PENTESTERRA

DORA GAP ASSESSMENT

La Tua Resilienza Operativa Digitale È Testata Davvero?

Gap assessment sui 26 controlli DORA lungo i 5 pilastri - risk management ICT, gestione incidenti, resilienza operativa digitale, rischio di terze parti ICT - per entità finanziarie UE.

COS'È, IN BREVE

Copre i 5 pilastri di DORA: gestione del rischio ICT (Art. 5-16), gestione e segnalazione degli incidenti ICT (Art. 17-23), test di resilienza operativa digitale (Art. 24-27), rischio ICT di terze parti (Art. 28-30) e condivisione di informazioni (Art. 45).

26	Art. 24-27	UE
Controlli DORA coperti su 5 pilastri	Test di resilienza operativa digitale	Entità finanziarie e fornitori ICT critici

LA SITUAZIONE OGGI

CHI SEI

Sei il CISO o il responsabile rischio ICT di un'entità finanziaria UE - banca, assicurazione, gestore di fondi, fornitore di servizi di pagamento - soggetta a DORA dal gennaio 2025.

COSA È SUCCESSO

Il tuo assicuratore, un cliente istituzionale o l'autorità di vigilanza chiede evidenza dei test di resilienza operativa digitale richiesti dall'Art. 24-27.

PERCHÉ FA MALE

DORA richiede test di resilienza periodici e documentati. Un'entità che non può dimostrarli rischia sanzioni e, più concretamente, di perdere la fiducia di partner e supervisori.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, controllo per controllo, cosa è soddisfatto, cosa è parziale e cosa manca - con un'evidenza tecnica reale allegata a ogni risposta, non una dichiarazione ottimistica che nessuno ha verificato.

LA SOLUZIONE

Il DORA Gap Assessment di Pentesterra: una valutazione strutturata su tutti i controlli, con compilazione automatica dei controlli tecnici a partire da scansioni di vulnerabilità, penetration test, OSINT e monitoraggio dell'esposizione esterna, dove l'evidenza esiste.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo questionario di autovalutazione, e non stiamo parlando di un parere legale. Stai lavorando con [NOME AZIENDA] - fornitore certificato, italiano, con quasi 20 anni di storia nel settore della sicurezza informatica. Probabilmente ci conosci già, o conosci qualcuno - un collega, un fornitore, un concorrente - che è già stato nostro cliente. E il gap assessment non si ferma a una checklist cartacea: i controlli tecnici vengono auto-compilati dall'evidenza già raccolta, con mappatura cross-standard verso gli altri 12 framework supportati dalla piattaforma, così un secondo audit non riparte da zero.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con copertura di tutti i controlli e riferimento diretto alla base normativa. Se emergono gap, ti proponiamo le misure aggiuntive per colmarli: vulnerability assessment, penetration test di rete o applicativo, formazione e simulazioni di phishing.

COSA INCLUDE DAVVERO

Non una checklist generica - i controlli reali di DORA, raggruppati come li vedrai nella piattaforma.

Pilastro 1: Gestione del rischio ICT (Art. 5-16)

Il framework di governance e gestione del rischio ICT richiesto dall'organo di gestione.

- Responsabilità dell'organo di gestione sul rischio ICT
- Identificazione, protezione e prevenzione
- Rilevamento, risposta e ripristino

Pilastro 2: Gestione incidenti ICT (Art. 17-23)

Classificazione e segnalazione degli incidenti ICT rilevanti.

- Processo di classificazione degli incidenti
- Segnalazione alle autorità competenti
- Analisi post-incidente e lezioni apprese

Pilastro 3: Test di resilienza operativa (Art. 24-27)

Il pilastro dove Pentesterra offre l'evidenza tecnica più diretta.

- Programma di test basato sul rischio
- Test di penetrazione guidati da minacce (TLPT)
- Correzione dei risultati e retest

Pilastro 4-5: Terze parti ICT e condivisione (Art. 28-30, 45)

Il rischio della catena di fornitura ICT.

- Registro dei fornitori ICT critici
- Clausole contrattuali obbligatorie
- Condivisione di informazioni sulle minacce cyber

COSA RICEVI

- ✓ Una matrice di controllo esportabile in XLSX, con lo stato di ogni singolo controllo
- ✓ Un gap report editabile in DOCX, pronto per il tuo auditor o il tuo consiglio
- ✓ Compilazione automatica dei controlli tecnici dall'evidenza già raccolta dalla piattaforma
- ✓ Verifica di applicabilità guidata per settore, paese e dimensione aziendale
- ✓ Mappatura cross-standard verso gli altri 12 framework supportati - una risposta, riusata su più standard
- ✓ Un pacchetto per l'auditor in un click: questionario, evidenza tecnica e gap report insieme
- ✓ Raccomandazioni di remediation prioritizzate per i gap trovati

COME FUNZIONA

1

Definiamo il perimetro

Ambito dell'assessment, sistemi e processi coinvolti - stabiliamo insieme lo scope.

2

Raccogliamo l'evidenza

Compiliamo automaticamente i controlli tecnici dall'evidenza già raccolta dalla piattaforma.

3

Completiamo il questionario

I controlli non tecnici vengono verificati con il tuo team.

4

Ti consegniamo il report

Un PDF completo con i gap trovati e le azioni da intraprendere.

Scopri quanto sei pronto per DORA

Un report completo, pronto da presentare a clienti, auditor o al tuo consiglio di amministrazione.

Richiedi il tuo DORA Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance