

Vibecoding in produzione

Le verifiche da chiudere prima di mettere un applicativo generato con strumenti di AI davanti a un utente reale. Da compilare a ogni rilascio. Chi non supera il gate ha un prototipo.

A Triage di perimetro

Il criterio del Cyber Resilience Act è dove il software viene eseguito. Segnare il caso che corrisponde e archiviare la motivazione.

Che cosa avete portato in produzione	Cyber Resilience Act	Si applica comunque
☐ Web app usata solo da browser	FUORI AMBITO	AI Act, GDPR, NIS2 se in perimetro
☐ App mobile scaricabile da uno store	IN AMBITO	Anche il backend che la fa funzionare
☐ Desktop, Electron, estensione browser, CLI	IN AMBITO	Tutto il resto
☐ SaaS con agente installabile o SDK distribuito	IN AMBITO	Il backend entra col prodotto
☐ Backend che fa funzionare un dispositivo del cliente	IN AMBITO	Come elaborazione dati a distanza
☐ Progressive web app installabile sul dispositivo	ZONA GRIGIA	Documentare la scelta caso per caso

B Le quattro esposizioni che restano comunque

Valgono anche fuori dal Cyber Resilience Act. Le prime due sono già applicabili oggi.

Obbligo	Applicabile da	Domanda di controllo
☐ Trasparenza AI Act, articolo 50	2 agosto 2026	L'utente sa che sta parlando con un sistema AI? I contenuti sintetici sono marcati?
☐ Alfabetizzazione, articolo 4	2 febbraio 2025	Esiste un registro di formazione con date, contenuti e partecipanti?
☐ Alto rischio, Allegato III	2 dicembre 2027	L'app fa selezione del personale, gestione dei lavoratori, credito, biometria o istruzione?
☐ NIS2 e protezione dei dati	già in vigore	Siamo in perimetro per settore e dimensione? La minimizzazione è stata progettata da qualcuno?

C Il gate: otto verifiche prima del rilascio

Tutte devono risultare superate o non applicabili. Mezza giornata la prima volta, un'ora a ogni rilascio successivo.

#	Verifica	Che cosa va dimostrato
☐ 1	Triage di perimetro	Decisione scritta, datata e archiviata, con la motivazione per ogni regime.
☐ 2	Distinta base (SBOM)	Generata in formato standard, archiviata col commit, scansione vulnerabilità eseguita, versioni fissate e non a intervallo aperto.
☐ 3	Autorizzazioni sul database	Sicurezza a livello di riga attiva su ogni tabella, nessuna condizione sempre vera, test negativo eseguito con esito di rifiuto.
☐ 4	Segreti fuori dal client	Ricerca sul bundle di produzione e sulla cronologia del repository. Le chiavi trovate vanno ruotate, rimuoverle dal codice non basta.
☐ 5	Trasparenza	Informativa su ogni componente generativo esposto e marcatura dei contenuti sintetici.
☐ 6	Log e conservazione	Log strutturati, periodo di conservazione definito e applicato, verifica che non contengano dati non previsti.
☐ 7	Contatto e procedura	Contatto di sicurezza pubblicato, procedura scritta, tempi interni definiti a ritroso dalle ventiquattro ore.
☐ 8	Titolarità e contratto	Titolare nominato e confine di responsabilità col committente messo per iscritto.

Esito. Otto su otto superate o non applicabili: prodotto, rilascio autorizzato. Anche una sola non conforme o non eseguita: prototipo, rilascio non autorizzato.

D Verifiche sui fornitori

Una colonna per fornitore. La risposta accettabile è un documento o una clausola, mai una risposta verbale in una call di vendita.

Piatt.	DB	Modello	Verifica
☐	☐	☐	Esportabilità reale del codice e proprietà del repository, provata con un export effettivo
☐	☐	☐	Trattamento dei prompt e del codice, con conferma esplicita su uso o non uso per addestramento
☐	☐	☐	Elenco aggiornato dei sub-responsabili del trattamento e residenza dei dati
☐	☐	☐	Certificazioni e verifiche indipendenti, con la data dell'ultima verifica di sicurezza offensiva
☐	☐	☐	Canale e tempi di divulgazione delle vulnerabilità, compatibili con la finestra di ventiquattro ore
☐	☐	☐	Controllo societario e giurisdizione, in ottica di designazione futura della catena di fornitura
☐	☐	☐	Posizione del fornitore rispetto a NIS2
☐	☐	☐	Storico degli incidenti e delle interruzioni, ricostruito in modo indipendente
		☐	Politica di versioning e preavviso di deprecazione del modello
		☐	Comportamento in caso di aggiornamento del modello sotto lo stesso nome commerciale
		☐	Luogo di elaborazione dei dati in inferenza
		☐	Clausole contrattuali sull'uso degli input inviati in inferenza

E Verifiche sul team

Meno numerose e più difficili da superare, perché toccano competenze e responsabilità invece che documenti.

Verifica	Che cosa va dimostrato
☐ Titolarità nominata	Una persona con nome e cognome risponde dell'applicativo, della segnalazione e della documentazione.
☐ Autorizzazione al rilascio	Un secondo paio di occhi obbligatorio sul deploy, anche in un team di due persone.
☐ Competenza di lettura	Almeno una persona sa leggere il codice generato su autorizzazioni, gestione dei segreti e validazione degli input.
☐ Alfabetizzazione documentata	Registro di formazione con date, contenuti e partecipanti.
☐ Presidio dell'orologio	Chi riceve la segnalazione il venerdì sera, con quale canale, escalation e sostituto in ferie.
☐ Conoscenza del perimetro	Il team sa se l'applicativo ricade nell'Allegato III, e lo sapeva prima del primo prompt.

F Come si eseguono i controlli tecnici

Controllo	Operazione concreta
Distinta base	Generare dal gestore di pacchetti in formato standard, archiviare con data e commit, passare a uno scanner di vulnerabilità note. Fissare le versioni: un intervallo aperto significa che il prodotto in produzione cambia senza che nessuno lo rilasci.
Autorizzazioni	Elencare le tabelle, verificare che la sicurezza a livello di riga sia attiva, leggere la condizione di ogni policy. Poi aprire una sessione con un utente qualsiasi e provare a leggere la riga di un altro. Finché non si vede un rifiuto, la policy è un'ipotesi.
Segreti	Cercare le chiavi nel pacchetto di produzione servito al browser, non nel sorgente. Ripetere sulla cronologia del repository. Ruotare quello che si trova.
Superficie esposta	Elencare funzioni serverless ed endpoint pubblicati, verificare per ciascuno quale controllo di autenticazione applica. Gli endpoint di supporto creati durante lo sviluppo restano raggiungibili.
Log	Leggere una giornata di registrazioni e cercare quello che non dovrebbe esserci: indirizzi email, contenuti degli utenti, token.
Regressione	Scrivere i tre test sulle operazioni più sensibili ed eseguirli a ogni rilascio. Tre test eseguiti battono trenta test pianificati.

Voce	Contenuto
Titolarità	© 2026 ZeroFive.AI, unità di consulenza di ICONI.CO srl, Roma. Tutti i diritti non espressamente concessi restano riservati.
Licenza	Questo documento è rilasciato con licenza Creative Commons Attribuzione - Non commerciale 4.0 Internazionale (CC BY-NC 4.0) . Testo completo: creativecommons.org/licenses/by-nc/4.0/deed.it
Cosa potete fare	Usarlo, stamparlo, compilarlo e adattarlo all'interno della vostra organizzazione per i vostri applicativi, anche se siete un'impresa. Condividerlo con colleghi, fornitori e clienti. Citarlo in articoli, corsi gratuiti, presentazioni e documentazione interna.
Precisazione sull'uso non commerciale	In qualità di licenziante chiariamo l'interpretazione della clausola: l'uso interno da parte di un'azienda sui propri prodotti non è considerato uso commerciale ai fini di questa licenza. La clausola non commerciale vieta di rivendere il documento o di incorporarlo in un servizio a pagamento.
Cosa non potete fare	Rivenderlo. Includerlo, anche modificato, in offerte di consulenza, audit, formazione o software a pagamento erogate a terzi. Ridistribuirlo come materiale proprio. Rimuovere o alterare l'attribuzione, il logo o questa sezione.
Attribuzione richiesta	Ogni riproduzione, adattamento o citazione deve riportare in modo leggibile: “Fonte: ZeroFive.AI, Checklist Vibecoding in produzione, zerofive.ai” , con collegamento a zerofive.ai quando il formato lo consente. Nelle versioni adattate va indicato che si tratta di un adattamento.
Uso commerciale	Per includere questo materiale in servizi a pagamento, prodotti o programmi formativi commerciali serve un accordo scritto. Richieste a hello@zerofive.ai .
Limitazione	Documento fornito così com'è, senza garanzie. Supporta la decisione e non costituisce parere legale né attestazione di conformità. La responsabilità delle valutazioni resta di chi lo utilizza. I riferimenti normativi sono aggiornati a settembre 2026 e vanno verificati alla data d'uso.

Consegna di un prototipo a terzi. Il contratto deve dire quattro cose: che l'artefatto è un prototipo destinato alla validazione, quali verifiche sono state eseguite e quali escluse con l'elenco, che il passaggio in produzione richiede un intervento ulteriore definito in perimetro e prezzo, chi assume la titolarità dal momento della consegna e da quale data.

Riferimenti. Guidance della Commissione europea sull'applicazione del Regolamento (UE) 2024/2847, documento C(2026) 5252 del 27 luglio 2026, e bozza interpretativa del 3 marzo 2026. Regolamento (UE) 2024/1689 come modificato dal Regolamento (UE) 2026/1744. Direttiva (UE) 2022/2555. Questo documento supporta la decisione e non sostituisce un parere legale.