A RISK-FIRST PLAYBOOK

Vibe coded. What's next?

You shipped with Lovable, Bolt, v0, Replit or Cursor. You have real users, no dedicated engineer and a budget close to zero. Most teams like yours don't need a scalability audit yet. They need to know if they're one leaked API key away from a bad week. This playbook shows what to check first, what you can fix yourself for free, and where outside help is worth paying for.

Do this yourself today — free

DO THIS	WHY AND HOW
Rotate any API keys that might be exposed	If a key ever touched client-side code, a public repo or an AI chat log, treat it as burned. About 30 minutes if you know where to look.
Turn on your host's backups	Supabase, Railway, Render, Neon and most others have it built in, often free. If you've never checked, assume it's off.
Set up a free uptime monitor	UptimeRobot or Better Uptime will tell you the app is down before a user does.
Add a free error tracker	Sentry's free tier catches bugs that would otherwise pile up unseen.
Turn on 2FA everywhere	Hosting, domain registrar, payment processor, GitHub: every account that could sink the company if taken over.
Publish a privacy policy and terms	Free templates exist. Don't skip this, even pre-revenue, if you collect any user data.

What to check, in order

Ordered by what is most likely to hurt a small team first: security and data loss, then outages, then a codebase someone else can pick up. Scale and investor readiness come last, once there's real traffic or a real raise.

#	RISK	WHAT COULD GO WRONG	FIX IT YOURSELF?	WHERE WE HELP
1	**Exposed secrets & broken auth** High · High	Keys, database credentials or admin routes exposed in client code, git history or default settings. The #1 way AI-built apps get hacked or hit with a surprise bill.	Partly. You can rotate keys, but not see everything that's exposed	Risk Scan finds every exposure; Secrets & Auth Sprint fixes it
2	**No backups** Med-high · Catastrophic	One bad migration or dropped table, and nothing to restore from.	Mostly: a one-click toggle	We test that restore actually works: Backup & DR Setup
3	**No monitoring** High · Medium	You learn the app is down from an angry support email, hours later.	Yes, with free tools	Monitoring & Alerting Setup, configured right the first time
4	**Fragile, undocumented code** Medium · Blocks next step	Nobody can explain how half the app works, so every fix gets riskier and hiring or handoff stalls.	Partly, if you have the time	Codebase Handoff Docs
5	**Cost & performance landmines** Low now · Rises with growth	Inefficient queries and no caching turn a free tier into a real bill at 10x usage.	Rarely; invisible until the invoice	Cost & Query Sanity Check

6	**Privacy & compliance blind spots** Situational	Collecting emails, payments or personal data without consent flows or a GDPR/CCPA basics check.	Mostly for generic SaaS; not with sensitive data	Privacy Quick Screen, escalating to a full compliance audit if needed
7	**Scalability architecture** Low urgency	Built the way the tool defaults, not for 100x traffic.	Not worth fixing yet	Scale-Readiness, once traffic is real
8	**Investor & acquisition readiness** Situational	A term sheet suddenly needs technical answers nobody prepared.	No; build it before the ask	Investor Readiness, once a raise is real

Which situation are you in?

SITUATION	WHAT TO DO
A non-technical founder shipped an MVP with Lovable, v0 or Replit and has real users now	Run the free checklist above, then a **Risk Scan** before calling it "production-ready"
A technical co-founder used Cursor or Claude Code heavily and isn't sure what's in the codebase anymore	**Codebase Handoff Docs**
A user reported a bug that may have exposed someone else's data	Not a scan anymore: **Vibe Code Rescue**, today
The app is about to take real payments for the first time	**Secrets & Auth Sprint**, then **Privacy Quick Screen**
You're about to raise pre-seed or seed	**Risk Scan** now; **Investor Readiness** once the raise is real
You're hiring your first engineer	**Codebase Handoff Docs**
Usage just jumped after a launch or a viral post	**Cost & Query Sanity Check** before the next invoice
Something broke in production and nobody knows why	**Vibe Code Rescue**
An agency inherited a vibe-coded MVP and must quote a rebuild	**Risk Scan**, for an evidence-based starting point

WHEN YOU WANT A SECOND PAIR OF EYES

What you can get from us

START HERE

Vibe Code Risk Scan

1 day · remote · fixed price. A fast, evidence-based answer to "how much risk is hiding in here?" covering exposed secrets and auth, backups and monitoring.

- Every exposed key, route and insecure default we can find
- Backup and monitoring gaps
- A short, prioritized fix list
- A clear recommendation: fix it yourself, or which sprint you need

OFFER	WHAT IT SOLVES	FORMAT
Startup Starter Bundle Most teams start here	Risk Scan + Secrets & Auth Sprint + Backup & DR Setup, bundled at a lower price than buying them separately	≈ 2–3 days
Secure Secrets & Auth Sprint	Finds and fixes exposed keys, missing auth checks and insecure defaults	Under 1 day
Backup & Disaster-Recovery Setup	Turns on and tests backups, so "restore" is a real button	Half a day
Monitoring & Alerting Setup	Uptime and error monitoring, so you hear about problems first	Half a day
Codebase Handoff Docs	A plain-language map of how the app works, for the next person who touches it	Under 1 day

Cost & Query Sanity Check	Catches AI-generated queries and configs that get expensive at scale	Half a day
Privacy Quick Screen	Whether your data collection needs a privacy policy, consent flow or more	Half a day
Vibe Code Co-Pilot	A few hours a month of code review and questions: cheaper than hiring, faster than guessing	Monthly
Vibe Code Rescue Priority	48–72 hour response when production is down, data may be exposed, or a launch or raise is blocked	48–72 hours, priority

When it stops being a 1–5 person problem

Scale-Readiness

Infrastructure, DevOps and cost review sized for real growth.

Investor / Acquisition Readiness

Codebase, security and documentation packaged for technical due diligence.

Full Technical Audit

Our 10-module technical deep dive, once the codebase outgrows a light review.

Compliance Audit

SOC 2, GDPR, HIPAA, PCI DSS and more, once you handle regulated data.

Not sure where you stand? Book a Risk Scan

One day, one clear answer. Tell us what you built it with and what worries you.

info@gartsolutions.com
gartsolutions.com/services/it-audit-services/