA, UpGuard).
4. Zwiększenie gotowości do inspekcji KNF i wymagań raportowych EBA/EIOPA/ESMA,
5. Rozwój kompetencji w zakresie projektowania i wdrażania zgodności o operacyjnej odporności (compliance-by-design/ resilience-by-design).

Program szkolenia

1. Wprowadzenie do DORA:
   - Zakres podmiotowy i czasowy,
   - Kluczowe obowiązki: zarządzanie ryzykiem ICT, testowanie odporności, nadzór nad dostawcami ICT.
2. System Zarządzania Bezpieczeństwem Informacji wg ISO 27001:
   - Przegląd wymagań normy 27001:2022 (z uwzględnieniem Annex A),
   - Relacja SZBI do operacyjnej odporności cyfrowej.
3. Mapa zgodności DORA–ISO 27001:
   - Praktyczne porównanie wymagań (wg dokumentu „EU DORA to ISO 27001”),
   - Wskazanie luk i możliwości synergii.
4. Wdrażanie wymogów DORA w ramach SZBI:
   - Rejestr umów z dostawcami ICT, ocena ryzyka łańcucha dostaw,
   - Rejestry i dokumenty operacyjne wymagane przez DORA,
   - Program testów odporności, w tym TLPT,
   - Zasady audytu i przeglądów rocznych w ujęciu DORA.
5. Ćwiczenia i analiza przypadku:
   - Przeprowadzenie uproszczonej analizy luk zgodności DORA vs ISO 27001,
   - Opracowanie planu dostosowania organizacji.

Oczekiwane przygotowanie uczestnika

Aby w pełni skorzystać z treści i praktycznych ćwiczeń podczas szkolenia, uczestnicy powinni:

1. Mieć podstawową wiedzę o ICT – rozumieć podstawowe pojęcia z zakresu technologii informacyjno-komunikacyjnych i systemów ICT używanych w organizacji.
2. Znać strukturę organizacji i mieć ogólne pojęcie o funkcjonowaniu procesów w organizacji, zwłaszcza tych związanych z bezpieczeństwem ICT.
3. Mieć podstawową świadomość tematyki cyberbezpieczeństwa i operacyjnej odporności cyfrowej.
4. Znać ogólnie regulacje i wymogi prawne dotyczące cyberbezpieczeństwa w swojej branży (np. RODO, NIS2, KSC).
5. Być otwarci na nowe technologie, w tym korzystanie z cyfrowych narzędzi wykorzystywanych w trakcie szkolenia.
6. Mieć doświadczenie zawodowe w obszarze zarządzania zgodnością i ryzykiem, cyberbezpieczeństwa, audytu i kontroli wewnętrznej, ICT/IT (opcjonalne).

Uwaga: Szkolenie jest dostosowane również do osób bez zaawansowanego przygotowania technicznego, dzięki czemu może być wartościowe zarówno dla specjalistów, jak i menedżerów czy administratorów odpowiedzialnych za cyberbezpieczeństwo i cyfrową odporność operacyjną.

Szkolenie obejmuje

- Dzień pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty

Czas trwania

1 dni / 7 godzin

Język

- Szkolenie: polski
- Materiały: polski