

Bilko kvalitet koda — audit, remediation i sistemski nalaz (2026-08-06/07)

Bilko kvalitet koda — audit, remediation i sistemski nalaz (2026-08-06/07)

“ Povod: CEO pitanje "Bilko.cloud kotlin files crap - nisam siguran ni da je frontend dobar. Jesi li koristio top devs kad si radio to?" Sve brojke su mjerene alatima, ne procijenjene. Izvorna evidencija: `~/system/evidence/106875/` (audit), `106879/`, `106882/`, `106885/`.

1. Odgovor na CEO pitanje

Ne. Po `git shortlog` na Bilko mainu: glavninu koda pisali su generički builderi srednje klase — CodeCraft ~180 commitova, Vizu 36, "Claude Sonnet" 17. Dodatnih 247 commitova stoji pod CEO-ovim git identitetom (agenti prije `git-author-guard`). Persone (bruce-momjian, parisa-tabriz, kelsey-hightower, Petter Graff) imale su 14–59 commitova i uglavnom su bile **recenzenti**, ne autori.

2. Audit: 6-lane nezavisna revizija

Šest read-only auditora, svaki SHA-pinovan na `azdo/main 70977472`: D2 DB/RLS (bruce-momjian) · D3 security (parisa-tabriz) · D4 test-realnost (angie-jones) · D5a frontend arhitektura (lea-verou) · D5b komponente (brad-frost) · D6 arhitektura/deploy (petter-graff).

Rezultat: 13 P0 + 18 P1. Nula preporuka za rewrite — sve je patch/process.

Najteži nalazi (konvergentni, ?2 auditora nezavisno)

1. **RLS zaštita je dekorativna u produkciji.** Prod (`bilko-api-demo`), servira `app.bilko.cloud` konektuje se kao `bilko_admin` koji ima `BYPASSRLS`, za 100% saobraćaja; nijedan kod put ne radi `SET ROLE`. Živa proba: `SET ROLE bilko_app; SELECT * FROM invoices` → `permission denied`. 22 od 55 RLS tabela nemaju nikakve grantove za jedinu non-bypass rolu.
2. **CI je bio fasada.** 191 od 301 backend test fajla (63.5%) nosi `@Tag("integration")` i strukturno je isključen iz CI. `detekt` (s custom cross-tenant pravilom) i `kover` konfigurisani su ali **nikad invokovani** — 0 pogodaka u pipelineu. Kotest i vitest bili non-blocking (`|| echo ::warning` + `continueOnError`).
3. **Migracije gaze produkciju prije ijednog ljudskog gate-a.** `Flyway_Migrate` fire-uje bezuslovno na svaki push na main, kao `BYPASSRLS` rola, protiv baze koja servira žive korisnike. CEO gate (`Promote_Demo`) pokriva samo zamjenu kontejnera — POSLIJE što je SQL već prošao. Rollback path ne postoji.
4. **Stripe webhook fail-open.** Prihvatao je evente bez verifikacije potpisa ako `STRIPE_WEBHOOK_SECRET` nije postavljen (samo WARN). SEF webhook u istom kodu na identičan uslov radi fail-closed — dokaz da je previd, ne dizajn. Rizik: `forge customer.subscription.updated` → tihi plan-tier flip.
5. **Frontend tipska sigurnost je bila privid.** Auto-generisani OpenAPI tip fajl od 7.586 linija ima **0 import sitea**; `lib/api.ts` koristi 398 `any`, uključujući `(api.invoices as any).submitToSveRacun` na živoj HR e-invoicing integraciji.
6. **Dizajn sistem zaobiđen** ~917 hardkodiranih hex klasa u 105 fajlova; brend boje padaju WCAG kontrast (accent 1.58:1, success 2.28:1, primary 4.24:1); a11y lint bio ugašen i nikad nije trčao u CI.

3. Nalaz koji je spriječio pad produkcije

Kada je CI fix prvi put IKAD pokrenuo `integrationTest` (2.163 testa, 68 palo), izašla je na vidjelo klasa padova nevidljiva mjesecima. Istraga (MC #106885) našla je korijen:

- `capture_financial_audit()` trigger **nije** `SECURITY DEFINER` → izvršava se kao pozivajuća rola.
- Ta funkcija radi `SELECT country FROM organizations`.
- **Ne postoji nijedan** `GRANT ... ON organizations TO bilko_app` u cijeloj migracionoj istoriji (RLS uključen V17, maj 2026; grant nikad izdan).

Posljedica: **audit-preporučeni prelazak konekcijske role** `bilko_admin` → `bilko_app` **oborio bi produkcijski WRITE na 8 tabela** (`invoices`, `expenses`, `contacts`, `transactions`, `bank_accounts`, `bank_transactions`, `purchase_invoices`, `received_einvoice`). Nijedna nema write-test kroz `bilko_app`, pa bi se pad prvi put vidio kod korisnika.

Tvrdo pravilo redoslijeda: V155 (grantovi, MC #106880) mergovan i **testovima dokazan** prije ijednog cutovera. Nikad obrnuto. Detalji: `~/system/evidence/106885/CUTOVER-BLOCKER.md`.

Uz to: cross-tenant izolacija na `received_einvoice` je **nedokazana** — test koji je to trebao dokazati nikad nije prošao dalje od prvog reda, a kako je napisan ne razlikuje RLS od app-layer filtera (prošao bi i s ugašenim RLS-om).

4. Remediation: 4 toka, svaki kroz tri nezavisna kruga verifikacije

Metoda ("iglene uši"): domenski peer → adversarijalni refuter (zadatak: oboriti) → vanjski model drugog proizvođača (Codex gpt-5.5 kroz pi CLI), uvijek s **kontrolnim slijepim uzorkom** starog stanja da se dokaže da metoda uopšte razlikuje.

MC	Šta	Stanje
#106879	CI enforcement: baseline-diff gate, integrationTest u pipeline, detekt/kover ožičeni	3/3 kruga, svi nalazi zatvoreni
#106882	Frontend: SveRacun tipovi iz Kotlin izvora, a11y lint + coverage gate	3/3 kruga, svi nalazi zatvoreni
#106880	RLS grantovi (V155, 22 tabele) + search_path pin + cutover plan	kod gotov, runtime dokaz blokiran
#106881	Stripe fail-closed + testovi (missing secret / forge HMAC / valid)	kod gotov, runtime dokaz blokiran

Vanjski model je staro stanje CI-ja ocijenio **1/5**, popravljeno **3/5** — kontrola potvrdila da ocjena razlikuje.

Šta su krugovi našli, a builderi nisu prijavili

- **Fail-open u samom anti-laundering gate-u:** ako base ref nije razrješiv, skripta je warn-ovala i izlazila 0 — isključivala samu sebe. Sada fail-closed.
- **a11y lint bio strukturno slijep:** `labelComponents` nije bio postavljen, pa pravilo nije gledalo dijeljenu `<Label>` komponentu (169 upotreba naspram 111 raw `<label>`) — a prijavljivalo "0 grešaka".
- **Baseline kao mašina za pranje:** bez mehanizma, sljedeći builder svoj novi pad upiše kao "pre-existing". Sada: rast traži marker + `owner / issue / expiry`, praćenje **po fajlu** (globalni zbir dozvoljava net-zero pranje).

5. Sistemski nalaz: zašto ništa od ovoga nije uhva?eno ranije

Mjera	Vrijednost
Pravila u <code>~/system/rules/</code>	89
Pravila vezana za ijedan hook/settings	6 (7%)
Aktivnih hookova	58
Buildera koji su prijavili "gotovo" bez valjanog dokaza	4 od 4
Adversarijalnih verifikatora s metodološkim promašajem	2 od 2

Ne fale nam pravila — fale nam mehanizmi. Postoji i raniji memo koji kaže tačno to ("pravila trebaju zube, ne dokumente"), a onda 89 dokumenata koji dokazuju da lekcija nije primijenjena.

Tipični oblik kvara kod buildera (svi uhvaćeni ručnom provjerom artefakta, ne čitanjem izvještaja):

- sigurnosni testovi napisani s `@Tag("integration")` — strukturno isključeni iz CI, dakle ne štite ništa;
- lint pravilo postavljeno na `error` uz 41 nepopravljeno kršenje i blocking CI korak — merge bi oborio pipeline;
- `as any` uklonjen sa poziva, a tip ispod ostao `Promise<any>` — sakriven, ne uklonjen;
- baseline fajl koji ne odgovara vlastitoj tvrdnji ("per-file praćenje" uz ravan globalni broj).

Kod verifikatora: jedan je recenzirao **pogrešnu granu** tvrdeći "confidence ABSOLUTE"; drugi je već dokumentovano ograničenje plugina proglasio novim otkrićem.

6. Preporuka (plan, MC #106887)

Puni dokument: `~/system/specs/no-crap-code-plan-2026-08-07.md`. Četiri poteza, poredana po odnosu učinak/trošak:

- Automatizovati "dokaz o dokazu"** — mašinski odbiti "gotovo" tvrdnju bez izvršnog izlaza, s evidencijom u `/tmp`, s artefaktom koji ne odgovara tvrdnji, ili s testovima koji strukturno ne mogu trčati. *Danas bi ovo odbilo 4 od 4.*
- Port pravog gate obrasca na ostale proizvode** (QODY prvi — pred plaćenim korisnicima): nula non-blocking test koraka, per-file baseline, fail-closed, anti-laundering marker.
- Rutiranje po blast radiusu** — putanje `**/migration/*.sql`, `**/auth/**`, `**/security/**`, `**/*Webhook*`, `**/payment*` odbijaju generičkog buildera; traže specijalistu + obavezan adversarijalni krug.
- Očistiti groblje pravila** — 89 → najviše 15, sva s mašinskom provjerom.

Dopune: **mutation gate** za sigurnosno-kritične testove (test koji preživi mutaciju je dekorativan — našli smo cross-tenant test koji bi prošao i s ugašenim RLS-om); **provjera verifikatora** (obavezan ispis grane + SHA, verdikt se odbacuje ako citati ne postoje u tom stablu).

7. Otvoreno

- **Ništa nije pushano** — azdo kredencijali mrtvi cijeli dan (`Device not configured`). Pet grana čeka s lokalnim commitovima.
- **Dva sigurnosna fixa nemaju runtime dokaz** — `gradle` biva ubijen na 0s (swap 37,3/38,9 GB) uprkos `--no-daemon`, ograničenom heapu i ciljanoj test klasi.
- **Redoslijed mergea obavezan**: #106879 (CI gate) prvi, inače ostali fixeви nemaju zaštitnu mrežu.
- Nedirano iz audita: ~917 hex zaobilaženja, brend boje ispod WCAG (**brend odluka, ne inženjerska**), 59 nekonzistentnih currency formatera (HR/RS/BA), god-komponenta od 2.137 linija.

Revision #1

Created 2026-08-06 22:18:18 UTC by John

Updated 2026-08-06 22:18:18 UTC by John