

Vibecoding in production

The checks to close before putting an AI-generated application in front of a real user. To be completed at every release. Anyone who fails the gate has a prototype.

A Scope triage

The Cyber Resilience Act criterion is where the software runs. Tick the matching case and file the reasoning.

What you put into production	Cyber Resilience Act	Applies anyway
☐ Web app used through a browser only	OUT OF SCOPE	AI Act, GDPR, NIS2 if in scope
☐ Mobile app downloadable from a store	IN SCOPE	Including the backend behind it
☐ Desktop, Electron, browser extension, CLI	IN SCOPE	Everything else
☐ SaaS with an installable agent or distributed SDK	IN SCOPE	The backend comes with the product
☐ Backend powering a customer's device	IN SCOPE	As remote data processing
☐ Progressive web app installable on the device	GREY AREA	Document the choice case by case

B The four exposures that remain in any case

They apply outside the Cyber Resilience Act too. The first two are already applicable today.

Obligation	Applicable from	Control question
☐ AI Act transparency, Article 50	2 August 2026	Does the user know they are talking to an AI system? Is synthetic content marked?
☐ Literacy, Article 4	2 February 2025	Is there a training record with dates, content and participants?
☐ High risk, Annex III	2 December 2027	Does the app handle recruitment, worker management, credit, biometrics or education?
☐ NIS2 and data protection	already in force	Are we in scope by sector and size? Did anyone actually design the data minimisation?

C The gate: eight checks before release

All must be passed or marked not applicable. Half a day the first time, one hour at every subsequent release.

#	Check	What has to be demonstrated
☐ 1	Scope triage	Written, dated and filed decision, with reasoning for each regime.
☐ 2	Bill of materials (SBOM)	Generated in a standard format, filed with the commit, vulnerability scan run, versions pinned rather than left as open ranges.
☐ 3	Database authorisation	Row-level security enabled on every table, no always-true condition, negative test run with a refusal as the outcome.
☐ 4	Secrets out of the client	Search across the production bundle and the repository history. Keys found must be rotated; removing them from the code is not enough.
☐ 5	Transparency	Notice on every generative component exposed to users and marking of synthetic content.
☐ 6	Logging and retention	Structured logs, retention period defined and enforced, check that they hold no data they should not.
☐ 7	Contact and procedure	Published security contact, written procedure, internal timings set backwards from twenty-four hours.
☐ 8	Ownership and contract	Named owner and boundary of responsibility with the client set out in writing.

Outcome. Eight out of eight passed or not applicable: product, release authorised. Even one failed or not run: prototype, release not authorised.

D Supplier checks

One column per supplier. The acceptable answer is a document or a clause, never a verbal answer on a sales call.

Platf.	DB	Model	Check
☐	☐	☐	Real code portability and repository ownership, proven with an actual export
☐	☐	☐	Treatment of prompts and code, with explicit confirmation on use or non-use for training
☐	☐	☐	Current list of sub-processors and data residency
☐	☐	☐	Certifications and independent assessments, with the date of the last offensive security test
☐	☐	☐	Vulnerability disclosure channel and timelines, compatible with a twenty-four hour window
☐	☐	☐	Corporate control and jurisdiction, with future supply chain designation in mind
☐	☐	☐	The supplier's position relative to NIS2
☐	☐	☐	Incident and outage history, reconstructed independently
		☐	Model versioning policy and deprecation notice period
		☐	Behaviour when the model is updated under the same commercial name
		☐	Location of data processing for inference
		☐	Contractual clauses on the use of inputs sent for inference

E Team checks

Fewer and harder to pass, because they touch competence and accountability instead of documents.

Check	What has to be demonstrated
☐ Named ownership	One person, with a name, accountable for the application, its reporting and its documentation.
☐ Release authorisation	A mandatory second pair of eyes on deploy, even in a two person team.
☐ Reading competence	At least one person can read generated code across authorisation, secret handling and input validation.
☐ Documented literacy	Training record with dates, content and participants.
☐ Owning the clock	Who receives the security report on a Friday evening, through which channel, with which escalation and stand-in.
☐ Knowing the perimeter	The team knows whether the application falls under Annex III, and knew it before the first prompt.

F How to run the technical checks

Check	Concrete operation
Bill of materials	Generate from the package manager in a standard format, file it with date and commit, pass it to a known-vulnerability scanner. Pin versions: an open range means the product in production changes without anyone releasing it.
Authorisation	List the tables, verify row-level security is enabled, read the condition of every policy. Then open a session as an ordinary user and try to read another user's row. Until you see a refusal, the policy is a hypothesis.
Secrets	Search for keys in the production package served to the browser, not in the source. Repeat across repository history. Rotate whatever turns up.
Exposed surface	List serverless functions and published endpoints, verify which authentication control applies to each. Helper endpoints created during development stay reachable.
Logs	Read one day of records and look for what should not be there: email addresses, user content, tokens.
Regression	Write the three tests covering the most sensitive operations and run them at every release. Three tests that run beat thirty that are planned.

G Licence, attribution and limits

Item	Content
Ownership	© 2026 ZeroFive.AI, consulting unit of ICONI.CO srl, Rome, Italy. All rights not expressly granted are reserved.
Licence	This document is released under a Creative Commons Attribution - NonCommercial 4.0 International licence (CC BY-NC 4.0) . Full text: creativecommons.org/licenses/by-nc/4.0/
What you may do	Use, print, complete and adapt it inside your own organisation for your own applications, including as a commercial company. Share it with colleagues, suppliers and clients. Cite it in articles, free courses, presentations and internal documentation.
Clarification on non-commercial use	As licensor we state our interpretation of the clause: internal use by a company on its own products is not considered commercial use for the purposes of this licence. The non-commercial clause prohibits reselling the document or embedding it in a paid service.
What you may not do	Resell it. Include it, modified or not, in paid consulting, audit, training or software offerings delivered to third parties. Redistribute it as your own material. Remove or alter the attribution, the logo or this section.
Required attribution	Every reproduction, adaptation or citation must legibly carry: “Source: ZeroFive.AI, Vibecoding in Production Checklist, zerofive.ai” , with a link to zerofive.ai where the format allows. Adapted versions must state that they are an adaptation.
Commercial use	Including this material in paid services, products or commercial training programmes requires a written agreement. Requests to hello@zerofive.ai .
Limitation	Provided as is, without warranty. It supports the decision and does not constitute legal advice or an attestation of conformity. Responsibility for the assessments remains with the user. Regulatory references are current as of September 2026 and should be verified at the date of use.

Delivering a prototype to a third party. The contract should say four things: that the artefact is a prototype intended for validation, which checks were performed and which were excluded with the list, that moving to production requires further work defined in scope and price, and who takes ownership from the moment of delivery and from what date.

References. European Commission guidance on the application of Regulation (EU) 2024/2847, document C(2026) 5252 of 27 July 2026, and draft interpretative guidance of 3 March 2026. Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744. Directive (EU) 2022/2555.