kod szkolenia: DORA ICT / PL DL 1d

Zapewnienie zgodności z DORA przez dostawcę usług ICT - sektor finansowy z wykorzystaniem Systemu Zarządzania Bezpieczeństwem Informacji - ISO 27001

Co powinno być gotowe na 17 stycznia 2025 r.?

Jednodniowe szkolenie praktyczne dla dostawców usług ICT dla sektora finansowego, w trakcie którego zapoznamy uczestników z kluczowymi aspektami zapewnienia zgodności z wymaganiami Rozporządzenia DORA.

W związku z wejściem w życie Rozporządzenia (UE) 2022/2554 (DORA), dostawcy usług ICT dla sektora finansowego stają się kluczowym ogniwem w budowaniu cyfrowej odporności instytucji regulowanych. Nowe wymogi nakładają na dostawców obowiązek spełnienia szeregu wymagań dotyczących bezpieczeństwa informacji, przejrzystości operacyjnej, testowania odporności oraz gotowości audytowej – potwierdzonych umownie i w praktyce.

Szkolenie dostarcza uczestnikom narzędzi niezbędnych do interpretacji wymogów DORA, ich zintegrowania z systemem zarządzania bezpieczeństwem informacji (SZBI) zgodnym z ISO/IEC 27001:2022 oraz przygotowania organizacji na współpracę z instytucjami finansowymi w zgodności z wymaganiami regulacyjnymi i kontraktowymi.

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

Uczestnicy po szkoleniu będą potrafili:

- zinterpretować wymagania DORA wobec dostawców ICT (w tym obowiązki z art. 28–30) i powiązać je z wymaganiami i zabezpieczeniami ISO 27001,
- przeprowadzić analizę luk zgodności względem DORA, wykorzystując podejście mapowania na SZBI,
- przeanalizować swoją ofertę usługową pod kątem zgodności z wymaganiami instytucji finansowych objętych DORA oraz opracować niezbędne uzupełnienia techniczne i proceduralne,
- opracować dokumentację zgodną z DORA – w tym rejestry umów z podmiotami trzecimi, mechanizmy nadzoru, testowania odporności oraz raportowania incydentów,
- dostosować SZBI (wg ISO 27001) jako jako podstawę zgodności kontraktowej, potwierdzającą dojrzałość operacyjną i bezpieczeństwo świadczonych usług ICT,
- przygotować organizację na obowiązki wynikające z umów ICT zgodnych z DORA i aktami wykonawczymi RTS/ITS, takie jak: obowiązek udostępniania informacji audytorom klienta, gotowość do udziału w testach TLPT czy zarządzanie ryzykiem i zgodnością łańcucha podwykonawców.

DORA Compliance Checklist

Odbiorcy szkolenia

Szkolenie skierowane jest do dostawców ICT, w szczególności:

- dostawców usług ICT, w tym firm oferujących rozwiązania chmurowe, outsourcing IT, SaaS, zarządzanie infrastrukturą,
- operatorów usług zewnętrznych dla banków, zakładów ubezpieczeń, TFI, podmiotów płatniczych,
- osób odpowiedzialnych za zgodność, bezpieczeństwo informacji, ryzyko, jakość usług ICT, zarządzanie SLA/KPI, relacje z klientami z sektora finansowego (regulowanymi),
- właścicieli procesów, osób pełniących funkcje DPO, ISO, CISO, kierowników ds. ryzyka, compliance officerów, audytorów wewnętrznych,
- zespołów projektowych odpowiedzialnych za wdrażanie SZBI, umowy ICT i zapewnienie zgodności z DORA.

Korzyści

Korzyści wynikające z ukończenia szkolenia:

1. Kompleksowe zrozumienie obowiązków DORA i umiejętność ich powiązania z praktyką ISO 27001.
2. Jasne i praktyczne wskazówki, jak dostosować organizację do nowej regulacji poprzez integrację wymagań DORA z ISO 27001.
3. Gotowość do efektywnej współpracy z sektorem finansowym w zgodności z wymogami prawnymi i audytowymi.
4. Praktyczne narzędzia do analizy luk zgodności, budowy rejestrów oraz wdrażania mechanizmów nadzoru.
5. Wzmocnienie pozycji konkurencyjnej poprzez budowę zaufania i spełnienie wymagań kontraktowych klientów z sektora finansowego.

Program szkolenia

1. Wymagania Rozporządzenia DORA wobec dostawców usług ICT:
   - zdefiniowanie obowiązków dostawcy w relacji z instytucją finansową,
   - analiza art. 28–30 i ich konsekwencji operacyjnych,
   - wymogi z RTS/ITS oraz ich przełożenie na zapisy umowne i praktyki operacyjne.
2. System Zarządzania Bezpieczeństwem Informacji wg ISO 27001 jako narzędzie zgodności:
   - przegląd kluczowych komponentów ISO 27001 w kontekście DORA,
   - rola SZBI w zapewnieniu przejrzystości, nadzoru i odporności operacyjnej.
3. Mapowanie wymagań DORA na ISO 27001 – analiza luk i działania dostosowawcze:
   - wykorzystanie szablonów mapowania,
   - warsztat z identyfikacji braków i formułowania działań korygujących,
   - ustalenie priorytetów zgodności w kontekście zakresu świadczonych usług.
4. Dokumentacja, klauzule umowne, rejestry, testy odporności i gotowość audytowa:
   - wzorcowe procedury i mechanizmy nadzoru: incydenty, zmiany, ciągłość działania,
   - wzorcowe klauzule umowne, rejestr umów z dostawcami, w tym poddostawcami i procesorami,
   - przygotowanie do udziału w TLPT i wymagania klientów dotyczące testów zgodności.
5. Praktyka współpracy z instytucją finansową – case study i najczęstsze błędy:
   - Oczekiwania klientów regulowanych – jak wygląda audyt u dostawcy?
   - Weryfikacja zgodności usług i deklaracji bezpieczeństwa (DS, SLA, RTO/RPO).

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, wymogi prawne oraz standardy dotyczące cyberbezpieczeństwa (np. ISO 27001 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