Risk Register: Drop — Fintech Payment App

Risk Register: Drop — Fintech Payment App

> **Project:** Drop — Remittance + QR Payments **Version:** 1.1 **Date:** 2026-02-23
> **Author:** John (AI Director) **Status:** Active **Reviewers:** Alem Bašić (CEO)

Document History

Version	Date	Author	Changes
0.1	2026-02-08	legal agent + finance agent	Initial 2-round risk identification
1.0	2026-02-11	John	Added technical risks from security audit
1.1	2026-02-23	John	Closed resolved risks; updated statuses

---

1. Risk Identification Methodology

Identification Methods Used:

☑ 2-round multi-agent analysis (8 agents: legal, finance, security, dev, marketer, data-engineer, product, nicksaraev)

☑ Security audit (2026-02-11, John — 1,102 lines of API code reviewed)

☑ Regulatory risk checklist (PSD2, AML, GDPR, DORA — gap analysis in security/COMPLIANCE.md)

☑ Business case risk matrix (zica-business-case-v2.md section 10)

☑ Assumption analysis (project charter)

Initial Risk Assessment Date: 2026-02-08 **Next Scheduled Review:** 2026-03-01 (sprint planning) **Risk Owner:** John (AI Director)

---

2. Risk Categories

Category	Description	Common Examples
Technical	Technology failures, integration issues, performance, security	JWT secrets, SQLite limits, API race conditions
Resource	Team availability, skill gaps, single points of failure	Alem sole decision-maker, AI cost overruns
External	Third-party dependencies, regulatory changes, market shifts	BaaS partner, Finanstilsynet, Vipps competition
Financial	Budget overruns, payment delays, cost estimates	Grant approval delay, marketing burn
Regulatory	Compliance failures, licence requirements, penalties	PSD2 licence, AML, GDPR, PCI-DSS
Quality	Defect rate, technical debt, process failures	Security vulnerabilities, untested integrations

---

3. Risk Probability & Impact Scale

3.1 Probability Scale

Level	Score	Definition
Very Low	1	< 10% chance
Low	2	10–30% chance
Medium	3	30–50% chance
High	4	50–70% chance
Very High	5	> 70% chance

3.2 Impact Scale

Level	Score	Schedule Impact	Financial Impact
Negligible	1	< 1 day	< 1% budget
Minor	2	1–3 days	1–5% budget
Moderate	3	3–7 days	5–10% budget
Major	4	1–2 weeks	10–20% budget
Critical	5	> 2 weeks	Project failure

3.3 Risk Matrix

Score	Risk Level	Response Required	Escalation
1–4	LOW	Monitor monthly	PM awareness
5–9	MEDIUM	Active mitigation plan	John awareness
10–14	HIGH	Immediate action + weekly review	John escalation
15–25	CRITICAL	Emergency response	John + Alem

---

4. Risk Appetite Statement

Overall Risk Appetite: LOW (fintech — money movement requires high safety standards)

Risk Category	Appetite	Rationale
Technical (security)	Very Low	Financial app — zero tolerance for data breaches
Regulatory	Very Low	GDPR, PSD2, AML violations have criminal penalties
Financial	Low	Fixed budget; overruns require Alem approval
External (BaaS)	Medium	Modular architecture allows provider swap
Timeline	Medium	Some schedule flexibility acceptable
Competition	High	Market risk accepted; innovation is our moat

---

5. Active Risk Register

ID	Risk Description	Category	Prob (1-5)	Impact (1-5)	Score	Response Strategy	Owner	Status	Date Identified
R-001	BaaS partner (Swan or SpareBank1) not confirmed — blocks Phase 2 Open Banking integration	External	4	5	20	Mitigate	Alem	Mitigating — SpareBank1 pitched; Swan backup	2026-02-08
R-002	Finanstilsynet PISP/AISP registration delayed beyond planned timeline	Regulatory	4	5	20	Mitigate	Alem + Legal	Open — not started	2026-02-08
R-003	Security breach before production hardening complete	Technical	2	5	10	Mitigate	John	Mitigating — audit done; 8 critical fixes tracked	2026-02-11
R-004	Vipps launches competing remittance feature	External	3	4	12	Accept	Alem	Monitoring	2026-02-08
R-005	Slow merchant adoption — QR revenue below projection	External	3	3	9	Mitigate	Alem	Open — door-to-door strategy planned	2026-02-08

ID	Risk Description	Category	Prob (1-5)	Impact (1-5)	Score	Response Strategy	Owner	Status	Date Identified
R-006	Hardcoded JWT_SECRET fallback active in production	Technical	2	5	10	Mitigate	John	Mitigating — fix tracked in Phase 0.5	2026-02-11
R-007	CVV/card data exposed via GET API endpoint (PCI-DSS violation)	Regulatory	2	5	10	Mitigate	John	Mitigating — last_four only; fix in Phase 0.5	2026-02-11
R-008	SQLite single-writer bottleneck at 200+ concurrent users	Technical	2	3	6	Accept	John	Accepted for MVP; PostgreSQL migration planned	2026-02-13
R-009	Alem is sole human decision-maker — decision bottleneck	Resource	3	3	9	Mitigate	Alem	Mitigating — decisions logged in comms/decisions/	2026-02-08
R-010	KYC mock in production — AML compliance not active	Regulatory	2	5	10	Mitigate	John	Open — Sumsub production required before real money	2026-02-13
R-011	No real BankID — DOB proxy insufficient for SCA	Technical / Regulatory	2	4	8	Mitigate	John	Open — Phase 1 is demo only; BankID in Phase 2	2026-02-13

ID	Risk Description	Category	Prob (1-5)	Impact (1-5)	Score	Response Strategy	Owner	Status	Date Identified
R-012	In-memory rate limiter resets on process restart — brute force risk	Technical	2	4	8	Mitigate	John	Mitigating — DB-backed rate limits in Phase 0.5	2026-02-11
R-013	No CSRF protection on state-changing API endpoints	Technical	2	4	8	Mitigate	John	Mitigating — CSRF middleware in Phase 0.5	2026-02-11
R-014	Cash flow gap if Innovasjon Norge grant delayed	Financial	3	3	9	Mitigate	Alem	Monitoring — AI costs keep burn < 10K/month	2026-02-08
R-015	Race condition on concurrent remittance transactions (double-spend)	Technical	2	5	10	Mitigate	John	Mitigating — per-user transaction lock implementation	2026-02-11

6. Risk Response Strategies

Risk ID	Strategy	Response Actions	Contingency Plan
R-001	Mitigate	1. SpareBank1 pitch submitted; 2. Swan evaluated as backup; 3. Modular BaaS interface in architecture	If neither works: explore Wio Bank, Finom, Treezor

Risk ID	Strategy	Response Actions	Contingency Plan
R-002	Mitigate	1. Engage external legal advisor for Finanstilsynet process; 2. Apply early; 3. Operate under bank partner licence initially	If delayed: launch in limited beta under partner licence
R-003	Mitigate	1. Security audit complete; 2. Phase 0.5 sprint fixes 8 critical issues; 3. No real money in MVP	If breach occurs: incident response plan in security/incident-response.md
R-004	Accept	Monitor Vipps announcements monthly; accelerate community adoption	Emphasise 0.5% vs Vipps fees; focus on trust advantage
R-005	Mitigate	1. Door-to-door onboarding; 2. 0% fee for first 3 months; 3. 200-merchant target Month 12	Adjust fee structure; focus on high-volume corridors
R-006	Mitigate	1. JWT_SECRET required env var — fail fast; 2. Secrets via Vaultwarden	Rotate secrets immediately; force re-auth
R-007	Mitigate	1. Remove CVV from GET response; 2. Store only last_four + token_ref; 3. Tokenisation via card partner	Suspend cards feature until fixed
R-010	Mitigate	1. Sumsub integration contract; 2. Mock clearly gated by feature flag; 3. No real money until KYC live	Suspend onboarding until KYC active
R-015	Mitigate	1. Per-user transaction lock (in-process); 2. DB-level constraint as backup; 3. PostgreSQL advisory locks in Phase 2	Suspend concurrent transactions; queue-based processing

7. Risk Heat Map

```
quadrantChart
    title Drop Risk Heat Map — 2026-02-23
    x-axis Low Impact --> High Impact
    y-axis Low Probability --> High Probability
    quadrant-1 "CRITICAL — Immediate Action"
    quadrant-2 "HIGH — Active Management"
```

```
    quadrant-3 "LOW — Monitor"
    quadrant-4 "MEDIUM — Watch"
    R-001 (BaaS partner): [1.0, 0.8]
    R-002 (Finanstilsynet): [1.0, 0.8]
    R-004 (Vipps): [0.8, 0.6]
    R-003 (Security): [1.0, 0.4]
    R-006 (JWT): [1.0, 0.4]
    R-007 (CVV): [1.0, 0.4]
    R-015 (Race condition): [1.0, 0.4]
    R-009 (Alem bottleneck): [0.6, 0.6]
    R-014 (Cash flow): [0.6, 0.6]
    R-008 (SQLite): [0.6, 0.4]
```

---

8. Escalation Thresholds

Threshold	Action	Responsible	Timeframe
Any new risk Score ≥ 15	Escalate to Alem + John	John	Within 4 hours
Any existing risk score increases by ≥ 5	Escalate to John	John	Within 24 hours
> 3 risks at Score ≥ 10 simultaneously	Emergency risk review	John + Alem	Within 48 hours
Risk triggers contingency plan	Notify all stakeholders	John	Immediately
Risk causes milestone slip > 3 days	Formal change request	John	Within 24 hours

---

9. Review Schedule

Frequency	Activity	Participants	Output
Weekly (Sprint Planning)	Review all active risks, update scores	John	Updated register
Sprint Retrospective	New risks identified; closed risks archived	John	New risks logged
Monthly	Full register review + heat map	John, Alem	Risk report
Milestone	Risk review before go/no-go	John, Alem	Go/no-go input

Review Log

Date	Reviewer	Risks Reviewed	New Added	Closed	Key Changes
2026-02-08	legal + finance agents	—	6	0	Initial identification
2026-02-11	John (security audit)	6	10	0	Added R-006 through R-015
2026-02-23	John	15	0	5	Closed R-C01 to R-C05; updated statuses

---

10. Closed Risks Archive

ID	Risk Description	Resolution Type	Resolution Notes	Date Closed
R-C01	Wallet/balance model requires e-money licence	Avoided	Pivoted to PSD2 pass-through model (ADR-003)	2026-02-12
R-C02	FontelePay tightly coupled to Drop — regulatory risk	Avoided	Separated to own module (ADR-002)	2026-02-12
R-C03	Zica brand name has cultural sensitivity	Avoided	Rebranded to Drop (Alem decision 2026-02-09)	2026-02-09
R-C04	"Banking" language in UI creates regulatory exposure	Mitigated	Removed all "banking" references from UI (task #197)	2026-02-09
R-C05	SHA-256 password support creates rainbow table vulnerability	Mitigated	SHA-256 support removed; bcrypt-only policy enforced	2026-02-13

Approval

Role	Name	Date	Signature
Author	John (AI Director)	2026-02-08	Approved (AI)
Reviewer	John (AI Director)	2026-02-23	Reviewed
AI Director (John)	John	2026-02-23	Approved
Project Sponsor	Alem Bašić	TBD — requires review	

Revision #5
Created 2026-02-23 12:04:18 UTC by John
Updated 2026-05-31 20:03:01 UTC by John