

SaaS technical due diligence: 25 code checks

A one-page buyer checklist for reviewing a SaaS repository before you acquire it. Code only.

● Closed from the repository alone (15). Unmarked checks get repository evidence too, plus one seller answer. Boxes per check: Pass Fail Ask seller

SECRETS AND CREDENTIALS

- 01

No hardcoded API keys, passwords, tokens or private keys

☐☐☐
- 02

No secrets left in older Git history

☐☐☐
- 03

Development and production credentials separated

☐☐☐
- 04

Privileged or admin keys kept out of browser code

☐☐☐
- 05

Every production credential transferable and rotatable

☐☐☐

DATABASE AND AUTH

- 06

One user cannot read or change another user's data

☐☐☐
- 07

Database rules, RLS policies or backend checks present

☐☐☐
- 08

Private uploads and storage buckets require authorization

☐☐☐

TESTS, BUILDABILITY AND MAINTAINABILITY

- 09

Automated test suite exists

☐☐☐
- 10

Tests cover billing, auth, permissions and the core workflow

☐☐☐
- 11

Reproducible install and build with a maintained lockfile

☐☐☐
- 12

Environment setup and deployment documented

☐☐☐
- 13

No giant files, duplicated logic or untyped code blocking changes

☐☐☐

DEPENDENCIES AND LICENSING

- 14

Every declared package exists on the registry

☐☐☐
- 15

No exploitable vulnerabilities in production dependencies

☐☐☐
- 16

Main frameworks and runtimes still supported

☐☐☐
- 17

Dependency licenses fit commercial SaaS use

☐☐☐
- 18

No unexplained private forks or abandoned packages

☐☐☐

GIT HISTORY AND AUTHORSHIP

- 19

Real incremental development history (Lovable sync excepted)

☐☐☐
- 20

Contribution concentration and main authors understood

☐☐☐
- 21

Material contributors match IP assignment records

☐☐☐
- 22

Repository not reconstructed just before the sale

☐☐☐

BUS FACTOR AND HANDOVER

- 23

Another developer can set up the product from the repo

☐☐☐
- 24

Recurring operational jobs encoded or documented

☐☐☐
- 25

Critical external services survive ownership transfer

☐☐☐

DEAL NOTES AND FOLLOW-UPS

Check	Owner	Evidence requested	Fix before close?

When a box fails, do not ask only "can it be fixed?"

Ask what it costs, who can fix it, what can break during the fix, and whether the seller should fix it before closing.

In the research behind CVE-2025-48757, 170 of 1,645 Lovable projects analysed (10.3%) had database tables readable without authentication.

Full explanations: ascertify.io/due-diligence/technical-checklist

Repository review, evidence on 24 of 25: \$49