afine

digitally secure

TLPT DORA

Checklista gotowości

Kompletny przewodnik operacyjny dla podmiotów finansowych

Umów konsultację TLPT

Na podstawie DORA RTS 2025/1190 | TIBER-EU 2025

Wersja 1.0 | Marzec 2026

SPIS TREŚCI

Jak korzystać z tej checklisty

Dla kogo. Liderzy zespołów kontrolnych, CISO, szefowie compliance i wszyscy odpowiedzialni za zarządzanie ćwiczeniem TLPT w ramach DORA. Niezależnie od tego, czy przygotowujesz się do pierwszego powiadomienia, czy doskonalisz podejście w kolejnym cyklu - ta checklista obejmuje pełny cykl 12-18 miesięcy.

Jak z nią pracować. Checklista podąża za 8 fazami TLPT w kolejności. Realizuj kolejne moduły w miarę postępów. Odznaczaj punkty po ich wykonaniu. Niektóre moduły mogą się nakładać - zobacz harmonogram na następnej stronie.

Każdy punkt ma odniesienie regulacyjne. Tekst monospace po każdym punkcie wskazuje konkretny artykuł z DORA RTS 2025/1190, samego rozporządzenia DORA lub frameworku TIBER-EU 2025. Twój zespół prawny i compliance może zweryfikować każdy wymóg.

Priorytety wskazują wagę regulacyjną. Elementy CRITICAL to wymogi regulacyjne blokujące postęp. HIGH to zdecydowanie zalecane działania. MEDIUM to dobre praktyki.

Napisana przez red team. Wskazówki praktyczne w całym dokumencie opierają się na wieloletnim doświadczeniu w ofensywnym bezpieczeństwie i operacjach red team. Opisują, co w praktyce idzie nie tak i jak tego uniknąć.

☐	Checkbox = zadanie do wykonania
CRITICAL	Wymóg regulacyjny, bezwzględny
HIGH	Zdecydowanie zalecane, brak powoduje opóźnienia
MEDIUM	Dobra praktyka, poprawia jakość
WSKAZÓWKA RED TEAM	Wskazówka praktyczna zespołu red team AFINE

Przegląd cyklu TLPT

Czas trwania łącznie: 18-28 miesięcy z przygotowaniem przed powiadomieniem. Minimum po powiadomieniu: 14-16 miesięcy.

Indeks modułów

01 Czy podlegam obowiązkowi?
Weryfikacja progów i wyznaczenia z art. 26 DORA

02 Struktura zarządzania
Zespół kontrolny, protokoły poufności, mapowanie CIF

03 Wybór dostawców
Ocena i kontrakty z dostawcami TI i red team

04 Faza przygotowawcza
Karta projektu, specyfikacja zakresu, koordynacja transgraniczna

05 Rozpoznanie zagrożeń
Scenariusze zagrożeń i raport TTI do zatwierdzenia przez organ

06 Testy red team
Ponad 12 tygodni aktywnych testów na systemach produkcyjnych

07 Faza zamknięcia
Raportowanie, purple teaming, raport podsumowujący

08 Remediacja i atestacja
Złożenie planu remediacji i formalne zatwierdzenie

Kluczowe produkty na każdym etapie

Annex I: Karta projektu (3 miesiące)

Annex II: Specyfikacja zakresu (6 miesięcy)

Annex III: Raport ukierunkowanej analizy zagrożeń

Annex IV: Plan testów red team

Annex V: Raport z testów red team (T + 4 tygodnie)

Annex VI: Raport blue team (T + 10 tygodni)

Annex VII: Raport podsumowujący (A + 8 tygodni)

Annex VIII: Atestacja

Kluczowe pojęcia

Powiadomienie	Formalne pismo od właściwego organu nadzoru nakazujące przeprowadzenie TLPT. Dzień 0 - od tego momentu biegną terminy regulacyjne.
CTL	Lider zespołu kontrolnego - osoba na wysokim stanowisku zarządzająca TLPT wewnętrznie. Musi mieć uprawnienia do podejmowania decyzji bez ujawniania szczegółów.
CIF	Funkcja krytyczna lub istotna - funkcja biznesowa, której zakłócenie istotnie wpłynęłoby na wyniki finansowe (DORA art. 3(22)).
Dostawca TI	Dostawca analizy zagrożeń - zewnętrzna firma badająca realistyczne scenariusze ataków na potrzeby TLPT.
TM	Menedżer testów - przedstawiciel organu TLPT nadzorujący test, zatwierdzający zmiany zakresu i walidujący wyniki.
T, A	W terminach produktów: T = zakończenie testów red team, A = data atestacji.
BAU	Business As Usual - normalna działalność operacyjna w zakresie bezpieczeństwa, w odróżnieniu od prac związanych z TLPT.

01

Czy podlegam obowiązkowi?

Ustal, czy Twój podmiot podlega obowiązkowi TLPT na podstawie progów z art. 26 DORA, wyznaczenia uznaniowego lub możliwości wyłączenia.

Kluczowy termin: Zakończ przed formalnym powiadomieniem

SCOPE

Moduł 01: Czy podlegam obowiązkowi?

- [ ] Ustal typ podmiotu - czy jesteś jednym z 21 typów podmiotów finansowych zgodnie z art. 2 DORA?
  CRITICAL [DORA Art. 2(1)]

- [ ] Sprawdź obowiązkowe progi (art. 2 RTS): instytucje kredytowe G-SII/O-SII, instytucje płatnicze >150 mld EUR, CSD/CCP automatycznie w zakresie, ubezpieczyciele >1,5 mld EUR GWP
  CRITICAL [RTS Art. 2]

- [ ] Sprawdź wyznaczenie uznaniowe - nawet poniżej progów, Twój krajowy organ nadzoru może Cię wyznaczyć na podstawie wpływu, znaczenia systemowego, profilu ryzyka ICT lub wielkości
  HIGH [RTS Art. 2; DORA Art. 26(8)]

- [ ] Sprawdź możliwość wyłączenia - właściwe organy mogą wyłączyć podmioty z niskim profilem ryzyka ICT, nawet jeśli technicznie podlegają obowiązkowi
  HIGH [DORA Art. 26(8)]

WSKAZÓWKA RED TEAM

Nie czekaj na formalne powiadomienie. Jeśli zbliżasz się do progów, zacznij przygotowania teraz. 3-miesięczny termin inicjacji biegnie od dnia powiadomienia - a scoping bez wcześniejszych przygotowań szybko pochłania to okno czasowe.

WSKAZÓWKA RED TEAM

Podmioty regularnie zakładają, że są wyłączone, bo nie przekraczają jednego progu - a trzy miesiące później zostają wyznaczone uznaniowo. Jeśli Twój krajowy organ nadzoru sygnalizował zainteresowanie Twoim profilem ryzyka ICT - lub jeśli podmioty z Twojego sektora zostały wyznaczone - traktuj to jako sygnał startu.

02

Struktura zarządzania

Zbuduj infrastrukturę organizacyjną: zaangażowanie organu zarządzającego, formowanie zespołu kontrolnego, protokoły poufności i mapowanie funkcji krytycznych.

Kluczowy termin: Rozpocznij 6+ miesięcy przed spodziewanym powiadomieniem

TEAM

Moduł 02: Struktura zarządzania

2A: Przygotowanie organu zarządzającego

- [ ] Poinformuj zarząd/kierownictwo o obowiązkach TLPT i harmonogramie (12-18 miesięcy)
  HIGH [DORA Art. 26(1); RTS Art. 9(6)]
- [ ] Potwierdź dostępność organu zarządzającego do formalnego zatwierdzenia specyfikacji zakresu
  CRITICAL [RTS Art. 9(6)]
- [ ] Wyznacz osobę decyzyjną w zakresie budżetu - typowe koszty TLPT to 150-500 tys. EUR za samą analizę zagrożeń + red team
  HIGH [Best Practice]
- [ ] Ustal cykliczność raportowania postępów TLPT na poziomie zarządu
  MEDIUM [RTS Art. 4; RTS Art. 9(4)]

2B: Formowanie zespołu kontrolnego

- [ ] Wyznacz lidera zespołu kontrolnego (CTL) z wymaganymi uprawnieniami i dostępnością
  CRITICAL [RTS Art. 4; RTS Art. 9(4)]
  - [ ] Wysoka pozycja organizacyjna z bezpośrednim dostępem do zarządu [RTS Art. 4]
  - [ ] Uprawnienia do podejmowania wiążących decyzji bez ujawniania informacji innym zespołom [RTS Art. 4]
  - [ ] Dostępność do poświęcenia znacznej ilości czasu przez 12-18 miesięcy [Best Practice]
  - [ ] Znajomość zarówno operacji biznesowych, jak i systemów ICT [RTS Art. 9(4)]
- [ ] Zbuduj zespół kontrolny (zalecane 3-5 osób)
  HIGH [RTS Art. 9(4)]
  - [ ] CTL (obowiązkowy) [RTS Art. 4]
  - [ ] Przedstawiciel ryzyka/compliance [RTS Art. 9(4)]
  - [ ] Przedstawiciel ICT/infrastruktury [RTS Art. 9(4)]
  - [ ] Przedstawiciel operacji biznesowych [RTS Art. 9(4)]
  - [ ] Przedstawiciel prawny/zamówień (opcjonalnie) [Best Practice]
- [ ] Ustanów protokoły poufności
  HIGH [RTS Art. 4]
  - [ ] Szyfrowane kanały komunikacji (oddzielne od poczty korporacyjnej) [RTS Art. 4; RTS Art. 9(2)]
  - [ ] Bezpieczne repozytorium danych dla dokumentów TLPT [RTS Art. 4; RTS Art. 9(2)]
  - [ ] Kryptonim ćwiczenia [RTS Art. 4; RTS Art. 9(2)]
  - [ ] Legendy na potrzeby spotkań zespołu kontrolnego [RTS Art. 4]
  - [ ] Protokół ograniczania incydentu w przypadku wykrycia aktywności red team przez blue team [RTS Art. 4; RTS Art. 11(9)]

2C: Mapowanie funkcji krytycznych

- [ ] Zidentyfikuj WSZYSTKIE funkcje krytyczne lub istotne (CIF) zgodnie z art. 3(22) DORA
  CRITICAL [DORA Art. 3(22); DORA Art. 26(2)]

- [ ] Dla każdej CIF zmapuj wspierające systemy ICT, status outsourcingu, dane dostawców, jurysdykcje i powiązania
  CRITICAL [RTS Art. 9(6); RTS Annex II]
  - [ ] Wspierające systemy, procesy i technologie ICT [RTS Annex II]
  - [ ] Status outsourcingu (wewnętrznie vs. dostawca zewnętrzny) [RTS Annex II]
  - [ ] Nazwa dostawcy i odniesienie do umowy (jeśli outsourcowany) [RTS Annex II]
  - [ ] Jurysdykcje, w których funkcja działa [RTS Annex II]
  - [ ] Powiązania z innymi funkcjami/podmiotami [RTS Art. 9(7)]

- [ ] Zastosuj 7 kryteriów z art. 9(7) RTS do rankingu CIF
  CRITICAL [RTS Art. 9(7)]

- [ ] Przygotuj uzasadnienie dla każdej CIF wyłączonej z zakresu TLPT
  CRITICAL [RTS Art. 9(6); RTS Annex II]

- [ ] Zdefiniuj wstępne flagi dla każdej CIF w zakresie
  HIGH [RTS Annex II]
  - [ ] Co najmniej jedna dotycząca poufności [RTS Annex II; RTS Annex III]
  - [ ] Co najmniej jedna dotycząca integralności [RTS Annex II; RTS Annex III]
  - [ ] Co najmniej jedna dotycząca dostępności [RTS Annex II; RTS Annex III]

WSKAZÓWKA RED TEAM

Rola lidera zespołu kontrolnego to pełnoetatowa praca udająca dodatkowy obowiązek. Gdy CTL jednocześnie prowadzi codzienne operacje bezpieczeństwa, problemy z harmonogramem pojawiają się do trzeciego miesiąca. Jeśli Twój CTL nie może zablokować 60-70% kalendarza na czas trwania - wyznacz kogoś, kto może.

WSKAZÓWKA RED TEAM

Twoja legenda zostanie przetestowana. Gdy blue team wykryje aktywność red team i eskaluje do reakcji na incydent, zespół kontrolny ma około 30 minut na opanowanie sytuacji bez ujawnienia ćwiczenia. Przygotuj legendy z wyprzedzeniem i przetestuj je pod presją.

WSKAZÓWKA RED TEAM

Mapowanie funkcji krytycznych to najtrudniejszy element. Większość banków nie ma czystego mapowania między procesami biznesowymi a systemami ICT. Zacznij to 6+ miesięcy przed spodziewanym powiadomieniem. Instytucje regularnie zużywają całe 6-miesięczne okno na scoping, bo muszą budować to mapowanie od zera.

03

Wybór dostawców

Oceń, punktuj i zakontraktuj dostawców analizy zagrożeń i red team zgodnie z minimalnymi wymaganiami z art. 7 RTS i kryteriami operacyjnymi.

Kluczowy termin: Rozpocznij 4-6 miesięcy przed testami

VENDOR

Moduł 03: Wybór dostawców

3A: Dostawca analizy zagrożeń - wymagania minimalne

- [ ] Zewnętrzny wobec podmiotu finansowego (obowiązkowe - brak wewnętrznego TI dla TLPT)
  CRITICAL [DORA Art. 27(2); RTS Art. 1]
- [ ] Kierownik z minimum 5-letnim doświadczeniem w analizie zagrożeń
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] Dodatkowy członek/członkowie zespołu z minimum 2-letnim doświadczeniem
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] Minimum 3 referencje klientów z poprzednich zleceń TI
  CRITICAL [TIBER-EU Procurement]
- [ ] Ubezpieczenie odpowiedzialności zawodowej obejmujące uchybienia i niedbalstwo
  CRITICAL [DORA Art. 27(1)(e); RTS Art. 7(1)]
- [ ] Certyfikaty zgodne z uznanymi standardami rynkowymi
  HIGH [DORA Art. 27(1)(c); RTS Art. 7(1)]
- [ ] Brak konfliktu interesów z podmiotem lub zaangażowanymi dostawcami ICT
  CRITICAL [RTS Art. 7(1)]
- [ ] Niewykonywanie jednocześnie zadań blue team dla podmiotu
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] Oddzielenie od personelu red team (jeśli ta sama firma świadczy oba)
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]

3B: Dostawca red team - wymagania minimalne i kompetencje techniczne

- [ ] Lider testów z minimum 5-letnim doświadczeniem w testach penetracyjnych i red team
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] Co najmniej 2 dodatkowych członków zespołu z minimum 2-letnim doświadczeniem każdy
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]
- [ ] Minimalna wielkość zespołu: 3 osoby z odpowiednią zdolnością zastępstwa
  CRITICAL [TIBER-EU Procurement]
- [ ] Minimum 5 referencji klientów z poprzednich zleceń testów penetracyjnych/red team
  CRITICAL [TIBER-EU Procurement]
- [ ] Ubezpieczenie odpowiedzialności zawodowej obejmujące uchybienia i niedbalstwo
  CRITICAL [DORA Art. 27(1)(e); RTS Art. 7(1)]
- [ ] Certyfikaty zgodne z uznanymi standardami rynkowymi
  HIGH [DORA Art. 27(1)(c); RTS Art. 7(1)]
- [ ] Brak konfliktu interesów z podmiotem lub zaangażowanymi dostawcami ICT
  CRITICAL [RTS Art. 7(1)]

- [ ] Niewykonywanie jednocześnie zadań blue team dla podmiotu
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]

3B-TC: Ocena kompetencji technicznych (16 obszarów)

- [ ] Zbieranie informacji z otwartych źródeł (OSINT)
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Tworzenie exploitów
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Tworzenie dedykowanego złośliwego oprogramowania
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Eksploatacja oparta na Active Directory
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Testy bezpieczeństwa fizycznego
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Ataki oparte na HID
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Omijanie AV/EDR/NDR/XDR
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Omijanie zabezpieczeń poczty elektronicznej
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Omijanie secure web gateway
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Omijanie rozwiązań anti-phishing
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Testy penetracyjne Web/API/Mobile
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Testy mainframe (jeśli dotyczy)
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Testy penetracyjne Wi-Fi
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Inżynieria społeczna
  HIGH [TIBER-EU Procurement 4.2]
- [ ] Znajomość reakcji na incydenty
  MEDIUM [TIBER-EU Procurement 4.2]
- [ ] Tworzenie ofensywnych narzędzi bezpieczeństwa
  MEDIUM [TIBER-EU Procurement 4.2]

3C: Kluczowe elementy umowy

- [ ] Zdefiniuj warunki uruchomienia kill switch i ścieżkę eskalacji
  CRITICAL [RTS Art. 11(10); RTS Art. 5]
- [ ] Określ zasady przetwarzania danych: generowanie, przechowywanie, agregacja, raportowanie, niszczenie
  CRITICAL [DORA Art. 27(3); TIBER-EU Procurement]
- [ ] Zdefiniuj granice zakresu: co jest dozwolone vs. zabronione
  CRITICAL [RTS Art. 11(1); RTS Annex IV]
- [ ] Uwzględnij wymagania dot. ubezpieczenia odpowiedzialności zawodowej
  CRITICAL [DORA Art. 27(1)(e)]
- [ ] Określ tygodniowy cykl i format raportowania
  HIGH [RTS Art. 11(7)]
- [ ] Zdefiniuj proces leg-up i łańcuch zatwierdzeń
  HIGH [RTS Art. 11(8)]
- [ ] Ureguluj kwestie własności intelektualnej i poufności
  HIGH [DORA Art. 27(3)]
- [ ] Uwzględnij przepisy dot. dostępu regulatora (TM może żądać raportów)
  CRITICAL [RTS Art. 12(3)]
- [ ] Jeśli ta sama firma świadczy TI i RT: umowne oddzielenie zespołów
  CRITICAL [RTS Art. 7(1); TIBER-EU Procurement]

WSKAZÓWKA RED TEAM

Przy ocenie dostawców red team, certyfikaty mówią tylko część historii. OSCE, OSED, OSEP, OSWE i CRTO wskazują, że zespół potrafi działać poza standardowymi testami penetracyjnymi - tworzenie exploitów, omijanie EDR, pełne operacje red team. Publikacje CVE dopowiadają resztę: dostawca, który znajduje i odpowiedzialnie ujawnia podatności w oprogramowaniu korporacyjnym (SAP, CyberArk, IBM, F5), wykazuje głębię badawczą przekładającą się bezpośrednio na jakość TLPT.

WSKAZÓWKA RED TEAM

Rotacja dostawców brzmi prosto - dopóki nie spróbujesz. Twój poprzedni red team zna Twoje środowisko, luki w detekcji i procedury reakcji na incydenty. Nowy zespół zaczyna od zera. Zaplanuj dodatkowe 2-3 tygodnie w fazie TI na wdrożenie nowego dostawcy.

WSKAZÓWKA RED TEAM

Brak spójności między dostawcą TI a red team to jeden z najczęstszych problemów jakościowych w TLPT. TTIR opisuje aktorów zagrożeń w abstrakcyjnych kategoriach - red team potrzebuje konkretnych ścieżek ataku. Wymagaj wspólnej sesji roboczej TI i red team przed finalizacją TTIR.

Kryteria oceny dostawcy TI

#	Kryterium	Waga	Ocena (1-5)
E1	Głębokość analizy zagrożeń sektora finansowego	Wysoka (3)	
E2	Zdolności wywiadowcze (HUMINT, OSINT, dark web)	Wysoka (3)	
E3	Wcześniejsze doświadczenie TLPT/TIBER	Wysoka (3)	
E4	Zdolność analizy geopolitycznej i sektorowej	Średnia (2)	
E5	Zdolności językowe dla badań inżynierii społecznej	Średnia (2)	
E6	Metodologia profilowania aktorów zagrożeń	Wysoka (3)	
E7	Jakość opracowania scenariuszy	Wysoka (3)	
E8	Jakość komunikacji	Średnia (2)	
E9	Protokoły przetwarzania i niszczenia danych	Średnia (2)	
E10	Dostępność i responsywność	Średnia (2)	
E11	Jakość raportów i wykonalność rekomendacji	Wysoka (3)	
E12	Stabilność zespołu i zdolność zastępstwa	Średnia (2)	
E13	Dostęp do własnych źródeł wywiadowczych	Średnia (2)	
E14	Historia współpracy z zespołami red team	Wysoka (3)	
	WAŻONY WYNIK (Maks.: 175)		

Sposób użycia. Oceń każde kryterium od 1 (słabe) do 5 (doskonałe). Pomnóż każdą ocenę przez wagę w nawiasie, następnie zsumuj wszystkie ważone wyniki. Maksimum: 175. Suma oblicza się automatycznie po wpisaniu ocen.

- 0 — Nie oceniony
- 1 - 87 — Nie angażować - krytyczne luki kompetencyjne
- 88 - 121 — Poniżej progu - konieczne znaczne usprawnienia
- 122 - 148 — Spełnia wymagania - akceptowalny kandydat
- 149 - 175 — Silny kandydat - przekracza wymagania

Kryteria oceny dostawcy red team

#	Kryterium	Waga	Ocena (1-5)
E1	Historia publikacji CVE	Wysoka (3)	
E2	Wcześniejsze doświadczenie TLPT/TIBER	Wysoka (3)	
E3	Doświadczenie w sektorze finansowym	Wysoka (3)	
E4	Doświadczenie w testach na systemach produkcyjnych	Wysoka (3)	
E5	Dojrzałość bezpieczeństwa operacyjnego	Wysoka (3)	
E6	Procedury kill switch i zatrzymania	Wysoka (3)	
E7	Zdolność omijania AV/EDR/XDR	Wysoka (3)	
E8	Metodologia inżynierii społecznej	Średnia (2)	
E9	Zdolność testów bezpieczeństwa fizycznego	Średnia (2)	
E10	Jakość raportów i głębokość ustaleń	Wysoka (3)	
E11	Jakość komunikacji i raportowania tygodniowego	Średnia (2)	
E12	Głębokość zespołu i zdolność zastępstwa	Średnia (2)	
E13	ISO 27001 lub równoważny SZBI	Średnia (2)	
E14	Dedykowane narzędzia i infrastruktura C2	Wysoka (3)	
E15	Współpraca z dostawcami TI	Średnia (2)	
E16	Rotacja dostawców	Niska (1)	
E17	Doświadczenie w procesie leg-up	Średnia (2)	
	WAŻONY WYNIK (Maks.: 210)		

Sposób użycia. Oceń każde kryterium od 1 (słabe) do 5 (doskonałe). Pomnóż każdą ocenę przez wagę w nawiasie, następnie zsumuj wszystkie ważone wyniki. Maksimum: 210. Suma oblicza się automatycznie po wpisaniu ocen.

0	Nie oceniony
1 - 104	Nie angażować - krytyczne luki kompetencyjne
105 - 146	Poniżej progu - konieczne znaczne usprawnienia
147 - 177	Spełnia wymagania - akceptowalny kandydat
178 - 210	Silny kandydat - przekracza wymagania

04

Faza przygotowawcza

Złóż kartę projektu i specyfikację zakresu do organu TLPT, skoordynuj działania z dostawcami zewnętrznymi i uzgodnij warunki transgraniczne.

Kluczowy termin: Miesiące 0-6 po powiadomieniu

PLAN

Moduł 04: Faza przygotowawcza

4A: Inicjacja (w ciągu 3 miesięcy od powiadomienia)

- [ ] Imię i nazwisko oraz dane kontaktowe lidera zespołu kontrolnego
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Decyzja o typie testerów: wewnętrzni / zewnętrzni / hybrydowi
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Kanały komunikacji: szyfrowanie poczty, repozytorium danych, komunikatory
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Kryptonim TLPT
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Funkcje krytyczne w innych państwach członkowskich (lista + jurysdykcje)
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Funkcje krytyczne wspierane przez zewnętrznych dostawców ICT
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Planowane terminy zakończenia poszczególnych faz
  CRITICAL [RTS Art. 9(2); RTS Annex I]
- [ ] Ustanów szyfrowane kanały komunikacji z organem TLPT
  CRITICAL [RTS Art. 9(2); RTS Art. 4]
- [ ] Uruchom bezpieczne repozytorium danych
  HIGH [RTS Art. 4]
- [ ] Potwierdź, że organ TLPT zwalidował informacje inicjujące
  CRITICAL [RTS Art. 9(3)]
- [ ] Potwierdź, że organ TLPT zwalidował skład zespołu kontrolnego
  CRITICAL [RTS Art. 9(5)]

4B: Specyfikacja zakresu (w ciągu 6 miesięcy od powiadomienia)

- [ ] Wymień WSZYSTKIE zidentyfikowane funkcje krytyczne/istotne
  CRITICAL [RTS Art. 9(6); RTS Annex II]
- [ ] Dla każdej wyłączonej CIF: udokumentowane uzasadnienie
  CRITICAL [RTS Art. 9(6); RTS Annex II]
- [ ] Dla każdej włączonej CIF: uzasadnienie, systemy ICT, status outsourcingu, jurysdykcje, flagi
  CRITICAL [RTS Art. 9(6); RTS Annex II]
  - [ ] Uzasadnienie włączenia [RTS Annex II]
  - [ ] Zidentyfikowane wspierające systemy ICT [RTS Annex II]
  - [ ] Status outsourcingu i identyfikacja dostawcy [RTS Annex II]
  - [ ] Jurysdykcje operacyjne [RTS Annex II]
  - [ ] Wstępne flagi (poufność, integralność, dostępność) [RTS Annex II]

- [ ] Uzyskano formalne zatwierdzenie organu zarządzającego
  CRITICAL [RTS Art. 9(6)]

- [ ] Specyfikacja zakresu złożona do organu TLPT
  CRITICAL [RTS Art. 9(6)]

- [ ] Otrzymano zatwierdzenie organu TLPT
  CRITICAL [RTS Art. 9(12)]

4C: Ocena ryzyka (przed rozpoczęciem testów)

- [ ] Ocena ryzyka ICT samego TLPT (art. 5 RTS)
  CRITICAL [RTS Art. 5]

- [ ] Uwzględnij ryzyka: dostęp do wrażliwych danych, zgodność regulacyjna, eskalacja incydentów, zakłócenia produkcyjne, ingerencja blue team, niekompletne przywrócenie
  HIGH [RTS Art. 5]

- [ ] Dla łączonych/wspólnych TLPT: dodatkowa wielopodmiotowa ocena ryzyka
  CRITICAL [RTS Art. 6]

- [ ] Skonsultuj ocenę ryzyka z menedżerami testów przed rozpoczęciem testowania
  HIGH [RTS Art. 9(10)]

4D: Koordynacja z dostawcami zewnętrznymi

- [ ] Zidentyfikuj wszystkich zewnętrznych dostawców ICT wspierających CIF w zakresie
  CRITICAL [DORA Art. 26(2); RTS Annex II]

- [ ] Przejrzyj umowy pod kątem klauzul współpracy z art. 30(3)(d) DORA
  CRITICAL [DORA Art. 30(3)(d)]

- [ ] Aneksuj umowy, jeśli brakuje klauzul współpracy
  CRITICAL [DORA Art. 30(3)(d)]

- [ ] Uzgodnij warunki dostępu z dostawcami
  HIGH [DORA Art. 26(3)]

- [ ] Uzgodnij środki zarządzania ryzykiem z dostawcami
  HIGH [DORA Art. 26(5)]

- [ ] Dla testowania łączonego: skoordynuj z innymi podmiotami finansowymi
  HIGH [DORA Art. 26(4); RTS Art. 8]

- [ ] Potwierdź udział dostawcy na piśmie
  HIGH [DORA Art. 26(3)]

4E: Koordynacja transgraniczna (jeśli dotyczy)

- [ ] Zidentyfikuj wszystkie państwa członkowskie, w których działają CIF w zakresie
  CRITICAL [RTS Art. 16(1)]

- [ ] Organ TLPT powiadamia organy przyjmujących państw członkowskich
  CRITICAL [RTS Art. 16(1)]
- [ ] Organy przyjmujące odpowiadają w ciągu 20 dni roboczych
  HIGH [RTS Art. 16(1)]
- [ ] Uzgodnij wiodący organ TLPT
  CRITICAL [RTS Art. 16(1)]
- [ ] Wynegocjuj warunki wzajemnego uznawania PRZED rozpoczęciem testów
  CRITICAL [DORA Art. 26(7); RTS Art. 16]
- [ ] Dla podmiotów grupowych: oceń, czy wspólny TLPT jest odpowiedni
  HIGH [RTS Art. 16(2)]

WSKAZÓWKA RED TEAM

Koordynacja ze stronami trzecimi to ukryte wąskie gardło czasowe. Dostawcy chmury i dostawcy core bankingowi działają wolno. Rozpocznij negocjacje kontraktowe w momencie, gdy dowiesz się, że będą w zakresie. Sam ten punkt potrafi opóźnić TLPT o 3+ miesiące.

WSKAZÓWKA RED TEAM

Aneks do umowy z zewnętrznym dostawcą ICT - to miejsce, gdzie TLPT umierają. Dostawcy core bankingowi i dostawcy chmury mają własne zespoły prawne, własny apetyt na ryzyko i własne harmonogramy. Zacznij tego dnia, w którym dowiesz się, że dostawca jest w zakresie.

WSKAZÓWKA RED TEAM

Brak zabezpieczenia porozumień o wzajemnym uznawaniu przed startem oznacza, że możesz skończyć prowadząc oddzielne testy w każdej jurysdykcji. Uporządkuj to w fazie przygotowawczej, nie po.

WSKAZÓWKA RED TEAM

Transgraniczne wzajemne uznawanie nie jest automatyczne nawet z atestacją DORA. Każdy organ przyjmujący ma 20 dni roboczych na decyzję, czy chce obserwować, czy uczestniczyć. Jeśli działasz w trzech państwach członkowskich, zakładaj trzy zestawy oczekiwań regulacyjnych do zarządzania.

Kluczowe ryzyka TLPT (wstępny rejestr)

10 najważniejszych ryzyk z pełnego rejestru 24 ryzyk. Art. 5 RTS wymaga oceny ryzyka ICT samego TLPT.

ID	Ryzyko	Kategoria	L	I	Wynik	Poziom
R-01	Zakłócenie systemów produkcyjnych przez narzędzia red team	Operacyjne	3	5	15	High
R-02	Rezydualne artefakty red team po testach	Operacyjne	4	4	16	**Critical**
R-04	Nieautoryzowany dostęp do danych osobowych/klientów	Poufność	4	4	16	**Critical**
R-06	Wyciek dokumentacji TLPT	Poufność	2	5	10	High
R-08	Testy wykraczają poza zakres umowy z dostawcą	Zgodność	3	5	15	High
R-10	Blue team eskaluje do pełnej reakcji na incydent	Reputacyjne	4	4	16	**Critical**
R-13	Dostawca ICT odmawia udziału w TLPT	Strony trzecie	4	4	16	**Critical**
R-17	Niekompletne mapowanie CIF	Zakres	4	4	16	**Critical**
R-20	Naruszenie poufności zespołu kontrolnego	Personel	4	4	16	**Critical**
R-22	Blue team blokuje całą infrastrukturę C2/phishing	Techniczne	3	3	9	Medium

05

Rozpoznanie zagrożeń

Dostawca TI gromadzi informacje, opracowuje scenariusze zagrożeń i dostarcza raport ukierunkowanej analizy zagrożeń do zatwierdzenia przez organ TLPT.

Kluczowy termin: 4-6 tygodni po zatwierdzeniu zakresu

INTEL

Moduł 05: Rozpoznanie zagrożeń

5A: Gromadzenie informacji o zagrożeniach

- [ ] Dostawca TI analizuje ogólne i sektorowe informacje o zagrożeniach
  CRITICAL [RTS Art. 10(1)]
- [ ] Dostawca TI identyfikuje istotne cyberzagrożenia i podatności
  CRITICAL [RTS Art. 10(1)]
- [ ] Dostawca TI gromadzi skontekstualizowane informacje o celu
  CRITICAL [RTS Art. 10(1); RTS Annex III]
  - [ ] Dane uwierzytelniające pracowników z wycieków [RTS Annex III]
  - [ ] Domeny imitujące (lookalike) [RTS Annex III]
  - [ ] Wyeksponowane podatne oprogramowanie/systemy [RTS Annex III]
  - [ ] Informacje o pracownikach możliwe do wykorzystania w inżynierii społecznej [RTS Annex III]
  - [ ] Sprzedaż danych w dark web [RTS Annex III]
  - [ ] Informacje z internetu/sieci publicznych [RTS Annex III]
  - [ ] Informacje do targetowania fizycznego [RTS Annex III]
- [ ] Dostawca TI identyfikuje profile aktorów zagrożeń najbardziej prawdopodobnych dla podmiotu
  CRITICAL [RTS Art. 10(2); RTS Annex III]

5B: Opracowanie scenariuszy

- [ ] Dostawca TI opracowuje szeroki zestaw kandydujących scenariuszy
  CRITICAL [RTS Art. 10(2)]
- [ ] Spotkanie selekcji scenariuszy odbyło się (CTL + dostawca TI + menedżerowie testów)
  CRITICAL [RTS Art. 10(3)]
- [ ] CTL wybiera minimum 3 scenariusze na podstawie rekomendacji TI, opinii TM, wykonalności i profilu podmiotu
  CRITICAL [RTS Art. 10(3)]
- [ ] Wybrane scenariusze obejmują różnych aktorów zagrożeń i TTPs
  CRITICAL [RTS Art. 10(2)]
- [ ] Każdy scenariusz celuje w inne funkcje krytyczne
  CRITICAL [RTS Art. 10(2)]
- [ ] Obowiązkowe pokrycie: co najmniej jeden scenariusz celujący w dostępność, jeden w integralność, jeden w poufność
  CRITICAL [RTS Art. 10(4); RTS Annex III]
- [ ] Maksymalnie 1 scenariusz może nie być oparty na zagrożeniach (scenariusz-X)
  HIGH [RTS Art. 10(4)]
- [ ] Dla łączonych TLPT: co najmniej 1 scenariusz celuje w systemy dostawcy zewnętrznego
  CRITICAL [RTS Art. 10(4)]

- [ ] Dla wspólnych TLPT: co najmniej 1 scenariusz celuje w systemy wewnątrzgrupowe
  CRITICAL [RTS Art. 10(4)]

5C: Raport ukierunkowanej analizy zagrożeń (TTIR)

- [ ] Dostawca TI dostarcza TTIR zgodnie z Annex III: zakres, ocena informacji, krajobraz zagrożeń, profile aktorów, min. 3 scenariusze
  CRITICAL [RTS Art. 10(5); RTS Annex III]
- [ ] Zespół kontrolny przegląda i przekazuje TTIR menedżerom testów
  CRITICAL [RTS Art. 10(6)]
- [ ] Organ TLPT zatwierdza TTIR
  CRITICAL [RTS Art. 10(6)]
- [ ] Zatwierdzony TTIR udostępniony red team
  CRITICAL [RTS Art. 9(8)]

WSKAZÓWKA RED TEAM

Ogólna analiza zagrożeń daje ogólne testy. Jeśli Twój TTIR czyta się tak, jakby mógł dotyczyć dowolnego banku w Europie, wyprodukuje scenariusze testujące Twoją bramkę e-mail i nic więcej. Nalegaj, by dostawca TI poszedł w głąb TWOJEGO stosu technologicznego, TWOJEJ geografii, TWOJEGO modelu biznesowego.

WSKAZÓWKA RED TEAM

Selekcja scenariuszy to moment, gdy wychodzą błędy w scopingu. Częsty błąd to zatwierdzenie trzech scenariuszy celujących w tę samą funkcję krytyczną z różnych kątów. Zmapuj scenariusze do CIF explicite przed zatwierdzeniem.

06

Testy red team

Realizuj plan testów red team przez minimum 12 tygodni aktywnych testów, zarządzając leg-upami, zdarzeniami wykrycia i ryzykiem operacyjnym w czasie rzeczywistym.

Kluczowy termin: Minimum 12 tygodni aktywnych testów

ATTACK

Moduł 06: Testy red team

6A: Plan testów red team

- [ ] Testerzy przygotowują plan testów red team (Annex IV) obejmujący komunikację, TTPs, środki zarządzania ryzykiem, szczegóły per scenariusz, ścieżki ataku, leg-upy, harmonogram, uwagi o infrastrukturze
  CRITICAL [RTS Art. 11(1); RTS Annex IV]
- [ ] Zespół kontrolny przegląda i zatwierdza plan
  CRITICAL [RTS Art. 11(3)]
- [ ] Organ TLPT zatwierdza plan
  CRITICAL [RTS Art. 11(3)]

6B: Realizacja aktywnych testów

- [ ] Rozpoczęcie aktywnych testów red team
  CRITICAL [RTS Art. 11(4)]
- [ ] Czas trwania minimum 12 tygodni (proporcjonalnie do zakresu i złożoności)
  CRITICAL [RTS Art. 11(5)]
- [ ] Scenariusze realizowane sekwencyjnie lub równolegle zgodnie z planem
  HIGH [RTS Art. 11(5)]
- [ ] Testerzy dostarczają minimum cotygodniowe raporty postępu zespołowi kontrolnemu i menedżerom testów
  CRITICAL [RTS Art. 11(7)]
- [ ] Dostawca TI pozostaje dostępny do konsultacji przez cały czas
  HIGH [RTS Art. 11(7)]
- [ ] Wszystkie działania testerów logowane
  CRITICAL [TIBER-EU Section 5.2]

6C: Zarządzanie operacyjne w trakcie testów

- [ ] Zespół kontrolny monitoruje postęp w odniesieniu do planu
  HIGH [RTS Art. 4; RTS Art. 11(6)]
- [ ] Leg-upy udzielane w miarę potrzeb: każdy udokumentowany kodem, typem, przyczyną; zatwierdzony przez CTL i TM
  CRITICAL [RTS Art. 11(8)]
- [ ] W przypadku wykrycia aktywności przez blue team: CTL proponuje środki kontynuacji do TM
  HIGH [RTS Art. 11(9)]
- [ ] Wszelkie zmiany planu wymagają zatwierdzenia CTL i TM
  CRITICAL [RTS Art. 11(6)]
- [ ] CTL może zawiesić TLPT w przypadku ryzyka dla danych, zasobów lub usług
  CRITICAL [RTS Art. 11(10)]

- [ ] Ograniczony purple teaming jako ostateczność (wlicza się do 12-tygodniowego minimum)
  HIGH [RTS Art. 11(10)]

- [ ] Walidacja TM wymagana dla ograniczonego purple teamingu
  CRITICAL [RTS Art. 11(10)]

WSKAZÓWKA RED TEAM

Zdefiniuj proces leg-up przed pierwszym dniem aktywnych testów, nie gdy red team utknie w czwartym tygodniu. Uzgodnij z góry kategorie, kto je zatwierdza, maksymalny czas odpowiedzi (48 godzin to rozsądny cel) i jaką dokumentację trzeba przygotować.

WSKAZÓWKA RED TEAM

12-tygodniowe minimum jest realne. Próby skrócenia tego terminu konsekwentnie się nie udają - regulatorzy się sprzeciwiają. Zaplanuj budżet na 12-16 tygodni aktywnych testów.

WSKAZÓWKA RED TEAM

Paraliż decyzyjny przy kill switch to realne zjawisko. Wyznacz z góry dokładnie jedną osobę z uprawnieniami do natychmiastowego zatrzymania testu i jedną osobę (inną) z uprawnieniami do wznowienia. Obie powinny być dostępne 24/7 w trakcie aktywnych testów.

07

Faza zamknięcia

Powiadomienie blue team, raportowanie red team i blue team, obowiązkowy purple teaming, informacja zwrotna 360 stopni i złożenie raportu podsumowującego.

Kluczowy termin: Do 18 tygodni po testach

REPORT

Moduł 07: Faza zamknięcia

7A: Powiadomienie blue team

- [ ] Zakończenie aktywnych testów (za zgodą wszystkich stron)
  CRITICAL [RTS Art. 11(5)]
- [ ] Lider zespołu kontrolnego informuje blue team o przeprowadzeniu TLPT
  CRITICAL [RTS Art. 12(1)]
- [ ] Blue team otrzymuje raport z testów red team (może być oczyszczony z informacji wrażliwych)
  HIGH [RTS Art. 12(3)]

7B: Raportowanie (ścisłe terminy)

- [ ] Raport z testów red team (Annex V) - w ciągu 4 tygodni od zakończenia aktywnych testów
  CRITICAL [RTS Art. 12(2)]
  - [ ] Celowane CIF i wspierające systemy [RTS Annex V(a)]
  - [ ] Podsumowanie per scenariusz [RTS Annex V(a)]
  - [ ] Osiągnięte i nieosiągnięte flagi [RTS Annex V(a)]
  - [ ] Skuteczne i nieskuteczne ścieżki ataku i TTPs [RTS Annex V(a)]
  - [ ] Odchylenia od planu (jeśli wystąpiły) [RTS Annex V(a)]
  - [ ] Przyznane leg-upy (jeśli wystąpiły) [RTS Annex V(a)]
  - [ ] Działania blue team wykryte przez testerów [RTS Annex V(b)]
  - [ ] Opisy podatności z oceną krytyczności [RTS Annex V(c)]
  - [ ] Analiza przyczyn źródłowych udanych ataków [RTS Annex V(c)]
  - [ ] Rekomendacje remediacyjne z priorytetyzacją [RTS Annex V(c)]
- [ ] Raport red team przekazany zespołowi kontrolnemu i menedżerom testów
  CRITICAL [RTS Art. 12(2); RTS Art. 12(3)]
- [ ] Raport blue team (Annex VI) - w ciągu 10 tygodni od zakończenia aktywnych testów
  CRITICAL [RTS Art. 12(4)]
  - [ ] Dla każdego kroku ataku: wykryte działania i odpowiadające wpisy w logach [RTS Annex VI]
  - [ ] Ocena ustaleń i rekomendacji testerów [RTS Annex VI]
  - [ ] Dowody ataku zebrane przez blue team [RTS Annex VI]
  - [ ] Analiza przyczyn źródłowych blue team [RTS Annex VI]
  - [ ] Wnioski i potencjał do doskonalenia [RTS Annex VI]
  - [ ] Lista tematów purple teamingu [RTS Annex VI]
- [ ] Raport blue team przekazany testerom i menedżerom testów
  CRITICAL [RTS Art. 12(4)]

7C: Purple teaming (obowiązkowy)

- [ ] Ćwiczenie powtórzeniowe: blue i red team przechodzą przez działania ataku i obrony
  CRITICAL [RTS Art. 12(5)]
- [ ] Purple teaming na wspólnie zidentyfikowanych tematach
  CRITICAL [RTS Art. 12(5); TIBER-EU PT Guidance]
  - [ ] Dyskusja tabelaryczna alternatywnych scenariuszy [TIBER-EU PT Guidance]
  - [ ] Ponowna eksploracja scenariuszy ataku na systemach produkcyjnych [TIBER-EU PT Guidance]
  - [ ] Eksploracja alternatywnych scenariuszy na systemach produkcyjnych [TIBER-EU PT Guidance]
  - [ ] Opracowanie proof-of-concept dla nieprzetestowanych wektorów [TIBER-EU PT Guidance]
  - [ ] Dyskusja nad przewidywanymi działaniami naprawczymi [TIBER-EU PT Guidance]
  - [ ] Scenariusze ćwiczeń ciągłości działania [TIBER-EU PT Guidance]
- [ ] Wszystkie strony wymieniają się informacją zwrotną
  CRITICAL [RTS Art. 12(6)]
- [ ] Menedżerowie testów mogą przekazać informację zwrotną
  MEDIUM [RTS Art. 12(6)]
- [ ] Przeprowadzono sesję informacji zwrotnej 360 stopni
  HIGH [RTS Art. 12(6); TIBER-EU Section 6.3]

7D: Raport podsumowujący (Annex VII)

- [ ] Udokumentowane strony zaangażowane
  CRITICAL [RTS Art. 12(7); RTS Annex VII(a)]
- [ ] Udokumentowany plan projektu
  CRITICAL [RTS Annex VII(b)]
- [ ] Zwalidowany zakres z uzasadnieniem CIF
  CRITICAL [RTS Annex VII(c)]
- [ ] Wybrane scenariusze i odchylenia od TTIR
  CRITICAL [RTS Annex VII(d)]
- [ ] Zrealizowane ścieżki ataku i zastosowane TTPs
  CRITICAL [RTS Annex VII(e)]
- [ ] Przechwycone i nieprzechwycone flagi
  CRITICAL [RTS Annex VII(f)]
- [ ] Odchylenia od planu testów red team (jeśli wystąpiły)
  CRITICAL [RTS Annex VII(g)]
- [ ] Detekcje blue team
  CRITICAL [RTS Annex VII(h)]
- [ ] Purple teaming przeprowadzony (jeśli w trakcie fazy testowej)
  CRITICAL [RTS Annex VII(i)]

- [ ] Udokumentowane leg-upy
  CRITICAL [RTS Annex VII(j)]
- [ ] Podjęte środki zarządzania ryzykiem
  CRITICAL [RTS Annex VII(k)]
- [ ] Podatności z oceną krytyczności
  CRITICAL [RTS Annex VII(l)]
- [ ] Analiza przyczyn źródłowych udanych ataków
  CRITICAL [RTS Annex VII(m)]
- [ ] Ogólny plan remediacji
  CRITICAL [RTS Annex VII(n)]
- [ ] Wnioski z informacji zwrotnej
  HIGH [RTS Annex VII(o)]
- [ ] Złożone do organu TLPT
  CRITICAL [RTS Art. 12(7); DORA Art. 26(6)]

WSKAZÓWKA RED TEAM

Sposób, w jaki poinformujesz blue team, nadaje ton wszystkiemu, co nastąpi. Przedstaw ustalenia jako 'oto co atakujący z zasobami państwowymi osiągnął przeciwko Waszej obronie' - nie 'oto co przeoczyliście'. Współpraca blue team decyduje, czy remediacja adresuje przyczyny źródłowe, czy łata objawy.

WSKAZÓWKA RED TEAM

Purple teaming to miejsce, gdzie jest prawdziwa wartość. Operacja red team ujawnia luki - ale purple teaming transferuje wiedzę do Twoich obrońców.

WSKAZÓWKA RED TEAM

Purple teaming to nie debrief ze slajdami. To praktyczne ćwiczenie techniczne. Najskuteczniejsze sesje polegają na tym, że blue team siedzi z red team i odtwarza ścieżki ataku w czasie rzeczywistym. Jeśli Twój plan to dwugodzinne spotkanie z PowerPointem, zostawiasz 80% wartości na stole.

08

Remediacja i atestacja

Udokumentuj działania naprawcze dla każdego ustalenia, złóż dokumentację do organu TLPT i uzyskaj formalną atestację potwierdzającą zgodność z DORA.

Kluczowy termin: 8 tygodni po złożeniu raportu podsumowującego

ATTEST

Moduł 08: Remediacja i atestacja

8A: Plan remediacji (w ciągu 8 tygodni od powiadomienia o TSR)

- [ ] Dla KAŻDEGO ustalenia udokumentuj wszystkie wymagane pola
  CRITICAL [RTS Art. 13(2)]
  - [ ] Opis uchybienia [RTS Art. 13(2)(a)]
  - [ ] Proponowane działania naprawcze z priorytetyzacją [RTS Art. 13(2)(b)]
  - [ ] Harmonogram realizacji i kamienie milowe [RTS Art. 13(2)(b)]
  - [ ] Analiza przyczyn źródłowych [RTS Art. 13(2)(c)]
  - [ ] Odpowiedzialne osoby/funkcje [RTS Art. 13(2)(d)]
  - [ ] Ocena ryzyka w przypadku BRAKU remediacji [RTS Art. 13(2)(e)]
  - [ ] Ocena ryzyka samego wdrożenia remediacji [RTS Art. 13(2)(e)]
- [ ] Plan remediacji złożony do organu TLPT ORAZ właściwego organu nadzoru (jeśli inny)
  CRITICAL [RTS Art. 13(1)]
- [ ] Ustanowiono proces monitorowania realizacji
  HIGH [DORA Art. 26(6)]

8B: Atestacja

- [ ] Organ TLPT potwierdza, że wszystkie raporty zawierają wymagane informacje
  CRITICAL [RTS Art. 14; DORA Art. 26(7)]
- [ ] Wydano atestację (Annex VIII) zawierającą: daty testów, CIF, podmioty, dostawców, informacje o testerach, czas trwania, organy, dokumenty
  CRITICAL [RTS Art. 14(1); RTS Annex VIII]
- [ ] Dla testów transgranicznych: atestacja udostępniona odpowiednim organom do wzajemnego uznania
  CRITICAL [RTS Art. 16(1); DORA Art. 26(7)]
- [ ] Planowanie kolejnego cyklu TLPT rozpoczęte (w ciągu 3 lat)
  HIGH [DORA Art. 26(1)]

WSKAZÓWKA RED TEAM

Najczęstszy błąd w remediacji: plan adresuje konkretną podatność zamiast słabości systemowej. Jeśli konto serwisowe ze słabym hasłem zostało skompromitowane, naprawa to nie 'zmień to hasło'. Naprawa to 'wdróż zarządzanie dostępem uprzywilejowanym dla wszystkich kont serwisowych'.

WSKAZÓWKA RED TEAM

Każde ustalenie wymaga uczciwej oceny ryzyka dla scenariusza, w którym remediacja jest opóźniona. Regulatorzy nie oczekują 100% remediacji w 8 tygodni. Oczekują wiarygodnego planu z realistycznymi terminami.

WSKAZÓWKA RED TEAM

Niszczenie danych po TLPT nie jest opcjonalne i nie jest formalnością. Twoja umowa powinna określać terminy niszczenia (30 dni po atestacji to rozsądny cel), metody niszczenia (kasowanie kryptograficzne) oraz podpisany certyfikat zniszczenia od każdego zewnętrznego dostawcy.

Porównanie krajowych wdrożeń TLPT

Status wdrożenia TIBER-EU / DORA TLPT w 32 jurysdykcjach. Aktualizacja: marzec 2026.

Kraj	Organ TLPT	Framework	Status	Testerzy wewnętrzni
EU/ECB (SSM)	ECB	TIBER-EU / SSM Guide	Operacyjne	Nie (wyłącznie zewnętrzni)
Austria	OeNB + FMA	TIBER-AT	Operacyjne	Zgodnie z RTS
Belgium	NBB	TIBER-BE	Operacyjne	Zgodnie z RTS
Czech Republic	CNB	TIBER-CZ	Operacyjne	Zgodnie z RTS
Denmark	Danish FSA + Nationalbank	TIBER-DK	Operacyjne	Zgodnie z RTS
Finland	FIN-FSA + Bank of Finland	TIBER-FI	Operacyjne	Zgodnie z RTS
France	Banque de France	TIBER-FR	Operacyjne	Zgodnie z RTS
Germany	BaFin + Bundesbank	TIBER-DE	Operacyjne	Zgodnie z RTS
Iceland	Sedlabanki	TIBER-IS	Operacyjne	Zgodnie z RTS
Ireland	Central Bank of Ireland	TIBER-IE	Operacyjne	Zgodnie z RTS
Italy	Banca d'Italia + CONSOB + IVASS	TIBER-IT	Operacyjne	Zgodnie z RTS
Liechtenstein	FMA LI	TIBER-EU LI	Operacyjne	Zgodnie z RTS
Luxembourg	CSSF + BCL	TIBER-LU	Operacyjne	Zgodnie z RTS
Malta	MFSA	TIBER-MT	Operacyjne	Zgodnie z RTS
Netherlands	DNB	TIBER-NL / ART	Operacyjne	Zgodnie z RTS
Norway	Norges Bank + Finanstilsynet	TIBER-NO	Operacyjne	Zgodnie z RTS
Portugal	Banco de Portugal	TIBER-PT	Operacyjne	Zgodnie z RTS
Romania	BNR	TIBER-RO	Operacyjne	Zgodnie z RTS
Slovakia	NBS	TIBER-SK	Operacyjne	Zgodnie z RTS
Spain	BdE + CNMV + DGSFP	TIBER-ES	Operacyjne	Zgodnie z RTS
Sweden	Sveriges Riksbank	TIBER-SE	Operacyjne	Zgodnie z RTS
Bulgaria	BNB	Brak krajowego frameworku	DORA stosuje się bezpośrednio	Zgodnie z RTS
Croatia	HNB + HANFA	Brak krajowego frameworku	DORA stosuje się bezpośrednio	Zgodnie z RTS

Kraj	Organ TLPT	Framework	Status	Testerzy wewnętrzni
Cyprus	CBC + CySEC	Brak krajowego frameworku	● DORA stosuje się bezpośrednio	Zgodnie z RTS
Estonia	Finantsinspektsioon	Brak krajowego frameworku	● DORA stosuje się bezpośrednio	Zgodnie z RTS
Greece	Bank of Greece	Brak krajowego frameworku	● DORA stosuje się bezpośrednio	Zgodnie z RTS
Hungary	MNB	Brak krajowego frameworku	● DORA stosuje się bezpośrednio	Zgodnie z RTS
Latvia	Latvijas Banka	Brak krajowego frameworku	● DORA stosuje się bezpośrednio	Zgodnie z RTS
Lithuania	Lietuvos bankas	Brak krajowego frameworku	● DORA stosuje się bezpośrednio	Zgodnie z RTS
Poland	KNF + NBP	TIBER-PL (planned)	● W opracowaniu	Zgodnie z RTS
Slovenia	Banka Slovenije	Brak krajowego frameworku	● Transpozycja opóźniona	Zgodnie z RTS
United Kingdom	BoE / PRA / FCA	CBEST + STAR-FS	● Operacyjne (independent)	Zgodnie z frameworkiem

● Operacyjne ● Published / W opracowaniu ● Delayed

afine
digitally secure

O AFINE

AFINE świadczy ofensywne usługi bezpieczeństwa informacji, specjalizując się w testach penetracyjnych, audytach bezpieczeństwa i operacjach red team.

Nasz zespół badawczy opublikował ponad 150 CVE w oprogramowaniu SAP, Microsoft, IBM, CyberArk, Check Point, F5, Rapid7, Palo Alto Networks i Adobe. To właśnie ta zdolność badawcza czyni różnicę w TLPT - znajdowanie podatności, których nie wykrywają skanery i standardowe testy penetracyjne.

150+	10	ISO 27001
PUBLISHED CVES	YEARS OPERATING	CERTIFIED

"AFINE keeps finding critical issues where other pentesters have not found them."

- Isabel Group

Certyfikacje zespołu: OSCP (minimum per researcher), OSCE, OSWE, OSED, OSEP, CRTO, CSSA, CISSP, CISA, BSCP

Klienci referencyjni: PKO BP, ING Bank, BGK, CPBil, BIK, Tpay, BPS, Altira

Kontakt
afine.com | pwoyke@afine.com

Gotowy, żeby rozpocząć TLPT?

Umów konsultację TLPT

AFINE sp. z o.o.
pwoyke@afine.com