RBR

DORA Compliance

Check lista w ramach #DORcompliance dla dostawców usług ICT:

Krok 1: Analiza zakresu i klasyfikacja

- Określenie czy firma kwalifikuje się jako dostawca krytycznych usług ICT
- Przeprowadzenie analizy świadczonych usług pod kątem ich krytyczności dla sektora finansowego
- Identyfikacja wszystkich podwykonawców w łańcuchu dostaw – ewidencja umów

Krok 2: Zarządzanie ryzykiem

- Wdrożenie kompleksowego systemu zarządzania ryzykiem
- Ustanowienie procesów identyfikacji i oceny zagrożeń
- Opracowanie strategii zarządzania ryzykiem

Krok 3: Dostosowanie umów

- Przegląd i aktualizacja wszystkich umów z podmiotami finansowymi
- Uwzględnienie wymogów DORA w zakresie poziomów usług (SLA)
- Wprowadzenie zapisów dotyczących audytów i kontroli

Krok 4: System raportowania incydentów

- Stworzenie procedur wykrywania i klasyfikacji incydentów
- Wdrożenie systemu szybkiego reagowania na incydenty
- Opracowanie procesu raportowania incydentów do klientów

Krok 5: Testy

Przygotowanie programu regularnych testów systemów

- Wdrożenie testów penetracyjnych
- Dokumentowanie wyników testów i działań naprawczych

Krok 6: Zarządzanie ciągłością działania

- Opracowanie planów ciągłości działania (BCP)
- Przygotowanie planów awaryjnych
- Regularne testowanie procedur odtworzeniowych

Krok 7: Bezpieczeństwo danych

- Wdrożenie mechanizmów ochrony danych
- Zapewnienie poufności, integralności i dostępności danych
- Ustanowienie kontroli dostępu i szyfrowania

Krok 8: Dokumentacja i rejestry

- Dokumentowanie procesów i procedur bezpieczeństwa
- Przygotowanie dokumentacji dla audytorów

Krok 9: Szkolenia i świadomość

- Przeprowadzenie szkoleń dla personelu
- Budowanie kultury cyberbezpieczeństwa
- Regularne aktualizowanie wiedzy zespołu

Krok 10: Program nadzoru

- Przygotowanie się na nadzór regulacyjny
- Ustanowienie procesów współpracy z organami nadzorczymi
- Zapewnienie transparentności działań