Open Tech Debt + Followups

Open Tech Debt + Followups

Context: Post-Sprint 0 landscape (2026-05-02)
Sprint program: Bilko stage UAT + bug-fix sprint

Active Followup MCs

MC #10500 — angie-jones Functional Smoke Re-run

Priority: M
Status: OPEN
Owner: TBD

Context: AC1 from UAT Phase 1 (MC #10487) was incomplete. Evidence file `/tmp/bilko-uat-bugs-10487.json` = 2 bytes (`{}`). No HAR files, no screenshots, no functional coverage per epic.

Scope:

- Re-run functional smoke test on stage with ALL 8 epics
- Capture evidence per epic: screenshot + HAR + reproduction steps
- Test AFTER Sprint 0 lands (MC #10494) so login works
- Output: structured JSON with ≥8 entries

8 epics to test:

1. Registration + org creation (now fixed — verify success flow)
2. Login + JWT token refresh
3. Invoice creation + PDV calculation
4. Expense recording + category assignment
5. Bank CSV import + auto-match
6. Chart of Accounts CRUD
7. P&L report generation
8. Multi-currency invoice with exchange rate lock

Acceptance criteria:

- `bilko-uat-bugs-RERUN.json` with structured findings (epic_name, urls_tested, screenshots[], har_files[], repro_steps[])
- HAR files saved to `/tmp/bilko-uat-har-<epic_name>.har`
- Screenshots saved to `/tmp/bilko-uat-screenshot-<epic_name>-<step>.png`

Blocker: Sprint 0 must land first (registration must work to proceed past login).

MC #10502 — PROD CUTOVER (Kotlin to Prod)

Priority: H
Status: OPEN
Category: BLOCKER

Context: TD-3 per DEPLOY-MAP.md. Prod `bilko-api` Cloud Run service is STILL running Express container (digest `sha256:2986d8b0...`, port 4000). Stage is Kotlin-safe. Cutover blocked.

Scope:

1. Verify stage Kotlin `bilko/api:stage-ab7d50d` is production-ready (Sprint 0 landed, registration works, no regression)
2. Audit prod Cloud SQL instance `bilko-db` schema state (Flyway version, jmbg/oib columns from V3, ENUM types)
3. Tag production-ready image: `docker tag bilko/api:stage-ab7d50d bilko/api:prod-<sha>`
4. Deploy to prod `bilko-api` Cloud Run service
5. Smoke test prod `/api/v1/health` + registration endpoint
6. Monitor for 24h (error rate, latency p95)
7. Document rollback procedure (Cloud Run traffic split to previous Express revision)

Blockers before cutover:

- Sprint 1 SEF decision (CEO choice: real integration vs honest banner) — cannot go to prod with stub if legal risk unacceptable
- Invoice email send (Sprint 1) — cannot market "send invoice" if email doesn't work
- TD-2 resolution (`postgres-socket-factory` + IAM auth) — MC #10240 (currently open)

Risk: Prod still on Express means any bug fix in Kotlin (e.g., registration fix #10494) does NOT reach prod users.

Decision authority: CEO (production cutover = revenue surface change)

MC #10504 — .gcloudignore Optimization

Priority: M
Status: OPEN
Parent: MC #10498 (Arch roadmap)

Context: Cloud Build web deploy uploads 492MB (includes `apps/api/build/`, `.gradle/`, all `node_modules/`). Upload step times out on slow connections (3+ minutes).

Scope:

1. Add to `.gcloudignore`:

```
apps/api/build/
apps/api/.gradle/
**/node_modules/
**/.next/
**/dist/
**/.turbo/
```

2. Test local: `gcloud meta list-files-for-upload` (dry-run to see filtered file list)
3. Verify upload size reduction: target <100MB
4. PR + merge
5. Verify next Cloud Build web deploy upload time <30s

Acceptance criteria:

- Cloud Build upload step duration <30s (down from 180s)
- Build still succeeds (no missing files causing build failures)

Tracked Tech Debt (DEPLOY-MAP.md)

TD-2: Cloud SQL Public IP, No SSL/IAM Auth

MC: #10240 (open)
Severity: MEDIUM (stage), BLOCKER (prod)

Current state:

- Stage DB `bilko-staging-db` allows connections from `0.0.0.0/0`
- `requireSsl=false` in connection string
- Direct TCP to public IP `35.228.33.112:5432`

- Password-based auth (secret in env var)

Risk:

- Credential rotation requires redeploy
- No certificate pinning
- Network traffic unencrypted

Required for prod:

- Implement `cloud-sql-socket-factory` in `build.gradle.kts`
- Switch to Cloud SQL IAM database authentication (service account-based)
- Remove public IP, use private VPC peering OR Cloud SQL Auth Proxy

Reference: ADR-023-postgresql-on-cloud-sql.md (exists, drives implementation)

TD-3: PROD Still on Express

MC: #10502 (see above)
Severity: BLOCKER

Pre-Existing Blueprint Violations (Score 61/100)

Source: `BUILD-BLUEPRINT.md` audit 2026-04-29

MEDIUM Violations (3)

1. Package Naming x2

What: Two packages violate ALAI package naming standard (`@alai/<name>`):

- `@bilko/api-types` (should be `@alai/bilko-api-types`)
- `@bilko/database` (should be `@alai/bilko-database`)

Impact: Cannot publish to ALAI npm registry (`npm.alai.no`) without rename.

Blocker for: Multi-repo code sharing (if Bilko utilities needed in other products).

Fix effort: Low (rename in `package.json` + update imports).

---

2. Dockerfile Base Image (Chainguard vs Distroless)

What: `apps/web/Dockerfile` uses `cgr.dev/chainguard/node:latest-dev` (resolved MC #10442 CVE fix). ALAI standard is `gcr.io/distroless/nodejs`.

Rationale for deviation: Chainguard swap was emergency CVE-2026-4878 mitigation. Distroless base had unpatched vulnerability at time of fix.

Status: Acceptable deviation (ADR-022 or inline justification should document this).

Action: No immediate change needed, but document rationale in `apps/web/Dockerfile` comment.

Known Unimplemented Features (From UAT)

1. Email Verification Flow (US-001 AC1-2)

Scope: Registration issues JWT immediately without email verification.

Security risk: Users can access financial data without verifying email ownership.

Required:

- Send verification email on registration (token link)
- `GET /auth/verify-email?token=<token>` endpoint
- UI confirmation page
- Block sensitive actions until verified (e.g., invoice send, bank connection)

Priority: P1 (security + compliance)

---

2. Automated Overdue Invoice Detection (US-012 AC2)

Scope: No scheduler exists to flip invoice status to `overdue` when `due_date < NOW()`.

Impact: Users never see overdue invoices unless status set manually via API.

Required:

- Cloud Scheduler job (daily at 06:00 UTC)

- Kotlin endpoint `POST /internal/invoices/check-overdue` (internal-only, auth bypass)
- Query invoices where `status = 'sent' AND due_date < NOW()` → update status to `overdue`
- Optional: send overdue notification email

Priority: P1 (core workflow)

---

3. Serbian CoA Seeding (US-001 AC4, US-030 AC1)

Scope: `CountryService.seedChartOfAccounts()` exists but not called from registration.

Impact: New orgs have empty chart of accounts.

Fix: Add function call in `AuthService.register()` after org creation.

Priority: P1 (user onboarding)

---

4. Multi-Org Support (US-004)

Scope: Each user has single `organizationId`. No switcher.

Impact: Accountants managing multiple companies must log out/in with different emails.

Required:

- `user_organizations` junction table
- `GET /users/me/organizations`, `POST /users/me/switch-organization`
- Org switcher dropdown in top-bar

Priority: P1 (SMB accountant use case)

---

5. Real SEF Integration (US-011)

Scope: Stub sefId (`SEF-STUB-<id>`) issued, no real efaktura.gov.rs HTTP.

Legal risk: Serbian e-invoicing law mandates real submission.

Decision pending: CEO choice (real integration vs honest banner).

Priority: P0 (legal compliance) or DEFERRED (if banner chosen)

Post-Sprint 0 Metrics

Completed Work (2026-05-02)

- **3 PRs merged:** #39 (Express deletion), #40 (Sprint 0 P0), #41 (Dockerfile fix)
- **2 P0 bugs fixed:** Registration ENUM + field contract
- **141 files deleted:** Express backend removal
- **1 regression resolved:** Web Dockerfile COPY reference

Open Bilko MCs (Post-Cleanup)

Total: 45 MCs remaining (down from 69 pre-cleanup, per MC #10300 sweep)

By priority:

- H: 8 (includes #10495, #10502)
- M: 22 (includes #10496, #10498, #10500, #10504)
- L: 15 (includes #10497)

By status:

- Open: 42
- In-progress: 3
- Blocked: 0 (after CEO triage)

References

MCs:

- MC #10487 — UAT Phase 1 (discovery)
- MC #10493 — Express deletion (DONE)
- MC #10494 — Sprint 0 P0 (DONE)
- MC #10495 — Sprint 1 (OPEN)
- MC #10496 — Sprint 2 (OPEN)
- MC #10497 — Sprint 3 (OPEN)
- MC #10498 — Arch roadmap (OPEN)
- MC #10500 — angie-jones re-run (OPEN)
- MC #10502 — PROD CUTOVER (OPEN, BLOCKER)
- MC #10504 — .gcloudignore (OPEN)

- MC #10240 — postgres-socket-factory (OPEN, TD-2)

Docs:

- DEPLOY-MAP.md — Cloud Run inventory + TD tracking
- BUILD-BLUEPRINT.md — Package standards + violations
- USER-STORIES.md — Acceptance criteria source
- ADR-023 — PostgreSQL on Cloud SQL (IAM auth guidance)

Evidence:

- `/tmp/bilko-uat-ux-10487.md` (maria-santos UX report)
- `/tmp/bilko-uat-gap-10487.md` (petter-graff architecture gaps)

Bilko repo: https://github.com/johnatbasicas/bilko

Revision #2
Created 2026-05-02 12:31:03 UTC by John
Updated 2026-06-07 20:01:01 UTC by John