AINNA Cooperation Command Centre (ACCC)

Proposal, Technical Specification, Roadmap and Cost Assumptions

AINNA

Table of Contents

1 PROPOSAL PEMBANGUNAN AINNA COOPERATION COMMAND CENTRE (ACCC)

1.1 Platform Pengurusan, Deployment dan Operasi Sistem Koperasi Berskala Besar

Dicadangkan oleh: AINNA
Platform utama: AINNA Cooperation Command Centre (ACCC)
Sistem koperasi: KOARGO
Konsep: Centralised System Management, Decentralised Data Ownership
Status: Cadangan sulit untuk penilaian dan discovery

1.2 1. Ringkasan Eksekutif

AINNA mencadangkan ACCC sebagai control plane pusat untuk mengurus deployment, infrastructure, subscription, billing, version, modules, support, security dan operational health bagi seluruh rangkaian KOARGO.

ACCC bukan pangkalan data pusat data ahli koperasi. Setiap koperasi menerima sekurang-kurangnya satu VPS dedicated, satu database, storage, domain, encryption context, backup dan konfigurasi sendiri.

Polisi asas:

1. One Cooperative - One Isolated VPS.
2. One Cooperative - One Isolated Database.
3. One Controlled Access Plane to ACCC.
4. No Direct Public Administrative Access.
5. ACCC Manages Systems - Not Cooperative Data.

Model ini membolehkan AINNA mengurus puluhan hingga ribuan sistem tanpa menghasilkan satu giant multi-tenant database yang mempunyai blast radius tinggi.

1.3 2. Visi dan Model Digital Franchise

ACCC bertindak sebagai Digital Franchisor HQ. Setiap deployment KOARGO ialah managed cooperative system node dengan Cooperative ID, Deployment ID, VPS ID, subscription, contract, domain, package, modules, infrastructure allocation, version, SLA, agents, backup policy, health status, development history dan billing history.

Setiap node kekal mempunyai data sovereignty sendiri. Kegagalan atau serangan pada satu node tidak sepatutnya membuka data atau menurunkan availability node lain.

1.4 3. Skop Fungsi ACCC

ACCC merangkumi:

- Cooperative Registry dan System Registry.
- VPS, domain, SSL dan infrastructure registry.
- Golden Template dan deployment blueprint.
- Automated provisioning dan installation tests.
- Node Agent, heartbeat, monitoring dan alerting.
- Backup, restore testing dan disaster recovery readiness.
- Golden Standard dan configuration drift detection.
- Version, module dan safe release management.
- Subscription, billing, contract dan renewal.
- Support ticket dan development request lifecycle.
- PAM, temporary access dan break-glass governance.
- NeuralOps routing, agents dan private AI gateway.
- Capacity planning, cost, margin dan upsell analytics.
- Complete audit trail dan offboarding workflow.

1.5 4. Data Governance

ACCC dibenarkan menerima metadata minimum seperti System ID, status, application version, CPU, RAM, storage, database connectivity, latency, queue backlog, SSL status dan backup outcome.

Secara default ACCC tidak menerima nama ahli, nombor pengenalan, alamat, akaun bank, transaction details, pinjaman, dividen, dokumen, financial records atau personal information.

Jika diagnostic memerlukan data pelanggan, akses mesti diluluskan oleh pentadbir koperasi, mempunyai tujuan khusus, tempoh pendek, full audit dan automatic revocation. AINNA tidak menyimpan permanent customer database credential.

1.6 5. Deployment Engine

Admin memilih Cooperative, Blueprint, Domain, Capacity dan Modules. ACCC kemudian menjalankan pipeline berikut:

1. Provision VPS.
2. Harden operating system dan firewall.
3. Establish private VPN.
4. Install runtime.
5. Deploy KOARGO Golden Template.
6. Create database dan encryption secrets.
7. Configure Redis, queue dan scheduler.
8. Verify domain dan issue SSL.
9. Register Node Agent.
10. Configure encrypted backup.
11. Run automated tests.
12. Create initial administrator dan activate system.

Golden Template merangkumi authentication, RBAC, membership, audit, notification, API, finance framework, document framework, module manager, queue, scheduler, backup agent, monitoring agent, NeuralOps connector, installer dan update manager.

1.7 6. Deployment Blueprint

Blueprint	Compute	RAM	Storage	Baseline
Small	2-4 vCPU	4 GB	80-100 GB	1-2 workers, daily backup
Standard	4 vCPU	8 GB	150 GB	2-4 workers, weekly snapshot
Enterprise	8 vCPU	16 GB	250-500 GB	4-8 workers, offsite backup
Large Enterprise	12-16 vCPU	32 GB	500 GB-1 TB	8-16 workers, object storage

Deployment sangat besar boleh memisahkan application, database dan object storage sambil kekal sebagai satu isolated franchise environment.

1.8 7. Domain dan Portal

ACCC menyokong managed subdomain, customer subdomain, full customer domain dan wildcard sub-sites. Customer domain perlu membuktikan ownership menggunakan DNS TXT token sebelum SSL dan routing diaktifkan.

Satu koperasi boleh mempunyai portal awam, ahli, shop, vendor dan admin. Wildcard domain membolehkan sub-site ahli diwujudkan tanpa perubahan DNS manual bagi setiap site.

1.9 8. Operations dan System Health

KOARGO Node Agent memantau CPU, RAM, disk, application health, database connectivity dan latency, Redis, queue, scheduler, backup, SSL, version, error rate dan network latency.

System Health Score menggabungkan infrastructure, security, backup, software version, configuration dan availability. Alert boleh membuka maintenance ticket, mencadangkan pembetulan atau menjalankan auto-remediation bagi perubahan low-risk yang telah diluluskan.

Capacity Agent menjangka tarikh resource akan habis dan mencadangkan perubahan compute, RAM, workers atau storage. Cadangan tersebut menjadi input operasi dan peluang infrastructure upsell, bukan perubahan automatik tanpa approval.

1.10 9. Security dan Privileged Access

ACCC ialah Tier-0 infrastructure. Semua administrative access melalui authorised device, VPN, identity, MFA, device verification dan bastion/PAM.

Tidak dibenarkan:

- Internet terus ke ACCC SSH.
- Internet terus ke ACCC database.
- Internet terus ke private admin backend.
- Developer terus ke customer database.

Temporary access mempunyai target, purpose, duration, approver, session log dan auto-revocation. Break-glass memerlukan dua authorised persons, MFA, documented reason, short expiry dan full audit.

1.11 10. Release, Backup dan Disaster Recovery

Software release bergerak melalui internal test, canary, lima pilot cooperatives, 20 peratus, 50 peratus dan 100 peratus. Rollout berhenti dan rollback dimulakan apabila error threshold dilanggar.

Service Tier	RPO	RTO	Restore Test Baseline
Standard	24 jam	8 jam	Quarterly
Enterprise	6 jam	4 jam	Monthly
Mission Critical	1 jam	1-2 jam	Monthly

Backup success sahaja tidak mencukupi. ACCC mesti merekod tarikh restore test terakhir, outcome dan corrective action.

1.12 11. NeuralOps

Flow utama ialah Request, Deterministic Logic, Parser, Detached System, Small Model dan LLM. LLM hanya digunakan apabila reasoning diperlukan.

Heavy model dikendalikan pada private NeuralOps server melalui VPN. Logical agents merangkumi Infrastructure, Deployment, Security, Backup, Support, Billing, Compliance, Domain, Capacity, Release, Sales Opportunity dan Documentation.

Majoriti agents menggunakan rule, parser, event, scheduler dan queue. Ia bukan 12 LLM yang berjalan tanpa henti.

1.13 12. Infrastructure ACCC

Cadangan baseline awal:

- 8-12 vCPU, 32 GB RAM dan 500 GB NVMe.
- Laravel, PostgreSQL, Redis, Laravel Queue dan Nginx.
- Private VPN dan firewall default deny.
- Encrypted offsite backup.
- Independent monitoring.

Apabila skala meningkat, application, database, Redis/queue, monitoring dan backup dipisahkan kepada failure domain masing-masing. Logical access plane kekal satu, tetapi VPN dan access gateway boleh redundant.

1.14 13. Commercial Management

Setiap deployment ialah commercial unit. ACCC merekod package, monthly fee, add-ons, AI entitlement, infrastructure fee, storage fee, support tier, contract, renewal dan outstanding balance.

Portfolio analytics merangkumi MRR, ARR, revenue per cooperative, infrastructure cost, AI cost, support cost, gross margin, outstanding invoices dan renewal forecast. Module gap dan capacity pressure boleh ditanda sebagai peluang upsell dengan human review.

1.15 14. Roadmap

Fasa	Tempoh Indicative	Deliverables Utama
1 ACCC Core	Bulan 1-3	Auth, registry, subscription, billing, audit
2 Deployment Engine	Bulan 3-6	Template, blueprint, provisioning, domain, SSL
3 Operations	Bulan 5-8	Agent, monitoring, backup, health, drift
4 Commercial	Bulan 7-10	Contract, renewal, analytics, margin, upsell
5 NeuralOps	Bulan 9-13	Agents, private gateway, routing, observability
6 Advanced Automation	Bulan 12-18	Prediction, remediation, canary, multi-node

1.16 15. Anggaran Perancangan

Scope	Indicative Build Budget
Foundation, Fasa 1-2	RM280,000-RM420,000
Operational Platform, Fasa 1-4	RM620,000-RM950,000
Full ACCC + NeuralOps, Fasa 1-6	RM1,100,000-RM1,800,000

Julat ini bukan sebut harga muktamad. Ia tidak termasuk SST, per-node cloud usage, domain, lesen pihak ketiga, GPU hardware, major legacy-data cleansing, independent certification dan perubahan skop. Discovery perlu menghasilkan backlog, acceptance criteria, security threat model, delivery team, vendor quotation dan total cost of ownership sebelum kontrak build.

1.17 16. Target Scale dan Outcome

Architecture disasarkan untuk 10-30 koperasi pada Phase 1, 30-100 pada Phase 2, 100-500 pada Phase 3 dan 500-1,000+ pada Phase 4.

Outcome strategik ialah recurring revenue, faster deployment, lower support cost, standardisation, simpler migration dan offboarding, reduced

central data risk serta customer retention melalui nilai operasi, bukan data lock-in.

1.18 17. Keputusan Diperlukan

AINNA mencadangkan kelulusan untuk menjalankan discovery dan architecture validation sebelum build. Discovery perlu mengesahkan operating model, legal entities, PDPA roles, data classification, cloud vendors, SLA tiers, integration inventory, initial pilot cooperatives, commercial packages dan governance board.

1.19 Kesimpulan

ACCC bukan sekadar administrative dashboard. Ia ialah deployment engine, operations centre, infrastructure manager, commercial platform, security control plane dan NeuralOps management layer bagi A Managed Digital Cooperative Network.

Centralised Management. Isolated Infrastructure. Decentralised Data Ownership. Intelligent Operations.

2 ACCC TECHNICAL SPECIFICATION

2.1 1. Architecture Boundaries

- ACCC is the control plane; KOARGO nodes are isolated execution planes.
- Every production cooperative has a dedicated security boundary and database.
- Management traffic traverses a private VPN fabric.
- Public traffic terminates at each node's approved domain/SSL gateway.
- ACCC stores telemetry and management metadata only by default.

2.2 2. Core Components

Component	Baseline Technology	Responsibility
ACCC Web/API	Laravel	Registry, workflow, commercial and control UI
Primary Data	PostgreSQL	ACCC metadata and immutable audit references
Cache/Queue	Redis + Laravel Queue	Cache, jobs, events and deployment orchestration

Component	Baseline Technology	Responsibility
Reverse Proxy	Nginx	TLS termination and application routing
Private Network	WireGuard or equivalent	Management plane connectivity
Node Agent	Signed lightweight service	Metrics, heartbeat and approved remote actions
Object Storage	S3 compatible	Encrypted artifacts and backup metadata
NeuralOps Gateway	Private API	Policy, routing, model access and cost controls

2.3 3. Minimum Domain Model

- cooperatives, contacts, contracts and subscriptions.
- systems, deployments, nodes, environments and blueprints.
- domains, DNS verifications and certificates.
- modules, entitlements, versions and release rings.
- health checks, metrics, alerts and incidents.
- backups, restore tests, RPO/RTO policies and retention.
- access requests, approvals, sessions and revocations.
- invoices, cost allocations, margin snapshots and renewals.
- support tickets, development requests and change orders.
- audit events with actor, target, before/after, reason and outcome.

2.4 4. Node Agent Contract

The agent must authenticate using a unique node identity, rotate credentials, sign payloads, enforce a command allowlist and reject unsigned actions. Heartbeat payloads must exclude customer records. Remote actions must be idempotent, timeout-bound, policy-authorised and audited.

Example allowed payload fields: cooperative_id, system_id, agent_version, app_version, health state, CPU, RAM, disk, database connectivity, latency, queue depth, certificate expiry, backup result and timestamp.

2.5 5. Security Controls

- MFA and device-aware identity for privileged users.
- RBAC plus approval workflow for sensitive actions.
- Bastion/PAM for temporary server access.

- Default-deny firewall and no public database ports.
- Secrets in a managed vault, never in source control.
- Encryption in transit and at rest.
- Append-only audit export to an independent store.
- Vulnerability management, patch policy and signed releases.
- Break-glass under dual control with short expiry.
- Annual penetration test and recurring restore drills.

2.6 6. Availability and Recovery

The access plane is logically singular but may use redundant VPN gateways and application instances. Monitoring must remain independent from the monitored ACCC stack. Backup copies require a separate account or failure domain. Production recovery must be proven through scheduled restore tests.

2.7 7. Deployment and Release

Provisioning should use an infrastructure-as-code provider abstraction. Every build is derived from a versioned Golden Template and produces an evidence bundle: template version, configuration checksum, test result, domain verification, certificate, backup policy and activation approval.

Release rings: internal, canary, pilot, 20%, 50% and 100%. Rollout gates include error rate, latency, failed jobs, health score and business acceptance. Rollback artifacts must be prepared before rollout.

2.8 8. Non-Functional Acceptance Baseline

- All privileged actions are attributable and auditable.
- No customer database is reachable from the public internet.
- A compromised node cannot authenticate as another node.
- ACCC unavailability does not stop core KOARGO transactions already running locally.
- Node telemetry contains no customer personal or financial records by default.
- Backup and restore evidence is reportable per cooperative.
- Pilot deployment is repeatable without manual server configuration.
- Mobile and desktop admin interfaces meet agreed accessibility criteria.

2.9 9. Open Decisions for Discovery

Confirm cloud providers, Malaysian data residency requirements, PDPA controller/processor roles, certificate authority, VPN technology, secrets manager, SIEM destination, monitoring stack, supported OS versions,

KOARGO runtime baseline, legacy migration scope, billing integration and target SLA.

3 ACCC ROADMAP, TEAM AND COST ASSUMPTIONS

3.1 Delivery Model

Recommended delivery uses six gated phases across an indicative 12-18 months. Security architecture, data classification and pilot acceptance criteria must be approved before production rollout.

3.2 Phase Plan

Phase	Indicative Window	Exit Gate
ACCC Core	Month 1-3	Registry, auth, MFA, audit and commercial records accepted
Deployment Engine	Month 3-6	Pilot node reproducibly deployed from Golden Template
Operations	Month 5-8	Agent, alerts, backups and health score proven
Commercial	Month 7-10	Contract, invoice, cost and renewal workflows accepted
NeuralOps	Month 9-13	Private routing and initial agents meet policy controls
Advanced Automation	Month 12-18	Canary, rollback, prediction and safe remediation proven

3.3 Indicative Team

- Product owner / cooperative operations lead.
- Solution architect / security architect.
- Two to four Laravel engineers.
- Platform / DevOps engineer.
- Frontend and UX engineer.
- QA automation engineer.

- Data / integration engineer as needed.
- NeuralOps engineer from Phase 5.
- Project governance, finance and legal stakeholders part-time.

3.4 Budget Bands

Option	Included Scope	Indicative Budget
Foundation	Phases 1-2	RM280,000-RM420,000
Operational Platform	Phases 1-4	RM620,000-RM950,000
Full ACCC + NeuralOps	Phases 1-6	RM1,100,000-RM1,800,000

These are planning bands, not a supplier quotation. They exclude SST, per-cooperative cloud charges, domains, third-party licences, GPU hardware, major data migration, formal certification, travel and material scope change.

3.5 Recurring Cost Categories

- ACCC compute, database, backup and independent monitoring.
- VPN gateways, bastion/PAM and secrets management.
- Per-node VPS, object storage, traffic and snapshots.
- Email, SMS, WhatsApp and payment integration usage.
- NeuralOps GPU or inference usage.
- Security testing, support coverage and on-call operations.

3.6 Commercial Gate Before Build

Discovery should produce a fixed scope or prioritised backlog, delivery schedule, named acceptance criteria, risk register, threat model, data-processing roles, pilot list, vendor quotations, staffing plan and five-year total cost of ownership.

3.7 Recommended First Release

Start with ACCC Core plus Deployment Engine and three to five pilot cooperatives. Defer broad AI automation until telemetry quality, operational runbooks and deployment repeatability have been proven.