Non-Functional Requirements

Non-Functional Requirements (NFR): Bilko

> **Project:** Bilko — Balkan Accounting SaaS **Version:** 0.1 **Date:** 2026-02-23
> **Author:** John (AI Director) **Status:** Draft **Reviewers:** Alem Bašić (CEO)

Document History

Version	Date	Author	Changes
0.1	2026-02-23	John (AI Director)	Initial draft — Phase 1 Serbia MVP

---

1. NFR Overview

Category	# Requirements	Highest Priority	Owner
Performance	8	Critical	John
Scalability	5	High	John / DevOps agent
Availability	6	Critical	John / DevOps agent
Security	10	Critical	John
Reliability	6	Critical	John
Usability	7	High	John / Designer
Compatibility	6	High	John
Maintainability	6	Medium	John
Compliance	8	Critical	John + Asmir
Data	8	Critical	John

2. Performance Requirements

ID	Requirement	Metric	Target	Measurement Conditions	Measurement Method	Priority
NFR-P01	Dashboard page load (initial)	Time to Interactive	< 3 seconds	4G connection, cold cache	Lighthouse / WebPageTest	Must Have
NFR-P02	Dashboard page load (subsequent)	Time to Interactive	< 1 second	Warm cache, average device	Lighthouse	Must Have
NFR-P03	Invoice creation wizard navigation	Time per step	< 500ms	Any device, warm cache	Lighthouse	Must Have
NFR-P04	API response time (standard CRUD)	p95 response time	< 300ms	≤ 1000 concurrent users	APM tool / k6	Must Have
NFR-P05	API response time (reports)	p95 response time	< 2 seconds	≤ 1000 concurrent orgs	APM tool	Must Have
NFR-P06	SEF submission response	End-to-end latency	< 30 seconds	SEF API response time	API monitoring	Must Have
NFR-P07	Core Web Vitals: LCP	Largest Contentful Paint	< 2.5 seconds	Mobile, 4G	Lighthouse	Must Have
NFR-P08	Core Web Vitals: CLS	Cumulative Layout Shift	< 0.1	Any device	Lighthouse	Must Have

3. Scalability Requirements

ID	Requirement	Metric	Launch Target	12-Month Target	Measurement Method	Priority
NFR-S01	Concurrent organizations	Active organizations	1,000	10,000	Load testing (k6)	Must Have
NFR-S02	Concurrent user sessions	Simultaneous sessions	500	5,000	Load testing	Must Have
NFR-S03	API throughput	Requests per second	200 RPS	2,000 RPS	k6 load test	Must Have

ID	Requirement	Metric	Launch Target	12-Month Target	Measurement Method	Priority
NFR-S04	Data volume per organization	Transactions per org/year	50,000	200,000	Storage + query monitoring	Should Have
NFR-S05	Auto-scaling response	Time to add new instance	< 3 minutes	< 3 minutes	Cloud console metrics	Should Have

---

4. Availability Requirements

ID	Requirement	Target	Measurement Period	Exclusions	Priority
NFR-A01	System uptime SLA	≥ 99.9%	Monthly rolling	Scheduled maintenance windows	Must Have
NFR-A02	Scheduled maintenance window	Max 2 hours/month	Monthly	Preferred: Sunday 02:00-04:00 CET	Must Have
NFR-A03	Maintenance notification lead time	≥ 48 hours notice	Per event	Emergency patches: 4 hours	Must Have
NFR-A04	RPO (Recovery Point Objective)	Max 1 hour data loss	Per incident	N/A	Must Have
NFR-A05	RTO (Recovery Time Objective)	System restored within 4 hours	Per incident	N/A	Must Have
NFR-A06	Database backup frequency	Daily full + hourly transaction log	Ongoing	N/A	Must Have

SLA Calculation Reference:

Uptime %	Annual Downtime	Monthly Downtime
99.9%	8.7 hours	43.8 minutes
99.5%	43.8 hours	3.6 hours
99.0%	87.6 hours	7.3 hours

---

5. Security Requirements

ID	Requirement	Category	Target / Standard	Measurement Method	Priority
NFR-SEC01	Authentication	Auth	JWT (access: 15min TTL) + refresh token (30d rolling TTL); bcrypt password hashing (cost factor ≥ 12)	Code review	Must Have
NFR-SEC02	Password policy	Auth	Min 8 chars, 1 uppercase, 1 number, 1 special character	Automated test	Must Have
NFR-SEC03	Account lockout	Auth	5 failed attempts → 15-min lockout; logged in LoggedAction	Automated test	Must Have
NFR-SEC04	Data encryption in transit	Encryption	TLS 1.3 minimum; HTTP → HTTPS redirect enforced	SSL Labs scan (grade A+)	Must Have
NFR-SEC05	Data encryption at rest	Encryption	Database encryption at rest (cloud provider); bcrypt for passwords	Infrastructure review	Must Have
NFR-SEC06	Input validation	Injection Prevention	All inputs sanitized server-side with Zod; parameterized queries via Prisma	Code review + SAST	Must Have
NFR-SEC07	XSS prevention	Injection Prevention	React default encoding + CSP headers; no dangerouslySetInnerHTML	OWASP ZAP / code review	Must Have
NFR-SEC08	Rate limiting	DDoS/Abuse	Auth endpoints: 5 req/min; General API: 100 req/min per IP	Load test + monitoring	Must Have
NFR-SEC09	Audit logging	Compliance	All auth events, financial mutations logged in LoggedAction (append-only) with user ID + timestamp	Log review	Must Have

ID	Requirement	Category	Target / Standard	Measurement Method	Priority
NFR-SEC10	Organization data isolation	Multi-tenancy	All database queries scoped to organizationId via middleware; no cross-tenant queries	Code review + penetration test	Must Have
NFR-SEC11	Security headers	HTTP Security	HSTS, X-Frame-Options: DENY, X-Content-Type-Options: nosniff, CSP	securityheaders.com scan	Must Have
NFR-SEC12	Dependency security	Supply Chain	No known critical CVEs; automated scan in CI	Snyk / npm audit in CI	Should Have

6. Reliability Requirements

ID	Requirement	Metric	Target	Measurement Method	Priority
NFR-R01	Application error rate	5xx errors / total requests	< 0.1%	APM monitoring	Must Have
NFR-R02	ACID compliance	Transaction integrity	100% — all financial transactions ACID-compliant	PostgreSQL guarantees + DB tests	Must Have
NFR-R03	Double-entry balance integrity	Debit = Credit for all transactions	Zero imbalance events	CI test: balance check on all transactions	Must Have
NFR-R04	SEF queue reliability	Failed SEF submissions retried	Max 3 retries; success on retry > 99% for transient failures	SEF monitoring	Must Have
NFR-R05	Data integrity	Zero data corruption	0 corruption events per 12 months	Database integrity checks	Must Have
NFR-R06	Health check endpoint	System health observable	/api/health returns 200 when healthy	Uptime monitoring	Must Have

7. Usability Requirements

ID	Requirement	Target	Measurement Method	Priority
NFR-U01	Time to create first invoice	New user creates first invoice in < 10 minutes	Beta user testing	Must Have
NFR-U02	Invoice wizard completion rate	≥ 85% of users who start wizard complete it	Analytics (funnel)	Must Have
NFR-U03	WCAG compliance	WCAG 2.1 Level AA	axe-core automated + manual	Must Have
NFR-U04	Keyboard navigation	All interactive elements reachable by keyboard	Manual testing	Must Have
NFR-U05	Mobile responsiveness	Fully functional on 375px–1440px viewport	Manual + Lighthouse	Must Have
NFR-U06	Language: Serbian	Full UI in Serbian (Latin script) for Phase 1; Cyrillic toggle	Manual review by native speaker	Must Have
NFR-U07	Error messages	All errors in Serbian language; actionable advice included	Content audit	Must Have

8. Compatibility Requirements

ID	Requirement	Category	Target	Priority
NFR-C01	Web browsers (desktop)	Browser	Chrome 100+, Firefox 100+, Safari 16+, Edge 100+	Must Have
NFR-C02	Web browsers (mobile)	Browser	Safari iOS 15+, Chrome Android 100+	Must Have
NFR-C03	Mobile operating systems	OS	iOS 15+, Android 11+	Must Have
NFR-C04	Screen resolutions	Responsive	375px to 2560px viewport width	Must Have
NFR-C05	SEF API compatibility	External API	SEF API v1 (UBL 2.1 XML, REST)	Must Have

ID	Requirement	Category	Target	Priority
NFR-C06	Bank CSV formats	Import	Serbian bank CSV formats: Raiffeisen, UniCredit, OTP, Banca Intesa	Should Have

9. Maintainability Requirements

ID	Requirement	Metric	Target	Measurement Method	Priority
NFR-M01	Test coverage (backend)	% code covered by automated tests	≥ 80% overall; ≥ 95% for financial logic (double-entry, VAT, SEF)	CI coverage report	Must Have
NFR-M02	TypeScript strict mode	Type safety	`strict: true` in tsconfig for all packages	CI type-check	Must Have
NFR-M03	Deployment frequency	Time to deploy bug fix to production	< 1 hour from PR merge	CI/CD metrics	Should Have
NFR-M04	Database migrations	Schema change process	All changes via Prisma migration; never edit existing migration	Code review	Must Have
NFR-M05	Monorepo build time	Turborepo build	Full build < 3 minutes; incremental < 30 seconds	CI metrics	Should Have
NFR-M06	Logging completeness	Log coverage	All external API calls (SEF, email, FX), all errors, all financial mutations logged	Log review	Must Have

10. Compliance Requirements

ID	Regulation	Applicability	Requirement	Technical Implementation	Priority

NFR-COMP01	Zakon o elektronskom fakturisanju (Serbia)	Yes — mandatory B2B 2023	Submit e-invoices to SEF in UBL 2.1; sequential numbering; digital signature	SefService module; UBL 2.1 XML generation	Must Have
NFR-COMP02	Zakon o PDV (Serbia)	Yes — all VAT-registered orgs	20% standard, 10% reduced PDV; monthly filing by 15th; PDV report format for ePorezi	PDV calculation engine; report export	Must Have
NFR-COMP03	Zakon o računovodstvu (Serbia)	Yes	Double-entry; 10-year document retention; annual balance sheet; audit trail	LoggedAction (append-only); DB retention policy	Must Have
NFR-COMP04	GDPR (EU / Norwegian Personvernloven)	Yes — ALAI Holding AS is Norwegian; processes EU citizen data	Lawful basis for processing; right to deletion within 30 days; DPA in place; breach notification within 72h; data export (Article 20)	User data deletion API; audit logs; DPA	Must Have
NFR-COMP05	GDPR — Data minimization	Yes	Collect only data necessary for accounting function	BA review of data model; field-level PII audit	Must Have
NFR-COMP06	GDPR — Cookie consent	Yes — if tracking cookies used	Explicit consent before non-essential cookies	Cookie consent banner; opt-in only analytics	Must Have
NFR-COMP07	Multi-tenancy data isolation	Yes — SaaS requirement	Organization data strictly scoped; no cross-tenant access	organizationId middleware + DB constraint	Must Have
NFR-COMP08	WCAG 2.1 AA	Yes — accessibility standard	Digital accessibility for all users	NFR-U03, NFR-U04	Must Have

11. Data Requirements

ID	Requirement	Category	Target	Implementation	Priority

NFR-D01	Monetary precision	Data type	ALL monetary fields: NUMERIC(19,4) — NEVER float, NEVER JavaScript number	Prisma schema: Decimal type enforced	Must Have
NFR-D02	Data retention — financial records	Retention	10 years minimum (Serbia); 11 years (Croatia)	Retention policy in DB; no auto-delete of financial records	Must Have
NFR-D03	Data retention — logs	Retention	Application logs: 90 days; Audit logs (LoggedAction): retain permanently	Log rotation + LoggedAction never purged	Must Have
NFR-D04	Database backup	Backup	Full backup daily; transaction logs every 1 hour	Automated backup schedule in cloud provider	Must Have
NFR-D05	Backup encryption	Backup	Backups encrypted at rest (AES-256)	Cloud provider encryption	Must Have
NFR-D06	PII identification	Privacy	All PII fields documented; user email, name, tax ID (PIB) identified	Data dictionary + Prisma annotations	Must Have
NFR-D07	Data export (portability)	Portability	User can export all organization data (invoices, expenses, transactions, contacts) in JSON/CSV	Export API endpoint	Must Have
NFR-D08	Exchange rate immutability	Integrity	Exchange rate locked at transaction date; cannot be retroactively edited	DB constraint + LoggedAction on change attempt	Must Have

12. NFR Testing & Verification Plan

NFR Category	Testing Method	Tools	Frequency	Pass Criteria
Performance	Lighthouse + k6 load test	Lighthouse, k6	Pre-launch + monthly	All NFR-P targets met at normal load

NFR Category	Testing Method	Tools	Frequency	Pass Criteria
Scalability	k6 stress test (2× normal load)	k6	Pre-launch	Graceful degradation; no data corruption under stress
Security	SAST + OWASP ZAP + manual code review	Snyk, OWASP ZAP	CI (SAST), Pre-launch (DAST)	No critical/high unresolved vulnerabilities
Compliance (SEF)	SEF sandbox end-to-end test	SEF sandbox API	Pre-launch	100% invoice submission success in sandbox
Compliance (PDV)	Manual accounting verification + test data	Test data set	Pre-launch + each PDV change	PDV calculations match expected values for 20 test cases
Compliance (GDPR)	Manual review + deletion test	Manual	Pre-launch + annual	Right to deletion completes within 30 days; export works
Accessibility	axe-core + keyboard manual test	axe-core	Per sprint	WCAG 2.1 AA — 0 critical violations
Availability	Uptime monitoring + DR drill	Uptime monitor	Ongoing + quarterly	SLA ≥ 99.9% monthly
Data integrity	DB constraint tests + balance check in CI	Prisma + custom tests	CI (every PR)	0 debit/credit imbalances; 0 NUMERIC precision errors

Approval

Role	Name	Date	Signature
Author	John (AI Director)	2026-02-23	
Reviewer			
Tech Lead	John	2026-02-23	
Business Analyst	John	2026-02-23	
Product Owner	John	2026-02-23	
AI Director (John)	John	2026-02-23	
CEO (Alem)	Alem Bašić		

Revision #3
Created 2026-02-24 22:50:51 UTC by John
Updated 2026-05-31 20:03:47 UTC by John