AI App Risk Checklist

A quick founder-friendly pass over the risks that usually hide in AI-built apps: secrets, auth, data exposure, privacy basics, dependencies, and handoff gaps.

FOR	TIME TO COMPLETE	VERSION
AI-BUILT APP FOUNDERS AND OPERATORS	20-30 MINUTES	JULY 2026

How to use this

Work through the checklist before a demo, launch, investor call, or developer handoff. Anything marked No or Unknown becomes either a fix, a question for a developer, or a reason to book a deeper audit.

1 Secrets & configuration

AI-assisted builds often leak secrets through the client bundle, repo history, screenshots, or config files.

Check	Status	Notes / where checked
No API keys, service-role keys, database URLs, webhook secrets, or tokens are exposed in client-side code	Y / N / ?	
Secrets are stored in the deployment provider's environment variables, not in the repo	Y / N / ?	
Old keys have been rotated if they were ever pasted into prompts, commits, tickets, or screenshots	Y / N / ?	
Preview, staging, and production environments do not share powerful credentials unnecessarily	Y / N / ?	

2 Authentication & access control

Login is not the same as authorization. Check what users can actually read, change, or delete.

Check	Status	Notes / where checked
Private pages and API routes require authentication server-side	Y / N / ?	
Users cannot access another user's records by changing an ID in the URL or request body	Y / N / ?	
Admin actions are protected by a separate role or secret, not hidden only by the UI	Y / N / ?	
Database/storage rules default to deny and only allow intended reads/writes	Y / N / ?	
Row-level security or equivalent tenant isolation is tested, not just configured	Y / N / ?	

3 Personal data & privacy basics

If the app collects data about people, write down what you collect and why before traffic grows.

Check	Status	Notes / where checked
The app has a current privacy notice that matches actual data collection	Y / N / ?	
Each personal-data field has a purpose, retention expectation, and deletion path	Y / N / ?	
Analytics, cookies, pixels, and third-party tools are known and disclosed	Y / N / ?	
AI inputs/outputs are reviewed for personal, sensitive, confidential, or regulated data	Y / N / ?	
Logs, analytics, and error trackers do not capture secrets, prompts, files, or unnecessary personal data	Y / N / ?	

4 AI, abuse & failure modes

LLM apps fail differently: prompts leak, tools get abused, and model output can look authoritative when it is wrong.

Check	Status	Notes / where checked
Prompt injection, malicious uploads, and tool/function abuse have been tested	Y / N / ?	
Model outputs are constrained or reviewed before consequential actions	Y / N / ?	
Rate limits, spend limits, abuse monitoring, and user blocking exist	Y / N / ?	
Users are told when content or decisions are AI-assisted where that matters	Y / N / ?	

5 Dependencies, deployment & reliability

A small app can still depend on many packages, SaaS APIs, queues, model providers, and deployment settings.

Check	Status	Notes / where checked
Dependencies are installable from a lockfile and obvious unused packages are removed	Y / N / ?	
The app has basic error handling for failed payments, failed model calls, failed webhooks, and missing env vars	Y / N / ?	
Production build, lint, and core smoke checks have been run recently	Y / N / ?	
Backups or exports exist for user data that would be painful to lose	Y / N / ?	
Dependency audit, known vulnerable packages, and unused packages have been reviewed	Y / N / ?	

6 Handoff readiness

A future developer should not need to reverse-engineer the whole product before making one fix.

Check	Status	Notes / where checked
There is a README or runbook for local setup, env vars, deployment, and common commands	Y / N / ?	
The main data model, integrations, and background jobs are documented in plain language	Y / N / ?	
Known fragile areas, TODOs, and product assumptions are written down	Y / N / ?	
There is a prioritized list of fixes before launch, demo, or handoff	Y / N / ?	

7 Top risks to fix first

Pick the risks that would most damage trust, safety, or momentum if they failed in public.

#	Risk / gap	Severity	Owner / next action	Due
1		H/M/L		
2				
3				

Need a practical compliance review?

This template gets you started. If you'd like an engineer who does compliance to pressure-test your answers - or turn them into working controls, documentation, and audit-ready evidence - book a free 30-minute discovery call.

Book a free discovery call or visit rdelune.dev

This template is provided by rdelune LLC for general informational purposes only and does not constitute legal, regulatory, or professional advice, nor create a consultant-client relationship. Regulatory obligations depend on your specific facts and jurisdiction. Validate your completed document against the applicable law (e.g. the EU GDPR, the ePrivacy Directive, and the EU AI Act) and, where appropriate, with a qualified professional. © 2026 rdelune LLC. You may use and adapt this template freely within your organisation; please retain this attribution.