Governance

Decision authority and compliance

- Governance Framework

Governance Framework

Governance & Decision-Making Framework

Version: 1.0 **Last Updated:** 2026-01-28 **Owner:** Alem Basic **Prepared by:** John (Director) + Dženan Rizvanović (Risk & Compliance)

Executive Summary

This document defines WHO makes decisions, WHAT decisions require approval, HOW to make strategic vs operational decisions, and WHEN to escalate. It ensures Alem maintains control while empowering the team to move fast.

Core Principle: Alem has final authority. John executes. Team delivers.

---

1. Decision Authority Framework

1.1 Decision Categories

Category	Examples	Decision Maker	Escalation Path
Strategic	New products, markets, partnerships, fundraising, exits	Alem (final)	John prepares options → Alem decides
Operational	Daily execution, task assignment, priorities, bug fixes	John (immediate)	Logged for Alem review
Technical	Architecture, tech stack, infrastructure	Lejla (proposes) → Amina → John (approves)	Major changes → Alem
Financial (<€5K)	Tools, services, small purchases	John (immediate)	Logged to DB

Category	Examples	Decision Maker	Escalation Path
Financial (€5K-€50K)	Insurance, legal, marketing campaigns	Alem (decides)	John prepares business case
Financial (>€50K)	Series A, major contracts, acquisitions	Alem (decides)	Formal proposal
Legal/Compliance	Contracts, IP, regulatory	Dženan (reviews) → John → Alem	Always escalate
HR (hiring real humans)	Employees, contractors	Alem (approves)	John screens, Alem decides
Customer/Product	Feature priorities, pricing, packaging	Amina (proposes) → John → Alem	RICE-scored backlog

1.2 Alem's Reserved Powers (Non-Delegable)

Only Alem can decide:

- ☐ New product lines or major pivots
- ☐ Enter new markets (geography, vertical)
- ☐ Partnerships worth >€10K/year
- ☐ Fundraising (investors, debt, equity)
- ☐ Hiring employees (not contractors)
- ☐ Acquisitions, mergers, or exits
- ☐ IP strategy (patents, trademarks, licensing)
- ☐ Major legal agreements (>€10K liability)
- ☐ Charitable commitments (>€10K/year)
- ☐ Entity structure changes (holding company, new subsidiaries)
- ☐ Board decisions (if board exists)

Process:

1. John gathers data, prepares 2-3 options with pros/cons
2. John presents to Alem (written + verbal if needed)
3. Alem reviews and decides
4. John executes and logs decision

Timeline: John aims to present options within 48 hours, Alem decides within 48 hours.

1.3 John's Delegated Authority (No Approval Needed)

John can decide immediately:

- ☐ Task assignment to agents
- ☐ Sprint priorities (with Amina)
- ☐ Backlog refinement
- ☐ Purchases < €500/month
- ☐ Bug fixes and technical debt
- ☐ Customer support responses (via Selma)
- ☐ Deploy to staging
- ☐ Operational optimizations
- ☐ Process improvements
- ☐ Vendor selection (if <€5K/year and no BAA required)
- ☐ Content creation (blog, docs, marketing)
- ☐ Trading within approved strategy ($10K portfolio, -5% stop-loss, +8-10% take-profit)

Requirement: All decisions logged to john.db immediately for Alem's visibility.

---

2. Strategic Decision-Making Process

2.1 When to Make a Strategic Decision

Triggers:

- New opportunity emerges (partnership, market, product)
- Significant resource allocation needed (>€5K)
- Major risk identified (legal, compliance, competitive)
- External stakeholder request (investor, partner, customer)
- Quarterly planning cycle

Examples:

- "Should we build Bosnian Payment App in parallel with LumisCare?"
- "Should we raise Series A now or wait 6 months?"
- "Should we partner with bank X for Payment App?"
- "Should we hire a US-based sales rep?"

2.2 Strategic Decision Workflow

```
1. TRIGGER / OPPORTUNITY identified
   ↓
2. JOHN (or agent) gathers initial data
   ├─ What is the opportunity?
   ├─ Why now?
   ├─ What resources needed?
   └─ What are the risks?
   ↓
3. JOHN prepares decision brief (2-3 options)
   ├─ Option A: [Description, pros, cons, cost, timeline]
   ├─ Option B: [Description, pros, cons, cost, timeline]
   └─ Option C: Do nothing (status quo)
   ↓
4. JOHN presents to ALEM
   ├─ Written brief (1-2 pages)
   ├─ Verbal discussion (if needed)
   └─ Recommendation (John's opinion)
   ↓
5. ALEM reviews and decides
   ├─ Approve Option A/B/C
   ├─ Request more info
   └─ Defer decision (set deadline)
   ↓
6. JOHN executes decision
   ├─ Log to database
   ├─ Communicate to team
   └─ Track progress
```

Timeline:

- John prepares brief: 2-5 days
- Alem reviews: 2-3 days
- Total: 1 week for most strategic decisions

2.3 Decision Brief Template

```
# Strategic Decision Brief: [Title]

**Date:** YYYY-MM-DD
**Prepared by:** John
```

```
**Decision Owner:** Alem Basic

## Summary (2 sentences)
[What is the decision? Why does it matter?]

## Context
[Background, why now, what triggered this]

## Options

### Option A: [Name]
**Description:** [What would we do?]
**Pros:**
- [Benefit 1]
- [Benefit 2]
**Cons:**
- [Risk/downside 1]
- [Risk/downside 2]
**Cost:** €X
**Timeline:** X weeks/months
**Resources:** [Team, budget, tools]

### Option B: [Name]
[Same structure]

### Option C: Do Nothing
**Description:** Maintain status quo
**Pros:** No cost, no risk
**Cons:** Opportunity cost, competitive risk

## Recommendation
I recommend **Option A** because [rationale].

## Next Steps (if approved)
1. [Action 1] — Owner: [Name], Deadline: [Date]
2. [Action 2] — Owner: [Name], Deadline: [Date]

## Risks & Mitigation
- **Risk 1:** [Description] → **Mitigation:** [Plan]
- **Risk 2:** [Description] → **Mitigation:** [Plan]
```

```
## Decision
[ ] Approved — Option: _____
[ ] Defer — Reason: _____
[ ] Rejected — Reason: _____

**Decided by:** Alem Basic
**Date:** YYYY-MM-DD
```

---

3. Operational Decision-Making

3.1 Operational Decisions (John's Domain)

Examples:

- Which agent works on which task?
- Should we fix bug X before feature Y?
- Should we deploy to staging now or tomorrow?
- Should we buy tool X ($200/month)?
- How should we respond to customer support ticket?
- Should we allocate 20% sprint capacity to tech debt?

Process:

```
JOHN makes decision → Logs to DB → Executes → Reports to Alem (weekly summary)
```

No approval needed. Alem reviews logs and intervenes only if needed.

3.2 Operational Decision Checklist (John Self-Audit)

Before making operational decision, John asks:

- ☐ Is this within delegated authority? (Yes → proceed, No → escalate)
- ☐ Does this align with strategy? (Yes → proceed, No → escalate)
- ☐ Is cost < €5K? (Yes → proceed, No → escalate)
- ☐ Is this reversible? (Yes → proceed, No → escalate)
- ☐ Have I logged it to DB? (Yes → good, No → log it now)

If ANY answer is No → escalate to Alem.

---

4. Financial Governance

4.1 Budget Allocation

Annual Budget (Estimated, Scale Phase):

Category	Monthly	Annual	Owner
Infrastructure (AWS, hosting)	€2,000-4,000	€24K-48K	Nermin
SaaS tools	€500-1,000	€6K-12K	John
Marketing & sales	€1,000-3,000	€12K-36K	Selma
Team compensation	€5,000-15,000	€60K-180K	Asmir (SnowIT)
Professional services (legal, accounting)	€1,000-3,000	€12K-36K	Dženan
Insurance	€500-1,000	€6K-12K	Dženan
Trading capital	(€10K allocated)	—	Nick
Charity (50% of profit)	Variable	Variable	Alem
Total (excluding team compensation)	€5K-12K	€60K-144K	—

Budget Review: Monthly (John reports to Alem)

4.2 Financial Thresholds & Approval

Threshold	Approver	Process	Timeline
< €500	John	Immediate, logged	Same day
€500 - €5,000	John	Immediate, logged, Alem notified	Same day
€5,000 - €50,000	Alem	John prepares business case → Alem decides	3-7 days
> €50,000	Alem	Formal proposal, Alem pre-approves	1-4 weeks

4.3 Charitable Giving Governance (50% Commitment)

Policy:

- **50% of Fast Constructions (USA) net profit** → charity (annually)
- Net profit = Revenue - COGS - Operating Expenses - Taxes
- Donated annually (easier accounting)
- Alem selects charities (or delegates to John)
- Public transparency report published on lumiscare.com/impact

Example Calculation (Year 1):

- Revenue: €100,000
- COGS + OpEx: €60,000
- Net Profit: €40,000
- Charity: €20,000 (50%)
- Retained: €20,000

Charity Selection:

- Healthcare access (aligned with mission)
- Underserved communities
- US-registered 501(c)(3) or equivalent
- Verified via GuideStar/Charity Navigator

---

5. Risk Management Framework

5.1 Risk Identification & Logging

Who identifies risks:

- Dženan (primary risk manager)
- Any team member can flag risk
- John reviews risk register monthly

Risk Categories:

- **Strategic:** Competitive threats, market changes
- **Financial:** Cash flow, budget overruns
- **Operational:** Team capacity, infrastructure
- **Legal/Compliance:** HIPAA, contracts, IP

- **Technical:** Security vulnerabilities, tech debt
- **Reputational:** Customer churn, bad press

Risk Register Location: `~/clawd/org/risk-register.csv` + john.db

5.2 Risk Assessment Matrix

Probability	Impact	Risk Level	Action Required
High	High	**CRITICAL**	Escalate to Alem immediately
High	Medium	**HIGH**	Mitigation plan within 1 week
Medium	High	**HIGH**	Mitigation plan within 1 week
Medium	Medium	**MEDIUM**	Monitor, mitigation plan within 1 month
Low	High	**MEDIUM**	Monitor, mitigation plan within 1 month
Low	Medium	**LOW**	Monitor, review quarterly
Low	Low	**LOW**	Log, no immediate action

5.3 Top 10 Risks (as of 2026-01-28)

#	Risk	Probability	Impact	Level	Mitigation Owner
1	HIPAA breach (LumisCare)	Low	Critical	HIGH	Dženan
2	Bank partner withdraws (Payment App)	Medium	High	HIGH	Amina
3	Regulatory rejection (Payment license)	Medium	Critical	HIGH	Dženan
4	Key person dependency (Lejla/Nermin)	Medium	High	HIGH	Amina
5	Slow customer acquisition (LumisCare)	Medium	High	HIGH	Selma

#	Risk	Probability	Impact	Level	Mitigation Owner
6	Cash culture resistance (Payment App)	High	Medium	HIGH	Selma
7	Security vulnerability exploited	Low	Critical	HIGH	Nermin + Tarik
8	US market competition (LumisCare)	Medium	Medium	MEDIUM	Lejla + Selma
9	Infrastructure outage	Low	High	MEDIUM	Nermin
10	Scope creep / burnout	Medium	Medium	MEDIUM	Emir

Risk Review Cadence: Monthly (Dženan leads)

---

6. Compliance Governance

6.1 Regulatory Compliance Framework

LumisCare (US Healthcare)

Regulations:

- HIPAA (Privacy Rule, Security Rule, Breach Notification)
- HITECH Act
- State regulations (varies by state)
- 21st Century Cures Act (information blocking)

Compliance Owner: Dženan Rizvanović

Compliance Checklist (Quarterly Review):

- ☐ HIPAA risk assessment completed
- ☐ All vendor BAAs signed
- ☐ Privacy policy up to date
- ☐ Security controls tested
- ☐ Audit logs reviewed

- [ ] HIPAA training conducted (annual)
- [ ] Breach notification process tested

Audit Schedule:

- **Internal audit:** Quarterly (Dženan + Tarik)
- **External audit (SOC 2 Type II):** Annually (Month 6)

Payment App (Bosnia - Future)

Regulations:

- PSD2 (Strong Customer Authentication, open banking)
- PCI-DSS (card data security)
- BiH Banking Agency (payment institution license)
- AML/KYC (anti-money laundering, know your customer)
- GDPR (data protection)

Compliance Owner: Dženan Rizvanović

Timeline: Begin regulatory research Month 3, full compliance before GA launch.

6.2 Compliance Escalation

If compliance issue identified:

```
COMPLIANCE ISSUE detected
   ↓
DŽENAN investigates (within 1 hour)
   ├─ Assess severity (P1 = breach, P2 = risk, P3 = gap)
   ├─ Document findings
   └─ Escalate to John
   ↓
JOHN escalates to ALEM (within 1 hour for P1, 24h for P2/P3)
   ↓
ALEM decides response
   ├─ Notify customers (if breach)
   ├─ Notify regulators (if required)
   ├─ Engage legal counsel
   └─ Implement remediation
```

P1 Compliance Incidents:

- HIPAA breach (PHI exposed)
- PCI-DSS violation (card data exposed)
- Regulatory audit failure
- BAA violation by vendor

Response SLA: 1 hour to escalate, 24 hours to begin remediation

---

7. Intellectual Property Governance

7.1 IP Ownership Policy

Policy: All IP created by SnowIT for LumisCare is owned by Fast Constructions (USA).

Mechanism: Development Services Agreement (work-for-hire clause)

IP Assets:

- Source code
- Database schemas
- Design assets (UI/UX)
- Documentation
- Brand/trademarks
- Patents (future)

Assignment: All agents sign IP assignment clause in agreements.

7.2 Patent Strategy

Current Status:

- Provisional patent filing target: Within 60 days (by ~March 28, 2026)
- Innovation: Real-time AI clinical participation + video + home health forms (Vapi voice-to-assessment)

Governance:

- **Owner:** Fast Constructions (USA) — recommended
- **Decision:** Alem approves filing
- **Execution:** Patent attorney (Fish & Richardson or Finnegan)
- **Budget:** €3K-6K provisional, €50K-110K full utility over 3 years

Process:

1. Lejla documents technical innovation (2 weeks)
2. Dženan identifies patent attorney (2 weeks)
3. Attorney drafts application (4 weeks)
4. Alem reviews and approves (1 week)
5. File provisional (before 60-day deadline)

7.3 Trademark & Brand Governance

Current Trademarks:

- LumisCare (unregistered, use-based rights)

Action Required:

- ☐ File US trademark for "LumisCare" (word mark + logo)
- ☐ File trademark in EU/BiH (if expanding internationally)

Owner: Fast Constructions (USA) **Timeline:** File within 6 months (Month 6) **Budget:** €1,000-2,000 (US trademark)

---

8. Data Governance

8.1 Data Classification

Data Type	Sensitivity	Examples	Protection
PHI (Protected Health Information)	Critical	Patient names, diagnoses, visit notes	AES-256, TLS 1.3, RBAC, audit logs
PII (Personally Identifiable Information)	High	Email, phone, address	AES-256, TLS 1.3
Financial	High	Credit cards, bank accounts, transaction history	PCI-DSS, tokenization
Business Confidential	Medium	Revenue, customer list, roadmap	Access control, NDA
Public	Low	Marketing content, blog posts	No special protection

8.2 Data Retention Policy

Data Type	Retention Period	Rationale	Disposal Method
PHI (patient records)	6 years minimum (HIPAA)	Legal requirement	Secure deletion + audit log
Financial records	7 years (IRS requirement)	Tax compliance	Secure deletion
Audit logs	6 years (HIPAA)	Compliance	Secure deletion
Customer account data	90 days after cancellation	Business continuity	Secure deletion
Backups	30-90 days	Disaster recovery	Encrypted, auto-delete
Marketing data (non-PHI)	Indefinitely (or until opt-out)	Business use	Delete on request (GDPR)

8.3 Data Breach Response Plan

If PHI or PII breach detected:

```
1. DETECT breach (monitoring, report, audit)
   ↓
2. CONTAIN (within 1 hour)
   ├─ Nermin: Shut down affected system (if needed)
   ├─ Lejla: Identify scope of breach
   └─ Dženan: Begin documentation
   ↓
3. ASSESS impact (within 4 hours)
   ├─ How many individuals affected?
   ├─ What data was exposed?
   ├─ Was data encrypted?
   └─ Is this a HIPAA "breach" (legal definition)?
   ↓
4. NOTIFY (within legal deadlines)
   ├─ Customers affected (without undue delay, max 60 days)
   ├─ HHS (if >500 individuals, within 60 days)
   ├─ Media (if >500 individuals)
   └─ Business associates (if their data)
   ↓
5. REMEDIATE
   ├─ Fix vulnerability
   ├─ Enhance controls
   └─ Post-mortem
   ↓
6. DOCUMENT everything (legal defense)
```

Dženan owns breach response plan. Documented in `~/clawd/org/breach-response.md`.

---

9. Performance & Accountability

9.1 KPI Governance

Monthly Business Review (MBR) — Last Friday of Month

Attendees: Alem, John, Amina

Agenda:

1. Revenue & growth (MRR, customers, churn)
2. Product & development (features, velocity, tech debt)
3. Operations (uptime, incidents, support)
4. Trading (P&L, ROI)
5. Risks & compliance
6. Next month priorities

Dashboard: John maintains live dashboard (Notion, Grafana, or spreadsheet)

KPI Targets:

KPI	Target	Owner	Frequency
MRR (Monthly Recurring Revenue)	10%+ MoM growth	Selma	Monthly
Customer count	10 by Month 6, 50 by Month 12	Selma	Monthly
Churn rate	< 5% monthly	Selma + Amina	Monthly
Uptime	99.9% (LumisCare), 99.99% (Payment App)	Nermin	Daily
Deployment frequency	Daily (staging), weekly (prod)	Nermin	Weekly
Sprint velocity	Consistent ±10%	Emir	Per sprint
Bug escape rate	< 5%	Tarik	Per sprint
Test coverage	≥ 80%	Tarik + Lejla	Per release
Support response time	< 30 min (Tier 1)	Selma	Daily
Trading ROI	5%+ monthly	Nick	Monthly

KPI	Target	Owner	Frequency
Charity donations	50% of net profit	Alem	Annually

9.2 Accountability Mechanisms

How we ensure accountability:

- **RACI matrix** — every task has one owner (R = Responsible)
- **Daily standups** — public commitment to daily goals
- **Sprint reviews** — demo what shipped
- **Retros** — continuous improvement
- **Monthly KPI review** — Alem holds John accountable, John holds team accountable
- **Database logging** — all decisions logged, audit trail
- **GitHub** — all code changes tracked
- **Post-mortems** — blameless analysis of failures

Consequences for missed commitments:

- **First time:** Discussion, root cause analysis, improvement plan
- **Repeat pattern:** Re-assign task, escalate to Alem
- **Systemic issue:** Process improvement, not blame

Rewards for excellence:

- Public recognition (team meetings, retros)
- Increased responsibility (ownership of bigger projects)
- Future: Bonuses tied to KPIs (when profitable)

---

10. Change Management

10.1 How to Change This Document (GOVERNANCE.md)

Process:

1. Anyone can propose change (via John)
2. John reviews and assesses impact
3. If minor (typo, clarification): John updates, logs change
4. If major (authority change, new policy): John prepares proposal → Alem approves
5. Version control: All changes logged in document control table

Review Cadence: Quarterly (every 3 months)

10.2 Governance Evolution

As organization grows:

Stage	Headcount	Governance Changes
Startup (now)	1 owner + 1 AI + 10 agents	Alem = CEO, John = Director, informal governance
Growth (10-50 users)	+1-2 real humans	Formalize employment contracts, add HR policies
Scale (50-500 users)	+5-10 real humans	Create formal board, add CFO, legal counsel
Enterprise (500+ users)	+20+ real humans	Full C-suite, board of directors, formal governance

Current stage: Startup. Keep governance lean, bias toward action.

---

11. Document Control

Version	Date	Changes	Author
1.0	2026-01-28	Initial document	John + Dženan

Next Review: 2026-04-01 (quarterly)

Owner: Alem Basic **Maintained By:** John (Director) + Dženan Rizvanović (Risk & Compliance)

End of Governance Document

Clear authority. Clear escalation. Clear accountability. Alem controls, John executes, team delivers.