Piano vulnerability assessment e penetration testing

Organizzazione	CWNET S.R.L.	Sede	Via Degli Oliveti 110, 54100 Massa (MS), Italia
Norma	ISO/IEC 27001:2022	Audit	Audit Stage 2 - AR_01.2
Codice evidenza	EV-32	Periodo audit	15-17/04/2026

Finalita del documento

Fornire evidenza di pianificazione per la NC major relativa ai dettagli di vulnerability/penetration testing.

Collegamento al rapporto Stage 2

Il rapporto Stage 2 CWNET evidenzia un SGSI ISO/IEC 27001:2022 applicato ai processi, agli asset e ai sistemi utilizzati per progettazione, attivazione, erogazione, gestione tecnica, monitoraggio, supporto e assistenza dei servizi di accesso a Internet e telecomunicazioni. Le evidenze sono predisposte in coerenza con le risultanze e le risposte del cliente emerse in audit.

Ambito del test

Sistemi e servizi esposti, apparati di rete, sistemi server, servizi web o gestionali nel perimetro SGSI, configurazioni critiche, accessi amministrativi, componenti infrastrutturali a supporto dei servizi Internet/ICT.

Piano attivita

Fase	Descrizione	Responsabile	Output
Scoping	Definizione asset, finestre, autorizzazioni e vincoli	Responsabile tecnico/SGSI	Piano test approvato
Vulnerability assessment	Scansione controllata e identificazione vulnerabilita	Fornitore/tecnico qualificato	Report vulnerabilita
Penetration test mirato	Verifica sfruttabilita controllata su asset autorizzati	Fornitore qualificato	Report PT
Remediation	Classificazione, priorita, correzione e mitigazione	Responsabile tecnico	Piano remediation
Retest	Verifica chiusura vulnerabilita critiche/alte	Fornitore/tecnico	Report retest

Requisiti

Le attivita devono essere autorizzate, non distruttive, tracciate, condotte da personale competente e collegate al risk assessment, alla SoA e al piano di trattamento.

Approvazione e validazione

Ruolo	Nominativo	Firma	Data
Responsabile SGSI			
Direzione	Marco Bondielli		