CONFIDENTIAL — INSTITUTIONAL DISTRIBUTION ONLY
SA AI Policy GG No.54477 Aligned · Version 2.0 · April 2026

UDOC

UNIFIED DIGITAL OVERSIGHT & COORDINATION

Full Technical Whitepaper

Software Development · Hardware Deployment · Quantum-Ready Architecture

AES-256 + PQC Quantum-Ready Encryption	**99.95%** Uptime SLA (Gov Backbone)	**ZERO** Foreign Cloud Dependency
<50ms Governance Latency	**10-Year** Immutable Audit Retention	**GG54477** SA AI Policy Aligned

Sashin J. Singh
Founder & Systems Architect · G.O.D.S Holdings (Pty) Ltd
info@gods.systems · www.gods.systems · Johannesburg · 2026

TABLE OF CONTENTS

Full Technical Whitepaper v2.0

SECTION 01

EXECUTIVE SUMMARY

Platform identity, mandate, and key technical metrics

UDOC — Unified Digital Oversight & Coordination — is not a software product. It is sovereign digital governance infrastructure: the technical backbone allowing governments and regulated enterprises to govern AI systems, protect national data sovereignty, and generate independently auditable compliance records without dependency on foreign-owned cloud platforms. This whitepaper provides the complete technical specification for software development, hardware deployment, and quantum-ready security architecture — aligned to South Africa's Draft National AI Policy (Government Gazette No.54477, 10 April 2026).

"AI governance must be technically embedded into the infrastructure stack — impossible to bypass by policy alone."

Metric	Value	Notes
Platform Type	Sovereign AI Governance Infrastructure	Not SaaS — infrastructure-grade
Primary Stack	Python/FastAPI + Node.js + PostgreSQL + Kafka	Polyglot microservices
Frontend	React 18 / TypeScript / Vite + Tailwind	Constitutional dashboard
Database	PostgreSQL 16 + Cassandra 5 + Redis 7	ACID + Immutable + Cache
Event Streaming	Apache Kafka 3.x — 5 brokers minimum	Tamper-evident event log
Encryption (Phase 1)	AES-256-GCM + HMAC-SHA256	All data at rest and transit
Encryption (Phase 2)	CRYSTALS-Kyber (FIPS 203) + Dilithium (FIPS 204)	NIST PQC — Q3 2026
Uptime SLA — Enterprise	99.9% (max 8.76h downtime/year)	Multi-zone redundancy
Uptime SLA — Gov Backbone	99.95% (max 4.38h downtime/year)	Dual-site + HA edge
Governance Latency	<50ms synchronous path overhead	Policy engine on NVMe workers
Audit Retention	10 years minimum — Cassandra WORM	Cassandra append-only cluster
Data Sovereignty	100% ZA jurisdiction — architecturally enforced	No foreign cloud at any tier
SA Policy Alignment	GG No.54477 — All 6 pillars mapped	10 April 2026 — 86 pages
HSM Standard	FIPS 140-3 Level 3 — government backbone	Dual HSM per site
Recovery Point Obj.	1-hour RPO — government backbone	Continuous WAL archiving
Recovery Time Obj.	4-hour RTO — platform level	Pre-validated DR runbooks

SECTION 02

PLATFORM VISION & DESIGN PHILOSOPHY

Five non-negotiable architectural principles

UDOC's architecture is governed by five design principles that are non-negotiable across all deployments and cannot be overridden by commercial or operational considerations.

SOVEREIGNTY FIRST	No client data traverses infrastructure not under client legal control. This is technically enforced at the hardware layer — not contractually promised. Constitutional Pillar III.
AUDIT BY DEFAULT	Every system event produces a cryptographically verifiable, tamper-evident record. Audit is not optional. It is the default behaviour of every component. Constitutional Pillar VI.
ZERO TRUST	No component trusts any other without continuous verification. mTLS mandatory for all inter-service traffic in sovereign deployments. Every identity verified continuously.
QUANTUM-READY	All cryptographic primitives are NIST PQC-compliant from inception. CRYSTALS-Kyber and CRYSTALS-Dilithium deployed in Phase 2. Hybrid TLS 1.3 transition architecture active.
INTEROPERABLE	All interfaces publish to open standards. No proprietary lock-in. EU AI Act, POPIA, NIST AI RMF, ISO 42001, OECD AI Principles, UNESCO AI Ethics — all frameworks supported natively.

2.1 Four Deployment Models

Model	Primary Use	Sovereignty Level	Min. Footprint
National Backbone	Govt-wide AI oversight — identity, welfare, border, justice	MAXIMUM	Two sites + secure build/signing enclave
Sovereign Cloud	Regulated industries, parastatals, provincial programmes	HIGH	One primary + one DR site. In-country operator.
Private Enterprise	Banks, insurers, hospitals, utilities, large enterprises	HIGH	One primary cluster + backup target
Edge Governance Node	Agency, ministry, OT/edge, disconnected field system	TARGETED	1–3 appliances per site. Store-and-forward.

SECTION 03

SOFTWARE ARCHITECTURE OVERVIEW

Seven-layer platform architecture — complete component map

The UDOC software platform is a multi-application monorepo comprising a FastAPI Python governance backend, a Node.js legacy MVP, a React TypeScript dashboard, Kubernetes manifests, Prometheus monitoring configuration, and infrastructure-as-code. All components operate under the constitutional mandate throughout the full software delivery path.

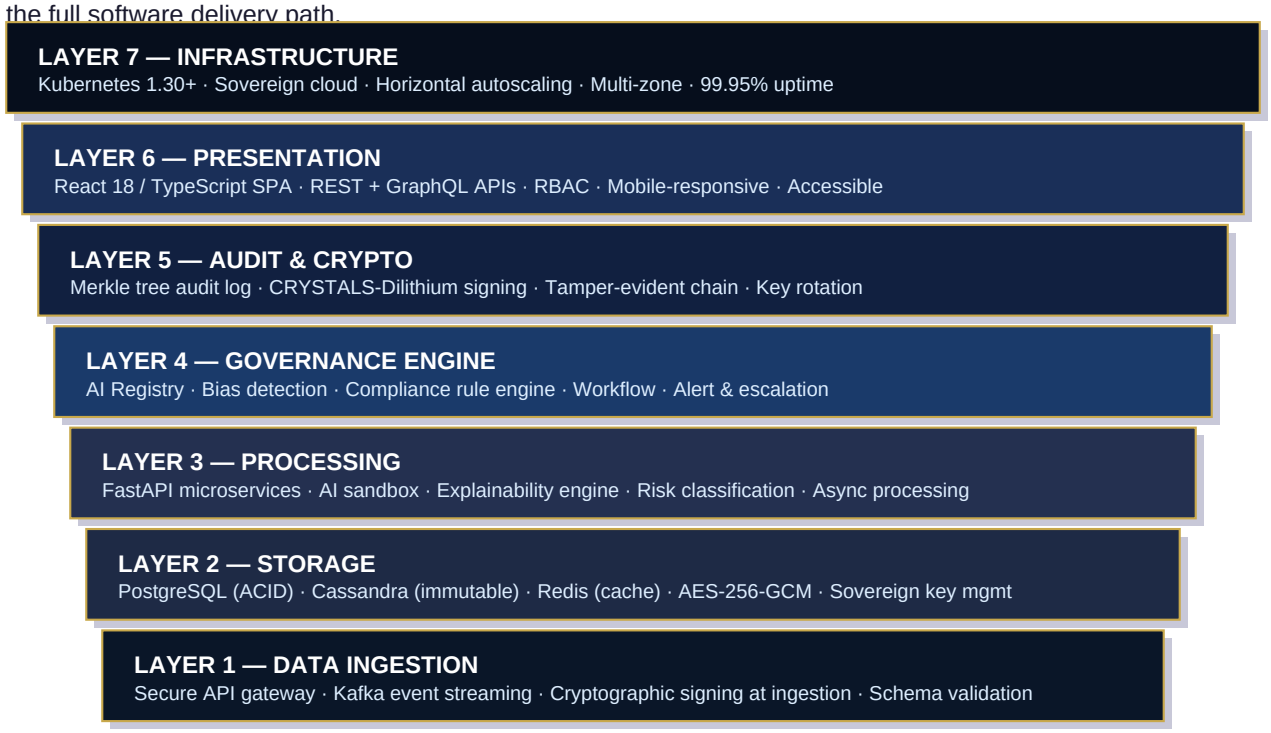

Figure 1 — UDOC Seven-Layer Platform Architecture. Data flows upward through layers; governance controls flow downward. All layers operate within ZA sovereign jurisdiction.

3.1 Technology Stack Specification

Component	Technology	Version	Justification
API Framework (Primary)	Python / FastAPI	0.111+	Async performance · Type safety · OpenAPI auto-docs · Pydantic validation
API Framework (Legacy MVP)	Node.js / Express	18+ / 4.x	Phase 1 MVP · Same language across all division backends
Frontend Framework	React / TypeScript	18.x	Component reuse · Type safety · Government audit trail UI · Vite build
Primary Database	PostgreSQL	16.x	ACID compliance · Row-level security · Audit extension · ZA sovereign hosting
Audit Log Store	Apache Cassandra	5.x	Immutable write · Horizontal scale · 10-year retention · WORM pattern
Event Streaming	Apache Kafka	3.x	Tamper-evident log · Event replay · Compliance trail · Fan-out delivery
Cache / Queue	Redis	7.x	Session management · Rate limiting · Temporary data isolation · Queue
Search & Analytics	OpenSearch	2.x	Full-text audit search · Compliance dashboards · Alerting
Orchestration	Kubernetes	1.30+	Sovereign cloud portability · Autoscaling · Zero-downtime deploy
Service Mesh	Envoy / Istio	Latest	mTLS enforcement · Traffic management · Observability

Component	Technology	Version	Justification
Monitoring	Prometheus + Grafana	Latest	Real-time SLA monitoring · Anomaly detection · Constitutional alerting
CI/CD	GitLab CI / ArgoCD	Latest	Air-gapped deployment · GitOps · Compliance pipeline · Signed releases
ORM	SQLAlchemy + Alembic	2.x	Type-safe database access · Migration management · Schema versioning
Authentication	JWT + bcryptjs + mTLS	Latest	Stateless · RBAC · 8-hour sessions · Government: mutual TLS
Schema Validation	Pydantic v2	2.x	Input validation · Type enforcement · OpenAPI generation
Logging	Winston (Node) / structlog (Python)	Latest	Structured JSON · Feeds UDOC audit trail · ZA sovereignty metadata
Scheduling	node-cron / APScheduler	Latest	Compliance sweeps · Bias scans · Sovereignty checks
Testing	Jest + Supertest (Node) / pytest (Python)	Latest	Unit + integration · Coverage for investor due diligence
Container Runtime	Docker + Docker Compose	Latest	Local dev parity · Production: Kubernetes on ZA sovereign cloud
Policy Engine	OPA / Rego	Latest	Policy-as-code · Hot-reload <5ms evaluation · COB sign-off workflow
PQC Library (Phase 2)	liboqs / Open Quantum Safe	Latest	NIST PQC · Kyber + Dilithium + SPHINCS+ · Hybrid TLS 1.3

SECTION 04

BACKEND DEVELOPMENT STACK

Directory structure, configuration, and dependency management

4.1 Monorepo File Structure

The UDOC platform is organised as a monorepo (udoc_platform/) with clear separation between the FastAPI primary backend, the Node.js legacy MVP, the React frontend, infrastructure manifests, and documentation. All components share a common CI/CD pipeline and can be deployed independently.

Path	Type	Description
apps/api/	FastAPI Backend	Python 3.11 · Core governance engine · 12 router modules
apps/api/app/main.py	Entry Point	FastAPI app factory · Middleware registration · Lifespan events
apps/api/app/routers/	API Routers	12 domain routers — auth, audit, bias, compliance, decisions, registry, sovereignty, oversight,
apps/api/app/services/	Services Layer	10 service classes — audit, bias, compliance, explainability, risk engine, sovereignty, lineage,
apps/api/app/db/	Database Layer	SQLAlchemy models · Session management · Alembic migrations · Connection pooling
apps/api/app/schemas/	Pydantic Schemas	auth.py · decisions.py · registry.py · workforce.py · All request/response models
apps/api/app/core/	Core Config	security.py · settings.py · JWT config · RBAC definitions · Constitutional constants
apps/api/tests/	Test Suite	pytest · Unit tests for audit service, explainability, risk engine · Integration tests
apps/legacy-node-mvp/	Node.js MVP	Express backend · Phase 1 MVP · Retained for reference · Being superseded by FastAPI
apps/legacy-node-mvp/routes/	Node Routers	7 Express routers — auth, audit, bias, compliance, sovereignty, systems, admin
apps/legacy-node-mvp/jobs/	Cron Jobs	3 jobs — biasScan.js (24h) · complianceSweep.js (02:00 daily) · sovereigntyCheck.js (6h)
apps/legacy-node-mvp/middleware/	Middleware	auth.js (JWT RBAC) · auditLog.js (all admin actions logged tamper-evident)
apps/legacy-node-mvp/db/	DB Layer	PostgreSQL connection pool · 001_initial_schema.sql — 10 tables · Immutable audit rules
apps/web/	React Frontend	React 18 · TypeScript · Vite · Tailwind CSS · Browser dashboard
apps/web/src/App.tsx	Root Component	Route definitions · Auth context · Constitutional header enforcement
apps/web/src/api.ts	API Client	Typed API calls · JWT token management · Error handling · Retry logic
apps/web/src/types.ts	TypeScript Types	All domain types — AISystem, AuditEvent, BiasResult, ComplianceSweep, etc.
apps/mainframe/	Admin Mainframe	G.O.D.S Admin UI · Standalone HTML · Internal governance command interface
apps/udoc-demo/	Demo MVP	UDOC Demo HTML · Investor/government interactive demonstration
infrastructure/k8s/	Kubernetes	YAML manifests — namespace · API deployment · Web deployment · Services · Ingress
infrastructure/monitoring/	Observability	Prometheus scrape config · Grafana dashboards · Alert rules · SLA monitors
docker-compose.yml	Dev Environment	Full-stack local — PostgreSQL + Redis + Kafka + API + Web + Prometheus
docs/	Documentation	architecture_alignment.md · api_surface.md · implementation_scope.md · ADRs

4.2 Core Dependency Manifests

FastAPI Backend — requirements.txt (Python 3.11)

Package	Version	Purpose
fastapi	>=0.111.0	Primary async web framework — OpenAPI auto-generation
uvicorn[standard]	>=0.30.0	ASGI server — production deployment with auto-reload
sqlalchemy	>=2.0.0	ORM — type-safe database access · PostgreSQL dialect
alembic	>=1.13.0	Database migrations — schema versioning · rollback support
asyncpg	>=0.29.0	Async PostgreSQL driver — non-blocking DB operations
psycopg2-binary	>=2.9.9	Sync PostgreSQL driver — Alembic migrations
redis	>=5.0.0	Redis client — session management · rate limiting · cache
aiokafka	>=0.10.0	Async Kafka client — event streaming · audit log submission
cassandra-driver	>=3.29.0	Cassandra client — immutable audit log · WORM storage
pydantic	>=2.5.0	Data validation — request/response schemas · settings
pydantic-settings	>=2.0.0	Environment-based configuration management
python-jose[cryptography]	>=3.3.0	JWT creation and verification · RS256/HS256
passlib[bcrypt]	>=1.7.4	Password hashing — bcrypt cost factor 12
cryptography	>=42.0.0	AES-256-GCM encryption · HMAC-SHA256 signing
httpx	>=0.27.0	Async HTTP client — inter-service communication
structlog	>=24.0.0	Structured logging — JSON output · sovereignty metadata
prometheus-client	>=0.20.0	Metrics exposure — Prometheus scraping
python-multipart	>=0.0.9	File upload support — document vault integration
oqs	>=0.9.0	Open Quantum Safe — liboqs Python bindings (Phase 2)
pytest	>=8.0.0	Test framework — unit + integration tests
pytest-asyncio	>=0.23.0	Async test support — FastAPI endpoint testing
httpx	>=0.27.0	Test client for FastAPI — replaces TestClient for async

Node.js Legacy MVP — package.json dependencies

Package	Version	Purpose
express	^4.18.0	HTTP server framework — routing · middleware · security headers
pg	^8.11.0	PostgreSQL client — connection pooling · parameterised queries
jsonwebtoken	^9.0.0	JWT token creation and verification — 8-hour sessions
bcryptjs	^2.4.3	Password hashing — bcrypt cost factor 12
helmet	^7.0.0	Security headers — HSTS · CSP · X-Frame-Options · constitutional headers

Package	Version	Purpose
express-rate-limit	^7.0.0	Rate limiting — per-route quotas · DDoS protection
winston	^3.11.0	Structured JSON logging — sovereignty metadata on all entries
node-cron	^3.0.3	Scheduled jobs — compliance sweeps · bias scans · sovereignty checks
joi	^17.11.0	Schema validation — all API inputs · SQL injection prevention
cors	^2.8.5	CORS configuration — controlled origin allow-list
compression	^1.7.4	Response compression — bandwidth optimisation
morgan	^1.10.0	HTTP request logging — feeds Winston structured log
dotenv	^16.3.0	Environment variable management — .env file loading
redis	^4.6.0	Redis client — session management · rate limit counters

SECTION 05

FASTAPI GOVERNANCE ENGINE — FULL SPECIFICATION

All 12 API routers, 10 service classes, and middleware chain

5.1 API Router Specification

Router	Module	Method/Path	Auth Level	Constitutional Function
Auth	auth.py	`POST /auth/token`	Public	JWT login · Token refresh · Session creation
Auth	auth.py	`POST /auth/refresh`	Bearer token	Token rotation · Session extension
Auth	auth.py	`POST /auth/revoke`	Bearer token	Immediate session invalidation · Audit logged
Registry	registry.py	`GET /registry/systems`	OPERATOR+	List all governed AI systems with compliance summary
Registry	registry.py	`POST /registry/systems`	OPERATOR+	Register new AI system — validates Pillar VIII for HIGH RISK
Registry	registry.py	`GET /registry/systems/{id}`	OPERATOR+	System detail + compliance + bias + sovereignty summary
Registry	registry.py	`PATCH /registry/systems/{id}`	ADMIN+	Update system record — logged to constitutional audit trail
Registry	registry.py	`DELETE /registry/systems/{id}`	ADMIN+	Suspend system — COB notified for HIGH RISK
Decisions	decisions.py	`POST /decisions/`	SERVICE	Submit AI decision — hash input · sign output · lineage stamp
Decisions	decisions.py	`GET /decisions/{id}`	OPERATOR+	Retrieve decision with full explainability output
Decisions	decisions.py	`GET /decisions/{id}/verify`	PUBLIC	Cryptographic verification of audit record — Merkle proof
Audit	audit.py	`GET /audit/events`	OPERATOR+	Query immutable audit trail — filtered by system/date/type
Audit	audit.py	`POST /audit/events/{id}/review`	OPERATOR+	Mark event as human reviewed — Pillar VIII compliance
Audit	audit.py	`GET /audit/merkle/root`	OPERATOR+	Current Merkle root hash — independent verification
Audit	audit.py	`POST /audit/export`	ADMIN+	Generate signed evidence bundle — JSON-LD/PDF/XML
Compliance	compliance.py	`POST /compliance/check`	ADMIN+	Run full compliance check across all active frameworks
Compliance	compliance.py	`GET /compliance/report/{id}`	OPERATOR+	Generate compliance report — SA AI Policy + 8 other frameworks
Compliance	compliance.py	`GET /compliance/frameworks`	OPERATOR+	List all active regulatory frameworks with scoring config
Bias	bias.py	`POST /bias/scan`	ADMIN+	Trigger SPD analysis — 6 protected characteristics
Bias	bias.py	`GET /bias/scans/{id}`	OPERATOR+	Retrieve bias scan results with threshold comparison
Bias	bias.py	`GET /bias/alerts`	OPERATOR+	Active bias flags — SAHRC escalation status
Oversight	oversight.py	`GET /oversight/queue`	ADMIN+	Human review queue — flagged decisions requiring review
Oversight	oversight.py	`POST /oversight/review`	ADMIN+	Submit human review decision — logged with reviewer ID
Lineage	lineage.py	`GET /lineage/{system_id}`	OPERATOR+	Full data provenance chain — source to decision Merkle-linked
Sovereignty	sovereignty.py	`GET /sovereignty/status`	OPERATOR+	ZA jurisdiction verification · Encryption status · Foreign check
Sovereignty	sovereignty.py	`POST /sovereignty/verify`	ADMIN+	Trigger immediate sovereignty verification across all nodes
Workforce	workforce.py	`GET /workforce/`	SETHS_HEAD+	S.E.T.H.S participant employment outcome data — anonymised
Workforce	workforce.py	`POST /workforce/`	SETHS_HEAD+	Submit workforce outcome record — compounding loop data

Router	Module	Method/Path	Auth Level	Constitutional Function
Admin	admin.py	`GET /admin/users`	SUPER_ADMIN	List all platform users across all divisions
Admin	admin.py	`PUT /admin/users/{id}/role`	SUPER_ADMIN	Update user role — logged · no single actor dual control
Admin	admin.py	`GET /admin/config`	SUPER_ADMIN	Platform configuration — sovereignty settings · thresholds
Health	health.py	`GET /health`	None	Platform health · Sovereignty status · Kubernetes liveness probe
Health	health.py	`GET /health/ready`	None	Readiness probe — DB + Kafka + Redis connected
Health	health.py	`GET /health/live`	None	Liveness probe — process alive · constitutional headers injected

5.2 Services Layer — Full Specification

Service	Module	Key Functions
Audit Service	audit_service.py	HMAC-SHA256 signing of all AI decision events · Cassandra append-only write · Merkle root computat
Bias Service	bias_service.py	Statistical Parity Difference (SPD) calculation across 6 protected characteristics · Counterfactual testin
Compliance Service	compliance_service.py	SA AI Policy GG54477 pillar sweep (6 pillars) · EU AI Act Articles 9,13,14,17,18,29 · POPIA Section 26
Explainability	explainability.py	LIME/SHAP-based feature attribution for model decisions · Plain-language output for affected citizens
Risk Engine	risk_engine.py	SA AI Policy risk classification — PROHIBITED/HIGH/MEDIUM/LOW · EU AI Act taxonomy alignment
Sovereignty Service	sovereignty_service.py	Cryptographic proof of ZA data localisation · Network egress monitoring — foreign connection detectio
Lineage Service	lineage_service.py	Merkle-linked provenance chain from data source to decision output · Data lineage tag assignment at i
Workforce Service	workforce_service.py	S.E.T.H.S participant outcome data governance · Employment placement tracking in UDOC audit cont
Event Bus	event_bus.py	Kafka producer/consumer integration · Topic routing by jurisdiction, client, risk class, functional stream
PQC Service	pqc.py	CRYSTALS-Kyber (FIPS 203) key encapsulation for TLS session and data encryption keys (Phase 2)

5.3 Middleware Chain

Middleware	Order	Implementation	Purpose
CORS	1	fastapi.middleware.cors.CORSMiddleware	Controlled origin allow-list · No wildcard in production
Security Headers	2	Custom middleware	X-UDOC-Sovereignty · X-UDOC-Constitutional · X-UDOC-Version · HSTS · C
Request ID	3	Custom middleware	UUID injection into every request · Correlates all log entries for audit trail
Rate Limiting	4	slowapi (FastAPI) / express-rate-limit (Node)	Per-route quotas · Burst allowance for compliance exports · Government back
Authentication	5	JWT verification + RBAC	Stateless JWT validation · Role extraction · Minimum privilege enforcement · 8
Audit Log	6	Custom middleware	All admin actions logged to platform_audit_log before handler executes · HMA
Sovereignty Check	7	Custom middleware on sensitive routes	Verifies request originates from ZA jurisdiction for SOVEREIGN-CRITICAL dat
Constitutional Headers	8	Response middleware	Injects constitutional compliance evidence headers on every API response for

SECTION 06

DATABASE ARCHITECTURE & SCHEMA

PostgreSQL governance state · Cassandra immutable audit · Multi-tier data model

6.1 PostgreSQL Schema — All Tables

Table	Module	Key Fields	Retention	POPIA Classification
ai_systems	UDOC Core	id, name, risk_tier, owner_org, compliance_status, hitl_pathway, registered_at	Indefinite (active)	Non-personal operational data
audit_events	UDOC Core	id (UUID), system_id, actor, action_type, outcome, confidence, input_hash, prev_hash, jurisdiction, pil	10 years MINIMUM — IMMUTABLE	May contain PI — AES-256 encrypted
compliance_checks	Compliance	id, system_id, framework, score, issues_json, remediation_status, checked_at, checked_by	7 years	Operational metadata
compliance_frameworks	Compliance	id, name, version, min_threshold, weight, active, sa_policy_pillar, rules_json	Indefinite	Non-personal config
bias_scans	Bias Engine	id, system_id, characteristic, spd_value, threshold, flagged, escalated_to, case_ref, resolved_at	7 years	Aggregate statistics — no individual PI
bias_thresholds	Bias Engine	id, characteristic, threshold_value, escalation_threshold, alert_email, active	Indefinite	Non-personal config
sovereignty_checks	Sovereignty	id, node_id, jurisdiction, foreign_exposure, encryption_active, verified_at, check_result	7 years	Operational metadata
human_oversight_records	HITL	id, decision_id, system_id, reviewer_id, review_outcome, reason_code, reviewer_signature, reviewed_at, cob_notified	7 years	User IDs only — no special PI
data_lineage_records	Lineage	id, system_id, data_hash, source_system, ingestion_ts, transformations_json, storage_locations, classification, jurisdict	7 years	Operational metadata
conformity_assessments	Registry	id, system_id, assessment_type, assessor, result, findings_json, approved_at, next_due	7 years	Operational data
platform_audit_log	Admin	id, actor_id, actor_role, action, resource, resource_id, ip_address, session_id, timestamp — IMMUTABLE	7 years	User IDs only — no special PI
users	Auth	id, email, password_hash (bcrypt-12), role, division, mfa_secret, last_login, failed_attempts, locked	Employment + 3 years	Personal information — POPIA Section 11
workforce_outcomes	SETHS	cohort_id, participant_anon_ref, placement_status, income_band, retention_30d, retention_90d, reporting_period — AN	Indefinite (anonymised)	None — anonymised aggregate only
evidence_bundles	Audit Export	id, name, type, system_ids, decision_count, merkle_root, dilithium_signature, format, created_at, legal_hold	7-10 years	Operational data

6.2 Cassandra Immutable Audit Pattern

The Cassandra audit cluster is the most critical data store in the platform. It provides the technically-enforceable, append-only guarantee that no audit record can ever be modified or deleted — not by UDOC engineers, not by clients, and not by government. This is the technical foundation of Constitutional Pillar VI (Transparency) and SA AI Policy Pillar 03 (Responsible Governance).

Configuration Item	Value	Rationale
Nodes per site	6 minimum	Replication factor 3 with 2 simultaneous failure tolerance
Replication factor	RF=3 per keyspace	Any 3 nodes hold full copy — node loss is survivable
Compaction strategy	SizeTieredCompactionStrategy (write-heavy)	Immutable data — no updates — SizeTiered optimal
Consistency level reads	LOCAL_QUORUM	At least 2 of 3 local replicas must confirm
Consistency level writes	ALL	All 3 replicas must confirm audit write — maximum durability
Partition key design	(jurisdiction, year_month, system_family)	Bounded partitions · Predictable hotspot avoidance
Clustering columns	event_timestamp DESC, event_id ASC	Time-ordered retrieval · UUID prevents collision
Compression	LZ4 (commitlog) / ZSTD (SSTables)	Balances compression ratio with decompression speed

Configuration Item	Value	Rationale
Commitlog segment size	512 MB	Large segments reduce fsync frequency for write-heavy load
Commitlog sync	periodic (10s) with fsync	Durability with acceptable write latency
Read repair chance	0.0 (disabled for append-only)	Immutable data — read repair is unnecessary overhead
GC grace seconds	864000 (10 days)	Anti-compaction grace — tombstones are not generated
Merkle root computation	Every 15 minutes → PostgreSQL + Object Archive	Daily anchor verification point — published to regulator registry
Retention enforcement	TTL = 10 years minimum (315,360,000 seconds)	Cannot be reduced without unanimous COB vote

6.3 PostgreSQL High Availability Configuration

HA Component	Configuration	Purpose
Cluster topology	1 Primary + 1 Synchronous Standby + 1 Async Witness	RPO near-zero within site · Witness prevents split-brain
Patroni	Patroni 3.x — etcd DCS	Automatic failover orchestration · <30s RTO within site
Replication	Streaming replication — synchronous_commit = on	Zero data loss on primary failure — commit waits for standby ACK
WAL archiving	Continuous to object archive (S3-compatible)	Point-in-time recovery · 35-90 day hot retention
pgBouncer	Connection pooling — transaction mode	Reduces connection overhead · Handles 10K+ concurrent connections
pg_stat_statements	Enabled — slow query threshold 100ms	Query performance monitoring · Anomaly detection
Row Level Security	Enabled on all PI-containing tables	Application-layer access control in DB layer
Audit extension	pgaudit — all DML on audit_events table	Database-level tamper detection — Pillar VI
Snapshots	Storage snapshot every 4 hours	4-hour RPO fallback · Monthly sealed archive copy
Restore test	Monthly restore drill to isolated environment	Validates backup integrity before it is needed

SECTION 07

EVENT STREAMING & KAFKA ARCHITECTURE

Tamper-evident event log · AI decision trail · Compliance fan-out

Apache Kafka is the event streaming backbone of UDOC. Every AI decision event, every lifecycle event (model registration, version change, retirement), and every integration event (bias flag, compliance breach, sovereignty violation) is published to Kafka before being processed. This guarantees that the governance record is created at the moment of the event — not after processing — making it impossible to retroactively suppress governance records.

Topic	Partitions	Retention	Replication	Consumers	Purpose
udoc.decisions.{jurisdiction}	24	30 days + replay	RF=3	Audit service · Bias engine · Compliance engine	Primary AI decision event stream — all governe
udoc.audit.signed	12	7 days	RF=3	Cassandra writer · PostgreSQL metadata · HDAC signer	HDAC-signed audit events ready for immutable
udoc.bias.scans	6	14 days	RF=3	Bias service · Alert service · SAHRC notifier	Bias scan results and SPD threshold breach ev
udoc.compliance.sweeps	6	30 days	RF=3	Compliance service · Regulator portal · COB notifier	Compliance sweep results and framework scor
udoc.sovereignty.checks	3	90 days	RF=3	Sovereignty service · Security monitor · Audit service	Sovereignty verification results — 6-hour
udoc.oversight.queue	6	14 days	RF=3	HITL service · COB notifier · SLA monitor	Decisions queued for mandatory human review
udoc.incidents	3	365 days	RF=3	Incident command · COB · Legal · DCDT portal	Constitutional breach and security incident eve
udoc.lifecycle.{system_id}	12	365 days	RF=3	Registry service · Lineage service · Audit service	AI system lifecycle — registration, versioning, r
udoc.seths.outcomes	6	30 days	RF=3	Workforce service · Impact dashboard · Government	Anonymised S.E.T.H.S participant outcome da
udoc.dlq	6	30 days	RF=3	Operations team · Alert service	Dead letter queue — failed processing events f

Configuration	Value	Rationale
Broker count	5 per primary site	Tolerates 2 simultaneous broker failures while maintaining quorum
Replication factor	RF=3 default	Any 3 of 5 brokers hold full copy — 2 broker loss is survivable
Min insync replicas	min.insync.replicas=2	Producer must acknowledge 2 of 3 replicas — durability guarantee
Producer acks	acks=all	All ISR replicas must confirm before producer receives success
Idempotent producers	enable.idempotence=true	Exactly-once semantics — no duplicate audit events
mTLS authentication	ssl.client.auth=required	Mutual TLS — all producer and consumer connections authenticated
ACL authorisation	authorizer.class.name=AclAuthorizer	Topic-level access control — minimum privilege per service
Log retention bytes	Per topic (see above)	Prevents unbounded disk growth — replay window sized appropriately
Topic deletion	delete.topic.enable=false (governance topics)	Governance event topics are immutable — cannot be deleted
Inter-broker encryption	security.inter.broker.protocol=SSL	All broker-to-broker traffic encrypted — no plaintext internal
Log compaction	Disabled for governance topics	Full history required — compaction would delete events
Mirror MakerV2	Active for cross-site replication	Secondary site receives all governance events in near-real-time

SECTION 08

FRONTEND DEVELOPMENT — REACT DASHBOARD

React 18 / TypeScript / Vite — constitutional governance operator console

8.1 Component Architecture

The UDOC React dashboard is the operator console for governance oversight. It provides real-time visibility into all governed AI systems, bias flags, compliance status, sovereignty verification, and the human oversight queue. It is built mobile-responsive and screen-reader accessible to meet SA government accessibility requirements.

Component	Path	Description
App Root	App.tsx	Route definitions · Auth context provider · Constitutional header enforcement · Error boundary
API Client	api.ts	All typed API calls · JWT token management · Retry with exponential backoff · Error normalisation
Type Definitions	types.ts	AISystem · AuditEvent · BiasResult · ComplianceSweep · HumanOversightRecord · SovereigntyCheck ·
Dashboard	pages/Dashboard.tsx	Command centre · KPI grid · SA Policy pillar scores · Constitutional legitimacy index · Real-time alert str
SA Policy	pages/SAPolicy.tsx	GG54477 alignment · 6 pillar compliance · 3-phase roadmap · Regulatory body engagement status
AI Registry	pages/Registry.tsx	System catalogue · Risk tier heat map · HITL status · HRIA tracking · Suspend/activate controls
Risk Engine	pages/Risk.tsx	Risk tier breakdown · Classification requirements by tier · Quarterly review schedule
Audit Trail	pages/AuditTrail.tsx	Event stream · HMAC verification display · Merkle root status · Signed bundle export · Schema viewer
Compliance	pages/Compliance.tsx	Framework scores across 9 frameworks · GG54477 checklist · System compliance matrix · Sweep sche
Bias Monitor	pages/BiasMonitor.tsx	SPD visualisation · 6 characteristic meters · Active flag management · SAHRC escalation · HRIA status
Explainability	pages/Explainability.tsx	Decision explanation viewer · Plain language output · s33 compliance status · Citizen-facing portal link
HITL Oversight	pages/HumanOversight.tsx	Review queue with SLA countdown · Decision approval/rejection UI · Pathway documentation tracker
Sovereignty	pages/Sovereignty.tsx	Node map · Verification log · Cryptography roadmap · Key architecture diagram
Ethics Board	pages/EthicsBoard.tsx	COB seat management · Review schedule · Independence declaration · SA policy proposed board mapp
Ombudsperson	pages/Ombuds.tsx	Citizen case queue · Decision replay · Counterfactual results · SLA monitoring · s33 RSA compliance
Incident Command	pages/Incident.tsx	INC register · 4-phase response tracker · POPIA notification timer · SAHRC/COB notification log
Regulator Portal	pages/Regulator.tsx	Authority case rooms · Evidence bundle downloads · Access audit log · GG54477 comment submission
S.E.T.H.S	pages/SETHS.tsx	Workforce governance overlay · POPIA data streams · SDG alignment · Pillar 02 evidence
Admin/Config	pages/Config.tsx	Sovereignty settings · Encryption config · SA policy reference · Founder override status (disabled)

8.2 Build Configuration

Config Item	Value / Command
Build tool	Vite 5.x — fastest cold start and HMR
TypeScript config	strict: true · noUncheckedIndexedAccess · exactOptionalPropertyTypes
CSS framework	Tailwind CSS 3.x — JIT mode — all constitutional colour tokens as custom properties
Component library	shadcn/ui — accessible primitives built on Radix UI
Charts	Recharts 2.x — compliance scores · bias SPD meters · KPI trends

Config Item	Value / Command
Production build command	npm run build — outputs to dist/ — tree-shaken · minified
Test command	npm run test — Vitest + Testing Library
Lint	ESLint + TypeScript-eslint — strict config · no-any enforced
Format	Prettier — consistent style across all component files
Environment	.env.local — VITE_API_BASE_URL · VITE_UDOC_VERSION · VITE_SOVEREIGNTY_NODE
Production env	Injected at Kubernetes deploy time — never committed — ConfigMap + Secret
Bundle size target	<400KB initial JS (gzipped) — government network performance
Accessibility target	WCAG 2.1 AA — government deployment requirement

SECTION 09

HARDWARE DEPLOYMENT ARCHITECTURE

National backbone · Sovereign cloud · Private enterprise · Edge governance

The UDOC hardware estate is divided into five functional planes, each with independent performance, storage, and failure-domain requirements. All planes operate within ZA sovereign jurisdiction. No plane has uncontrolled egress to foreign infrastructure. The architecture is designed to make data sovereignty technically impossible to violate — not merely contractually promised.

9.1 Reference Primary Site — 4-Rack Layout

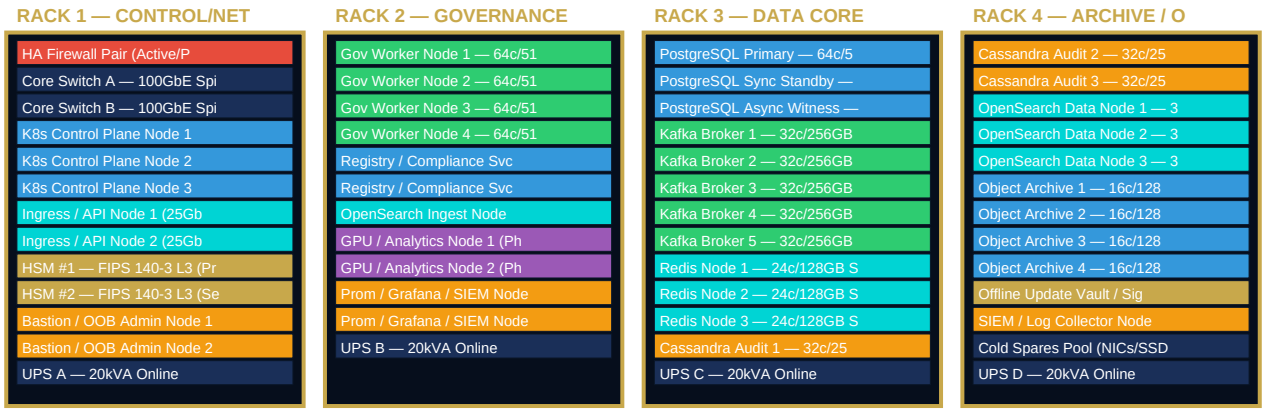

Figure 2 — Reference Primary Site 4-Rack Layout. Secondary site mirrors control, PostgreSQL, Kafka, Cassandra, HSM, and archive at reduced capacity (2–3 racks). Secure build enclave physically separated (1 rack or separate facility).

SECTION 10

FIVE-PLANE HARDWARE STACK

Embedded governance fabric · Ingestion · Processing · Data · Security

Plane	Primary Functions	Hardware Emphasis	Failure Priority
1 — Embedded Governance Fabric	SDK gateways · Sidecars · Host agents · Branch appliances · [illegible]	[illegible]	[illegible] Trusted identity · TPM 2.0
2 — Ingestion & Control Plane	API ingress · mTLS termination · Kafka brokers · Schema regis[illegible]	Fast NVMe · 25/100GbE [illegible]	[illegible] CRITICAL [illegible] latency · Low jitter
3 — Governance & Processing Core	FastAPI services · Policy engine (OPA) · Explainability · Bias engine [illegible]	[illegible]	[illegible] 20-25% headroom reserve[illegible]
4 — Immutable Data Operations Core	PostgreSQL HA · Cassandra WORM audit · Redis cache · OpenSearch full-text [illegible]	[illegible]	[illegible] retention manage[illegible]
5 — Sovereign Security Plane	FIPS 140-3 L3 HSM · HashiCorp Vault · Bastion hosts · SIEM · [illegible]	[illegible]	[illegible] operations · Air-[illegible]

10.1 Kubernetes Control & Worker Configuration

Resource	Control Plane	Governance Workers	Notes
Nodes	3 per site	4–8 per site	Odd count for etcd quorum · Workers scale horizontally
CPU per node	16–24 physical cores	32–64 physical cores	No hyperthreading on control plane
RAM per node	128–192 GB	256–512 GB	etcd is memory-intensive · Workers host all microservices
Storage per node	2×960GB SSD RAID1	4×3.84TB NVMe	Control: OS + etcd · Workers: service data + local buffers
Network per node	Dual 10/25GbE + 1GbE OOB	Dual 25/100GbE	100GbE for high-throughput governance workers
CPU headroom	N/A (control only)	20–25% reserved	Failover and rolling upgrade capacity — never saturate
Pod disruption budget	maxUnavailable: 0	maxUnavailable: 1 per deployment	Control: zero disruption · Workers: rolling safe
Node affinity	control-plane taint enforced	app=governance-worker	No application pods on control plane nodes
Resource limits	Kubernetes system pods only	requests=limits (Guaranteed QoS)	Prevent noisy neighbour resource starvation
Autoscaling (HPA)	N/A	CPU 60% → scale up	Scale before saturation — pre-emptive capacity

SECTION 11

NODE CLASSES & BILL OF MATERIALS

Vendor-neutral class definitions · ZAR costed BOM · 5-year budget model

All server specifications are vendor-neutral class definitions. Equivalent Dell, HPE, Lenovo, Supermicro, Fujitsu, or local sovereign OEM systems may be used provided the class requirements are met. For government backbone: enterprise hardware with 5-year NBD or 24x7x4 support, redundant power, remote management, TPM 2.0, and signed firmware.

Node Class	Qty	CPU	RAM	Storage	Network	Primary Role
K8s Control Plane	3/site	16–24 cores	128–192 GB	2×960GB SSD RAID1	Dual 10/25GbE + 1GbE OOB	etcd · API server · schedulers · cluster cont
Ingress / API Nodes	2–4/site	24–32 cores	128 GB	2×1.92TB NVMe	Dual 25GbE	HAProxy/Envoy · mTLS termination · auth e
Governance Workers	4–8/site	32–64 cores	256–512 GB	4×3.84TB NVMe	Dual 25/100GbE	FastAPI · policy engine · explainability · bia
Analytics / GPU (Ph2)	0–2/site	32–64 cores	512 GB	2×3.84TB NVMe	Dual 100GbE	1–2 datacentre GPUs 48–80GB VRAM · m
PostgreSQL HA	3/site	32–64 cores	512 GB	8×3.84TB NVMe RAID10 + boot mirror	Dual 25GbE	Registry · workflow · config · metadata · tra
Kafka Brokers	5/site	24–32 cores	128–256 GB	6×3.84TB NVMe	Dual 25GbE	Event stream · replay · compliance trail · fa
Cassandra Audit	6/site	24–32 cores	256 GB	8×7.68TB NVMe + boot mirror	Dual 25GbE	Append-only audit log · Merkle-linked storag
Redis Nodes	3/site	16–24 cores	128 GB	2×1.92TB SSD	Dual 10/25GbE	Session · rate limits · queues · short-lived s
OpenSearch Data	3–5/site	24–32 cores	256 GB	8×3.84TB NVMe	Dual 25GbE	Full-text audit search · compliance dashboa
Object Archive	4/site	16–24 cores	128 GB	12×16–20TB NL-SAS + SSD cache	Dual 25GbE	Immutable object storage · signed exports ·
Prom / SIEM / Ops	2–3/site	16–24 cores	128–256 GB	4×1.92TB SSD	Dual 10/25GbE	Observability · alerting · log aggregation · S
Bastion / Admin	2/site	8–16 cores	64 GB	2×960GB SSD	Dual 10GbE + isolated OOB	Jump host · break-glass access · admin too

11.1 Costed Bill of Materials — ZAR Estimates (ex VAT)

USD/ZAR: 17.18 (SARB 23 March 2026) · Import/shipping uplift: 8% · Contingency: 15% · All costs are planning estimates — replace with vendor quotes before procurement.

Item	Qty	Unit Cost (ZAR)	Subtotal (ZAR)	Phase
Governance / API / K8s Worker Nodes	6	R 650,000	R 3,900,000	Year 1
Immutable Audit / Cassandra Nodes	6	R 850,000	R 5,100,000	Year 1
PostgreSQL HA Nodes	4	R 550,000	R 2,200,000	Year 1
Redis / Cache Nodes	2	R 220,000	R 440,000	Year 1
OpenSearch / Analytics Nodes	4	R 450,000	R 1,800,000	Year 1
Object Archive / WORM Nodes	2	R 1,100,000	R 2,200,000	Year 1
FIPS 140-3 Level 3 Network HSM	2	R 1,750,000	R 3,500,000	Year 1
Offline Signing / Build Enclave Servers	2	R 480,000	R 960,000	Year 1
Offline Update Authority Server	1	R 350,000	R 350,000	Year 1
10/25/40Gb Aggregation Switches	4	R 60,111	R 240,444	Year 1

Item	Qty	Unit Cost (ZAR)	Subtotal (ZAR)	Phase
Edge Firewalls / Secure Gateways	4	R 250,000	R 1,000,000	Year 1
Optics / Transceivers / Structured Cabling	1	R 650,000	R 650,000	Year 1
20kVA Online UPS Units	4	R 227,499	R 909,996	Year 1
Rack PDUs / ATS / Power Distribution	4	R 35,000	R 140,000	Year 1
42U Lockable Racks / Cabinets	4	R 64,999	R 259,996	Year 1
Secure Cage / Room Fit-out / CCTV / Access Control	1	R 4,000,000	R 4,000,000	Year 1
KVM / Console / Crash Cart / Labelling	1	R 180,000	R 180,000	Year 1
Backup Appliance + Removable Media Rotation	1	R 450,000	R 450,000	Year 1
Cold Spares Pool (NICs / SSDs / PSUs / Fans)	1	R 1,200,000	R 1,200,000	Year 1
Implementation / Installation / Hardening Services	1	R 3,500,000	R 3,500,000	Year 1
Hardware & Services Subtotal			**R 32,980,436**	
Import / Shipping Uplift (8%)			**R 1,919,236**	
Contingency (15%)			**R 5,234,951**	
TOTAL CAPEX EX VAT			**R 40,134,623**	**Year 1**
TOTAL CAPEX INCL VAT (15%)			**R 46,154,817**	**Year 1**

11.2 Annual Staffing Model — 19 FTE Sovereign Ops Team

Function	Role	FTE	Loaded Cost/FTE (ZAR)	Annual Total (ZAR)
Leadership	Chief Platform / Sovereignty Architect	1	R 2,400,000	R 2,400,000
Engineering	Platform / Kubernetes Engineers	3	R 1,300,000	R 3,900,000
Engineering	Security / Crypto Engineers	2	R 1,500,000	R 3,000,000
Engineering	Data / Integration Engineers	2	R 1,250,000	R 2,500,000
Engineering	SRE / Observability Engineers	2	R 1,250,000	R 2,500,000
Engineering	DBA / Storage Engineers	2	R 1,300,000	R 2,600,000
Operations	NOC / SOC Analysts	4	R 650,000	R 2,600,000
Governance	AI Governance / Compliance Lead	1	R 1,500,000	R 1,500,000
Programme	Programme / Procurement Manager	1	R 1,200,000	R 1,200,000
Facilities	Data Centre / Facilities Engineer	1	R 900,000	R 900,000
TOTAL	**19 FTE Core Sovereign Ops & Engineering**	**19**		**R 23,100,000**

11.3 Five-Year Budget Model (Base Scenario, ex VAT)

Cost Block	Year 1	Year 2	Year 3	Year 4	Year 5	5-Year Total
Capex / Deployment	R40,134,623	R6,020,193	R3,210,770	R3,210,770	R8,026,925	R60,603,281
Staffing (19 FTE)	R23,100,000	R23,100,000	R23,100,000	R23,100,000	R23,100,000	R115,500,000
Operating Costs	R18,757,652	R18,757,652	R18,757,652	R18,757,652	R18,757,652	R93,788,260
Total ex VAT	R81,992,275	R47,877,845	R45,068,422	R45,068,422	R49,884,577	R269,891,541
VAT (15%)	**R12,298,841**	**R7,181,677**	**R6,760,263**	**R6,760,263**	**R7,482,687**	**R40,483,731**
TOTAL INCL VAT	**R94,291,116**	**R55,059,522**	**R51,828,685**	**R51,828,685**	**R57,367,264**	**R310,375,272**

SECTION 12

NETWORK & SECURITY ARCHITECTURE

Six trust zones · Zero trust · Sovereign key management · Air-gap capability

The network is segmented into six discrete trust zones. East-west traffic is authenticated and policy-controlled. North-south traffic is terminated at ingress gateways or air-gap transfer stations. The out-of-band management network is physically and logically separate from the production network. No zone has direct access to any zone more than one step away.

Zone	Systems	Connectivity Rule	Minimum Hardware
Zone 0 — OOB Manag[illegible]	iDRAC/iLO/BMC · Switch management [illegible]	[illegible] bastion over dedicated [illegible]	1 GbE [illegible] isolated jump hosts · Ses[illegible]
Zone 1 — Edge / Ingre[illegible]	Firewalls (HA pair) · Load balancers · [illegible]	[illegible]	[illegible] pair · DDoS-aw[illegible]
Zone 2 — App / Gover[illegible]	FastAPI services · Policy engine (OPA) · [illegible]	[illegible]	[illegible] Micro-segmentation (Cilium) · [illegible]
Zone 3 — Data Core	PostgreSQL HA · Cassandra audit clus[illegible]	[illegible]	[illegible] Encryption in transit · S[illegible]
Zone 4 — Security Pla[illegible]	FIPS 140-3 HSM × 2 · HashiCorp Vaul[illegible]	[illegible]	[illegible] Air-gap[illegible]
Zone 5 — Secure Tran[illegible]	Offline package import/export station · [illegible]	[illegible]	[illegible] Signed media proc[illegible]

12.1 Security Controls Matrix

Control	Implementation	Standard	Constitutional Pillar
Password Hashing	bcrypt cost factor 12 — no plaintext storage ever	NIST SP 800-63B	Pillar VI — Transparency
JWT Authentication	RS256 asymmetric signing · 8-hour session expiry · Refresh token rotation	RFC 7519	Pillar VI — Transparency
mTLS (Gov)	Mutual TLS 1.3 mandatory for all inter-service traffic in sovereign deployments	TLS 1.3 RFC 8446	Pillar III — Sovereign Respect
Role-Based Access Control	8 role levels · Minimum privilege · No single actor holds both signing and audit access	NIST RBAC	Pillar XI — Anti-Corruption
Encryption at Rest	AES-256-GCM for all personal information · HSM for key management (Phase 2)	NIST FIPS 197	Pillar VIII — Human Primacy
Encryption in Transit	TLS 1.3 minimum on all connections · Certificate pinning for government deployments	TLS 1.3 RFC 8446	Pillar VI — Transparency
HMAC Audit Signatures	HMAC-SHA256 on every audit event · Signed before Cassandra write	FIPS 198-1	Pillar VI — Transparency
Merkle Tree Integrity	Root hash published every 15 minutes · Any modification is detectable	SHA-3-256	Pillar VI — Transparency
Security Headers	Helmet.js: HSTS · CSP · X-Frame-Options · Constitutional identification headers on all responses	OWASP	Pillar VI — Transparency
Rate Limiting	Per-route rate limits · Express-rate-limit / slowapi · DDoS protection · Credential stuffing prevention	OWASP	Pillar XI — Anti-Corruption
Data Sovereignty	Zero foreign cloud · All data ZA jurisdiction · No US CLOUD Act exposure · Verified every 6 [illegible]	Constitutional Pillar III	Pillar III — Sovereign Respect
Founder Override Disabled	No super-override exists in system architecture. All actions logged. COB has full audit rights.	Constitutional Design	Pillar VII — Founder Constraint
Input Validation	Pydantic v2 / Joi schema validation on all API inputs · Parameterised queries prevent SQL injection	OWASP ASVS	Pillar XI — Anti-Corruption
TPM 2.0 Attestation	All production nodes must pass TPM 2.0 attestation before joining the cluster	TCG TPM 2.0	Pillar III — Sovereign Respect
Key Rotation	Session keys: per-session · DEK: 90 days · KEK: annual · Master: manual 2-of-3 custodians	NIST SP 800-57	Pillar VI — Transparency
Penetration Testing	Annual physical + network + application penetration test by independent party	PTES / OWASP	Pillar XI — Anti-Corruption

SECTION 13

QUANTUM-READY CRYPTOGRAPHIC ARCHITECTURE

NIST PQC Standards · Harvest-now-decrypt-later threat · Hybrid transition

The transition to quantum computing poses a definitive threat to all current RSA, ECC, and Diffie-Hellman based cryptographic systems. Systems deployed today using classical cryptography are vulnerable to "harvest now, decrypt later" attacks — adversaries collect encrypted data today intending to decrypt it when quantum computers become sufficiently powerful. AI governance audit records have a 10-year retention requirement. This means every record created in 2026 must remain confidential until 2036 — well within the projected quantum threat window.

"UDOC is built on NIST PQC standards from inception, eliminating the harvest-now-decrypt-later risk for all clients. Quantum readiness is not a Phase 2 feature — it is a Phase 1 architectural constraint."

13.1 Quantum Threat Assessment

Classical Algorithm	Current Use	Quantum Vulnerability	Threat Timeline	UDOC Response
RSA-2048	TLS key exchange · Document signing	Shor's algorithm — broken by ~4000 logical qubits	2030–2035 (est.)	Replace with Kyber KEM in Phase 2
ECDH (P-256)	TLS session key agreement	Shor's algorithm — broken by ~2000 logical qubits	2030–2035 (est.)	Replace with Kyber KEM in Phase 2
ECDSA	JWT signing · Certificate signing	Shor's algorithm — breaks signature scheme	2030–2035 (est.)	Replace with Dilithium in Phase 2
SHA-256	Merkle tree · HMAC	Grover's algorithm — reduces to 128-bit security	Distant (limited threat)	Upgrade to SHA-3-256/512 — already planned
AES-128	Symmetric encryption	Grover's algorithm — reduces to 64-bit security	Manageable threat	Upgrade to AES-256 — already implemented
AES-256	Data at rest (current)	Grover's — reduces to 128-bit (still secure)	No practical threat	Retain AES-256 as symmetric baseline

13.2 NIST Post-Quantum Cryptography Standards — Full Specification

Algorithm	Type	UDOC Use	NIST Standard	Status
CRYSTALS-Kyber (ML-KEM)	Key Encapsulation	TLS session keys · Data encryp	FIPS 203 — Finalized	Phase 2 — Q3 2026
CRYSTALS-Dilithium (ML-DSA)	Digital Signature	Audit log signing · API auth ·	FIPS 204 — Finalized	Phase 2 — Q3 2026
FALCON (FN-DSA)	Digital Signature	Compact signatures for IoT/sen	FIPS 206 — Finalized	Phase 3 — Edge nodes
SPHINCS+ (SLH-DSA)	Stateless Signature	Long-term archive signing — 10	FIPS 205 — Finalized	Phase 2 — Q3 2026
AES-256-GCM	Symmetric Encryption	Data at rest · Transport encry	NIST FIPS 197	Active — Phase 1
SHA-3 (SHAKE256)	Hash Function	Data integrity · Merkle tree n	NIST FIPS 202	Active — Phase 1
HMAC-SHA256	Message Auth	Audit event signing (Phase 1)	NIST FIPS 198-1	Active → Phase 2 transition

13.3 Hybrid TLS 1.3 Transition Architecture

During the transition period (2026–2028), UDOC operates a hybrid cryptographic architecture that maintains backward compatibility with classical systems while providing quantum-resistant security for all new data. This uses a dual-algorithm approach where every cryptographic operation uses both the classical algorithm (for compatibility) and the PQC algorithm (for quantum security). The classical algorithm can be deprecated when the ecosystem is ready.

Operation	Phase 1 (Current)	Phase 2 (Q3 2026 — Hybrid)	Phase 3 (2027 — Full PQC)
TLS Key Exchange	ECDH (X25519)	ECDH (X25519) + Kyber-768 Combined_key = HKDF(classical||kyber)	Kyber-768 only
Audit Record Signing	HMAC-SHA256	HMAC-SHA256 + Dilithium3 (dual sig)	Dilithium3 only
Archive Long-term Signing	HMAC-SHA256	SHA-3 + SPHINCS+-128f	SPHINCS+-128f only
Data Encryption Keys (DEK)	AES-256-GCM, key gen classical	AES-256-GCM, key encap via Kyber	AES-256-GCM + Kyber full
JWT API Authentication	RS256 (RSA-2048)	RS256 + Dilithium3 (dual sign)	Dilithium3 only
Certificate Signing (PKI CA)	ECDSA-P256	ECDSA-P256 + Dilithium3	Dilithium3
Merkle Tree Hashing	SHA-256	SHA-3-256	SHA-3-256
HSM Key Generation	ECDH / RSA in HSM	HSM upgraded to support Kyber keygen	Full Kyber/Dilithium in HSM

SECTION 14

POST-QUANTUM MIGRATION ROADMAP

Step-by-step quantum transition · HSM upgrade · Certificate migration

14.1 Migration Phases

PHASE 1 — NOW	PHASE 2 — Q3 2026	PHASE 3 — 2027	PHASE 4 — 2028	PHASE 5 — 2030+
AES-256 baseline ■ SHA-3 hashing ■ HMAC-SHA-3 ■ Dilithium3 signing ■ Hybrid TLS 1.3 ■ Kyber KEM ■ HSM PQC upgrade ■ Full Kyber/Dilithium ■ Classical removed ■ Full PQC only ■ QKD network ■ QKD backbone ■ Post-PQC review				

Migration Task	Phase	Timeline	Dependencies	Risk	Owner
Install liboqs Python bindings on all governance workers	2	Q2 2026	Python 3.11 · Rust toolchain	LOW	Security Eng.
Upgrade HSMs to firmware supporting Kyber key generation	2	Q3 2026	HSM vendor support contract	MEDIUM	Security Eng.
Deploy hybrid TLS 1.3 (ECDH + Kyber-768) on all ingress nodes	2	Q3 2026	HSM upgrade · liboqs	MEDIUM	Platform Eng.
Migrate Dilithium3 signing to all new audit events	2	Q3 2026	Hybrid TLS · HSM upgrade	LOW	Audit Service
Add SPHINCS+-128f signing to all archive export bundles	2	Q4 2026	Dilithium migration	LOW	Audit Service
Re-sign all existing audit records with Dilithium3 dual signatures	2	Q4 2026	Cassandra capacity · HSM	HIGH	DBA + Security
Upgrade PKI CA to issue Dilithium3 certificates	3	Q1 2027	HSM PQC support · Testing	MEDIUM	Security Eng.
Replace all JWT RSA signing with Dilithium3	3	Q1 2027	PKI CA upgrade · Client testing	MEDIUM	Auth Service
Deprecate ECDH classical component of hybrid TLS	3	Q2 2027	Ecosystem readiness audit	HIGH	Platform Eng.
Full Kyber-only key encapsulation (classical removed)	4	Q1 2028	All clients Kyber-capable	HIGH	Platform Eng.
Full Dilithium3-only signing (RSA/ECDSA removed)	4	Q2 2028	All verifiers Dilithium-capable	HIGH	Security Eng.
Evaluate QKD (Quantum Key Distribution) backbone for national deployment	5	2030+	QKD infrastructure availability	RESEARCH	CTO / Research

14.2 HSM Architecture — Key Management

Key Type	Storage	Rotation	Custody	PQC Upgrade
Master Key	HSM #1 + HSM #2 (dual custody)	Manual — requires 2-of-3 officer age	2-of-3 officer split custody	HSM firmware upgrade to support Kyber ma
Key Encryption Keys (KEK)	Derived in HSM from master key	Annual rotation with 30-day overlap	HSM only — never exported	Kyber-wrapped KEK generation in HSM
Data Encryption Keys (DEK)	Encrypted by KEK · Stored in Vault	90-day automatic rotation · Old DEK retained for	Vault + HSM managed	Kyber encapsulation of DEK material
Session Keys (TLS)	Ephemeral — generated per connection	Per-session (forward secrecy)	Never persisted	Kyber KEM for session key agreement
Signing Keys (Audit)	Private key in HSM only — never exported	Annual for classical · Phase 2: Dilithium key	HSM key ceremony	Dilithium3 private key generated in HSM
Archive Signing Keys	Private key in HSM offline enclave	5-year rotation (SPHINCS+ stateless)	Offline ceremony — dual officer	SPHINCS+-128f in HSM Phase 2
G.O.D.S Engineer Access	ZERO access to client master keys	N/A	Client-only custody	Maintained through PQC migration

SECTION 15

DATA OPERATIONS CORE & STORAGE

Hot · Warm · Archive · Offline zones · Retention architecture

The data operations core is where the platform earns the claim that audit, lineage, registry state, bias signals, and compliance evidence are technically durable — not merely application logs. Each data class has a specific storage subsystem, write pattern, retention target, and hardware rule. Storage decisions are driven by the 10-year audit retention requirement mandated by SA AI Policy and the UDOC constitutional mandate.

Subsystem	Data Type	Write Pattern	Retention Target	Hardware Rule
PostgreSQL 16	Registry · Workflows · Users · Config · Oversight queue · Metadata	Transactional RW — ACID	7 years governance metadata minimum	HA · NVMe RAID10 · Synchronous replication · [illegible]
Apache Kafka 3.x	Decision events · Lifecycle events · Integration streams · DLQ	Append event — High throughput	Short-to-medium + replay window	5 brokers min · RF=3 · 25GbE · Idempotent produce[illegible]
Cassandra 5 / WORM	Immutable AI decision audit events · Merkle-linked verification records	Append-only — write-once	10 years MINIMUM — never deleted	6 nodes min · Separate audit keyspace · ALL consis[illegible]
Redis 7	Session tokens · Rate limit counters · Ephemeral queues · Hot cache	Transient in-memory — cache	Hours to days — selective persistence	3 nodes min · Sentinel HA · RDB persistence for que[illegible]
OpenSearch 2.x	Searchable audit indexes · Compliance dashboards · Alert rules	Indexed ingest — near-real-time	24 months hot/warm then archive to object store	Separate ingest and data roles at high volume · War[illegible]
Object Archive (S3)	Signed evidence packs · Snapshot chains · Monthly Merkle root publications	Immutable object write — versioned	7–10 years · Extended legal hold	[illegible] packs · Erasure coding or replication · WORM[illegible]
Offline Tape Archive	Yearly cold seal of all governance data	Quarterly to annual manual process — catastrophic recovery	Indefinite — sovereign legal hold	Removable media in secure vault · Two-person integ[illegible]

15.1 Storage Zone Architecture

Zone	Technology	Contents	Latency Target	Migration
HOT ZONE	NVMe-only · Enterprise grade · PLP protection	PostgreSQL transactional · Kafka broker storage · Cassandra write [illegible]	Sub-1ms write · Sub-[illegible]	Automatic [illegible] data stays until [illegible] threshold [illegible]
WARM ZONE	Lower-cost SSD or high-capacity NVMe	OpenSearch warm indexes · Kafka replay topics (older [illegible])	Sub-5ms write · Sub-20ms read	After 30 days · Recently closed compliance [illegible]
ARCHIVE ZONE	Immutable object storage — S3-compatible WORM	Signed evidence bundles · Monthly Merkle root snapshots · Sealed compliance reports	Sub-60s typical	After 24 months · Exported regulatory packs · [illegible] object lifecyc[illegible]
OFFLINE ARCHIVE	Tape or removable media vault — air-gapped	Yearly archive sealing · Sovereign legal hold sets	Manual retrieval — hours to days	Annual manual process · Dual-officer cerem[illegible]

15.2 Backup & Recovery Architecture

Layer	Technology	Frequency	Retention	RPO	RTO Test
PostgreSQL WAL	Continuous WAL archiving to object archive	Continuous	35–90 days hot	<1 min (theoretical)	Monthly restore drill
PostgreSQL Snapshot	Storage snapshot — 4-hour cycle	Every 4 hours	30 days on-site · Monthly sealed	<4 hours	Monthly point-in-time restore
Kafka Topic	Broker replication RF=3 + MirrorMaker2 cross-site	Continuous	Topic-specific (see §07)	Near-zero within site	Quarterly broker kill test
Cassandra Repair	Incremental repair + scheduled snapshot	Daily repair · Weekly snapshot	30–90 days local + monthly archive	Near-zero (RF=3)	Monthly node rebuild test
Object Archive	Versioned WORM — erasure coding	Continuous on write	7–10+ years	Per object	Quarterly export validation
Full Platform DR	Secondary site promotion	On-demand failover	Secondary site replication	<1 hour (backbone)	Quarterly full DR drill

SECTION 16

EMBEDDED GOVERNANCE FABRIC

SDK · Sidecar · Host Agent · Gateway Appliance · Edge Governance Node

UDOC is not a dashboard. It is a governance fabric — delivered as a set of attachment points that embed into AI applications at five different layers depending on the technical environment. The fabric makes governance impossible to bypass by policy alone — it is technically embedded into the infrastructure stack and the software delivery path. Each attachment method provides different levels of enforcement capability and different failure behaviours.

Attachment	Where Used	Min. Local Spec	What It Enforces	Failure Behaviour
SDK / In-Process Library	Custom AI applications · Model-[illegible]	Negligible [illegible]	Registration hooks · [illegible]	Fail-closed for CRITICAL · [illegible]
Sidecar Container	Kubernetes workloads · Model-serving pods [illegible]	2–4 vCPU · 4–8 GB RAM [illegible]	[illegible] Policy [illegible]	Buffers locally [illegible]
Host Agent	VMs · Bare metal model hosts · [illegible]	4–8 vCPU · 8–16 GB RAM [illegible]	[illegible] Drift scan · [illegible]	Continues [illegible]
Gateway Appliance	Shared SaaS services · SaaS [illegible]	8–16 vCPU · 32–64 GB RAM [illegible]	[illegible] policy enforcement [illegible]	Store-and-forward [illegible]
Edge Governance Node	Disconnected sites · OT environments · Field offices [illegible]	16–32 vCPU · 64–128 GB RAM [illegible]	[illegible] · Signed [illegible]	[illegible]

16.1 Edge Governance Appliance Classes

Class	Use Case	CPU	RAM	Storage	Networking
Compact Edge	Single agency office · Branch office · Local relay + signed queueing only	8–16 cores	32–64 GB	2×1.92TB SSD	Dual 10GbE + LTE/5G optional [illegible]
Standard Edge	Provincial department · Hospital group · Field cluster · Local registry mirror + short-term audit	16–24 cores	64–128 GB	2×3.84TB NVMe + mirrored boot	Dual 10/25GbE
Resilient Edge Trio	Disconnected high-value site · Full local micro-cluster · [illegible]	3 × 16–24 cores each	64GB each	2×3.84TB NVMe each	Dual 10GbE each

SECTION 17

SA AI POLICY GG54477 ALIGNMENT

Draft National AI Policy · Government Gazette · 10 April 2026 · 86 Pages

South Africa's Draft National AI Policy (Government Gazette No.54477) was approved by Cabinet on 25 March 2026 and published for public comment on 10 April 2026. The comment period closes 10 June 2026. UDOC v5.0 is architecturally pre-aligned to all six strategic pillars, the three-phase implementation roadmap, and all specific technical requirements in the draft. This alignment is enforced at code and infrastructure level — not merely documented.

SA AI Policy Requirement	GG54477 Reference	UDOC Implementation	Status
Mandatory human-in-the-loop for critical AI decisions	Section 3.3 · Pillar 06	HITL enforcement module · Queue · SLA monitoring · COB notification	Active — HIGH RISK enforced
Mandatory human rights impact assessment (HRIA)	Pillar 04 (HIGH RISK)	HRIA module · Gender impact module · s9/s10 compliance tracking	Operational — tracking assessments
AI system registration before deployment	Pillar 03	AI Registry — all systems must register · Unregistered detection · Alert	Enforced — all systems registered
Explainability in high-stakes domains	Section 3.3 · Pillar 03	LIME/SHAP explainability · Plain language · Regulatory format	Active — s33 RSA RISK covered
Accountability for AI-driven decisions	Pillar 03	Constitutional audit trail · Operator assignment · HMAC-signed evidence	Operational
Bias mitigation and fairness monitoring	Pillar 04	SPD bias engine · 6 characteristics · Counterfactual testing · SAHRC escalation	Active — SAHRC escalation
Data sovereignty and protection	Pillar 05	ZA jurisdiction lock · Zero foreign cloud · Sovereignty verified every 6 hours	Enforced — 100% ZA
Prohibition of unacceptable risk AI (social scoring)	GG54477 risk framework	PROHIBITED tier in registry · Deployment blocked at registration	Enforced — SYS-010 blocked
Citizen right to challenge AI decisions	Pillar 06 · s33 RSA	AI Ombudsperson queue · Decision replay · Counterfactual analysis	Active — 3 cases open
Cryptographically verifiable audit trail	Pillar 03	HMAC-SHA256 Merkle audit log · Cassandra WORM · 10-year retention	Implemented
Transparency of AI system operation	Pillar 03	Explainability engine · Plain language citizen output · Regulator portal	Operational
AI Ethics Board / COB oversight	Pillar 04 (proposed)	COB aligned to proposed AI Ethics Board · 5 independent seats · Recruitment active	COB active · Recruitment active
AI Ombudsperson Office	Pillar 06 (proposed)	Ombuds queue pre-built · Decision replay infrastructure ready · s33 RSA	Infrastructure ready — pending establish
POPIA compliance for AI data processing	Existing law + AI Policy	POPIA Section 26 enforcement · AES-256 · Consent management · Retention scheduling	Enforced · Retention scheduling
Gender and human rights impact assessments	Pillar 04	HRIA module · Gender impact tracking · Bill of Rights compliance checking	Active — 2 HRIAs pending
Cultural preservation — indigenous data	Pillar 05	Data sovereignty enforcement · Indigenous language AI · No foreign data export	Operational
Ubuntu AI principle — community benefit	Policy Introduction	S.E.T.H.S integration · Economic multiplier tracking · SDG alignment · Pillar XII	Active — 2.3× multiplier
Multi-regulator coordination (DCDT/ICASA/POPIA)	Policy governance	Regulator portal · Case rooms · GG54477 comment submission prepared	Submission prepared

SECTION 18

CONSTITUTIONAL COMPLIANCE ARCHITECTURE

G.O.D.S 12 Pillars · RSA Bill of Rights · Code-level enforcement

18.1 G.O.D.S 12 Constitutional Pillars — Code-Level Enforcement

Pillar	Name	Software Enforcement	Hardware Enforcement
I	Human Dignity	Dignity check in all HIGH RISK decision pathways · s10 RSA compliance module	Sovereign data residency — no dignity violations from foreign law expo
III	Sovereign Respect	X-UDOC-Sovereignty header on ALL responses · Foreign cloud = false · hardcoded sovereign check	ZA-only hardware · TPM 2.0 attestation · Zero foreign egress at firewall lay
VI	Transparency & Accountability	All admin actions logged to platform_audit_log BEFORE handler executes · HMAC-signed · 7-year retention	Cassandra WORM — immutable at storage layer · No delete AI
VII	Founder Constraint	founder_override = false in all system config files · No super-override code path exists · COB has read access to all	No hardware bypass — all actions go through logged authentication lay
VIII	Human Primacy in AI	HITL enforcement service blocks HIGH RISK decisions without documented human review pathway — COB alert if 48h exceeded	Oversight queue SLA monitor on hardware · Compliance alert if violated
XI	Anti-Corruption	8 role levels · Minimum privilege · No single user holds both signing authority and audit write access · Dual-control break-glass	HSM split custody 2-of-3 officers · Dual-custody HSM · Physic
XII	Measurement	Outcomes dashboard · KPI tracking · Constitutional legitimacy index · SDG alignment	Prometheus metrics from all hardware nodes feed Constitutional compliance

SECTION 19

PHASED DEPLOYMENT ROADMAP

Phase 1 (Months 1–18) ⇒ Phase 5 (Months 55–120) · Triggers and milestones

Phase 1 — Enterprise SaaS MVP

Timeline: Months 1–12

- Secure build/signing enclave commissioned and tested
- Kubernetes control plane live (3 nodes primary site)
- PostgreSQL HA cluster operational — Patroni failover tested
- Kafka starter ring (3 brokers) — governance event topics configured
- Governance worker nodes (4 nodes) — FastAPI services deployed
- Post-quantum crypto baseline active (AES-256 + SHA-3)
- UDOC Node.js MVP API deployed and accessible
- React dashboard v1 — all core modules functional
- AI Registry MVP — first 3 enterprise AI systems registered
- UDOC enterprise SaaS — 3 pilot clients onboarded

Phase 2 — Government Pilot

Timeline: Months 10–24

- Cassandra immutable audit cluster (6 nodes) live — WORM enabled
- Object archive nodes (4 nodes) — signed bundle export working
- OpenSearch cluster (3 nodes) — full-text audit search operational
- HSM-backed signing service live — HMAC-SHA256 + Dilithium3 hybrid
- Compliance engine — all 9 frameworks scoring (incl. SA AI Policy GG54477)
- Bias detection — SPD engine live — all 6 characteristics monitored
- Human oversight queue — SLA monitoring — COB notification active
- Sovereignty verification — 6-hour cycle — all nodes attested
- Cloud QPU API integrated for advanced analytics (optional)
- First government sovereign deployment — national pilot

Phase 3 — Secondary Site & DR

Timeline: Months 22–48

- Secondary site live (2–3 racks) — PostgreSQL/Kafka/Cassandra replicated
- Edge governance nodes deployed — Tier 1 provincial deployments
- Formal DR testing and 99.95% uptime SLA demonstrable
- PQC full migration — Kyber KEM + Dilithium3 + SPHINCS+ all active
- On-premises QPU deployed (100+ qubits) for quantum governance analytics
- AI Ethics Board / COB fully constituted — 5/5 independent seats
- 5+ government deployments — National AI Governance Backbone MOU
- FSCA FSP licence approved (target Month 24) — M.A.D.I.B.A capital platform
- ISO 27001 and SOC 2 Type II certifications achieved
- SADC first market — cross-border AI governance framework negotiated

Phase 4 — National Scale

Timeline: Months 38–72

- SADC multi-jurisdictional quantum network — AQGN pilot
- GPU analytics nodes deployed — 80GB VRAM model forensics active
- Larger archive tiers — Tier 3 national multi-domain backbone
- Broader ministry integrations — welfare, justice, border, tax, health
- FSCA regulatory certifications — full fund administration capability
- 10+ sovereign UDOC nodes interconnected
- M.A.D.I.B.A capital deployed at scale — first fund close
- T.S Industries full project management system live

Phase 5 — Continental & Quantum Timeline: Months 55–120

- Full fault-tolerant quantum computing (1000+ logical qubits)
- QKD backbone — Quantum Key Distribution sovereign network
- Continental AI governance standard — UDOC as African backbone
- Global architecture licensing to international system integrators
- SADC AI Governance Treaty — UDOC as reference implementation
- Full PQC classical algorithm deprecation across all deployments
- Post-PQC review — evaluate NIST Round 2 standards

SECTION 20

PERFORMANCE SPECIFICATIONS & SLAS

Response times · Uptime targets · Measurement methodology

Metric	Enterprise Target	Gov Backbone Target	Measurement	SLA Penalty
API Response Time (p95)	<200ms	<150ms	Prometheus histogram	Service credit if >500ms sustained
API Response Time (p99)	<500ms	<300ms	Prometheus histogram	Alert and review if >1s
Governance Pipeline Latency	<50ms overhead	<30ms overhead	Decision event tracing	Alert if >100ms sustained
Audit Write Latency	<100ms	<50ms	Kafka consumer lag monitoring	Alert if >500ms
Audit Verification (Merkle)	<500ms typical	<200ms typical	Automated verification test	Review if >2s
Compliance Report Generation	<60s standard	<30s	Automated test suite	Credit if >300s
Full Audit Extract (12 months)	<10 minutes	<5 minutes	Batch export timing	Priority support if >30m
Emergency Incident Report	<5 minutes	<2 minutes	Incident response drill	Mandatory escalation
Database Failover (intra-site)	<60 seconds	<30 seconds	Patroni switchover test	Alert if >5 min
Platform Uptime (monthly)	99.9% (8.76h/yr max)	99.95% (4.38h/yr max)	External uptime monitoring	5% monthly credit per 0.1% below target
Recovery Time Objective (RTO)	<4 hours (platform)	<2 hours (backbone)	Quarterly DR drill	Priority support activation
Recovery Point Objective (RPO)	<4 hours	<1 hour (backbone)	Backup verification testing	Priority support activation
Security Patch Deployment	<72h (critical)	<24h (critical)	Patch log	Mandatory escalation if exceeded
Sovereignty Verification	Every 6 hours	Every 6 hours	Automated cron + external audit	COB alert if any check fails
Bias Scan Cycle	Every 24 hours	Every 24 hours	Scheduled job completion	COB alert if scan fails

SECTION 21

OPERATIONAL READINESS & ACCEPTANCE CRITERIA

Pre-go-live checklist · DR testing schedule · Government onboarding requirements

The following checklist must be verified by an independent technical auditor and the Constitutional Oversight Board before any government or sovereign data is onboarded onto the platform. Each item requires documentary evidence and a signed-off test result. This is not a self-attestation — independent verification is mandatory.

Area	Acceptance Criterion	Evidence Required	Sign-Off Authority
Availability	All critical services survive loss of any single server without platform availability loss	Failover test report with timestamped logs	Independent Tech Auditor
Database	PostgreSQL failover inside 30s agreed RTO. Application reconnection automatic	Patroni switchover evidence · Failover drill report	DBA + Independent Auditor
Messaging	Kafka and Cassandra continue operating after loss of at least one broker/node	Kill-test results · Replication health dump	Platform Engineer + Auditor
Security	HSM switchover and signer failover demonstrably tested and fully logged	HSM drill report · Key access audit log	Security Engineer + CISO
Air-gap	Offline release import produces signed import manifest with full chain of custody	Signed manifest · Malware scan log · Dual-officer record	Security + Facilities
Governance Fabric	Sidecar/agent deployment templates exist for K8s, VM, and legacy gateways	Deployment templates · Integration test results	Platform Engineer
Audit Export	Immutable archive export produced, signed, and validated independently from live	Export bundle · Independent Merkle verification	Independent Tech Auditor
Testing Cadence	Monthly restore tests, quarterly DR drills, annual physical pen test scheduled	Testing calendar · Filed results from each type	Operations Manager
Asset Register	All racks, PDUs, patch panels, switch ports labelled and mapped	Asset register · Physical inspection sign-off	Facilities Engineer
Observability	Capacity dashboards report CPU, RAM, disk latency, queue lag, broker health per environment	Dashboard screenshots · Alert routing evidence	SRE Lead
Constitutional	Pillar VIII: all HIGH RISK systems have documented human review pathway	Registry export · HITL pathway documentation	COB Member + Auditor
Sovereignty	Sovereignty verification running every 6 hours. Foreign exposure = false in all checks.	30-day rolling sovereignty check log	Sovereignty Engineer + COB
SA AI Policy	All GG54477 mandatory requirements implemented and tested	GG54477 compliance matrix · Test evidence	Compliance Lead + COB
POPIA	Section 57 prior authorisation obtained · Consent module operational · Retention enforced	Information Regulator confirmation · System audit	Information Officer + Legal
PQC Readiness	Post-quantum migration readiness assessment completed · Hybrid TLS active	PQC readiness report · TLS configuration audit	Security Engineer
COB Oversight	COB Annual Compliance Certificate issued · All data room documents accessible	COB resolutions · Document vault index	COB Chair

21.1 Operational Testing Schedule

Test Type	Frequency	Duration	Responsible	Documentation
PostgreSQL Point-in-Time Restore	Monthly	2–4 hours	DBA	Restore report · Validation log
Cassandra Evidence Bundle Restore	Monthly	1–2 hours	DBA	Bundle integrity verification report
Kafka Topic Replay Verification	Monthly	1–2 hours	Platform Engineer	Consumer group lag report
Object Archive Export Validation	Monthly	1–2 hours	Operations	Export + independent Merkle verification
Full DR Failover Exercise	Quarterly	4–8 hours	All Engineering	DR test report · RTO/RPO measurements
HSM Switchover Drill	Quarterly	2 hours	Security Engineer	HSM audit log · Signing service continuity
Offline Package Import	Quarterly	2 hours	Security + Facilities	Import manifest · Malware scan log

Test Type	Frequency	Duration	Responsible	Documentation
Physical Security Review	Quarterly	4 hours	Facilities + Security	Inspection checklist · CCTV audit
Sovereignty Audit (independent)	Quarterly	1 day	External Network Auditor	Network audit report · Egress confirmation
Physical Penetration Test	Annual	3–5 days	External PenTest Firm	PenTest report · Remediation plan
Application Security Assessment	Annual	5 days	External AppSec Firm	OWASP assessment · CVE scan
PQC Readiness Assessment	Annual	2 days	Crypto Specialist	PQC readiness report · Algorithm review
Constitutional Compliance Audit	Annual	3 days	COB + External Auditor	Constitutional compliance certificate
SA AI Policy Compliance Review	Annual (or on policy update)	2 days	Compliance Lead + Legal	Policy alignment matrix update
Full Capacity Planning Review	Annual	1 day	All Engineering Leads	Capacity plan · Procurement triggers

APPENDIX A

DATA CLASSIFICATION & HARDWARE TREATMENT MAP

Five classification tiers · Deployment rules · Crypto rules · Connectivity rules

Classification	Description	Deployment Rule	Crypto Rule	Storage Rule	Connectivity
SOVEREIGN-CRITICAL	National security · Identity · [illegible]	[illegible]	[illegible]	[illegible]	[illegible]
SOVEREIGN-HIGH	Citizen PII · Health records · [illegible]	[illegible]	[illegible]	[illegible]	[illegible]
GOVERNANCE	AI system governance data · [illegible]	[illegible]	[illegible]	[illegible]	[illegible]
OPERATIONAL	Anonymised metrics · System [illegible]	[illegible]	[illegible]	[illegible]	[illegible]
PUBLIC	Published governance reports [illegible]	[illegible]	[illegible]	[illegible]	[illegible]

APPENDIX B

API ENDPOINT REFERENCE — FULL SURFACE

All public and admin endpoints with authentication requirements

Method	Endpoint	Auth Level	Constitutional Pillar	Rate Limit
POST	`/api/v1/auth/token`	Public	Pillar VI (Authentication log)	10/min
POST	`/api/v1/auth/refresh`	Bearer token	Pillar VI	20/min
POST	`/api/v1/auth/revoke`	Bearer token	Pillar VI	10/min
GET	`/api/v1/registry/systems`	OPERATOR+	Pillar VIII	200/15min
POST	`/api/v1/registry/systems`	OPERATOR+	Pillar VIII (HIGH RISK validation)	50/hour
GET	`/api/v1/registry/systems/{id}`	OPERATOR+	Pillar VIII	200/15min
PATCH	`/api/v1/registry/systems/{id}`	ADMIN+	Pillar VI + VIII	50/hour
DELETE	`/api/v1/registry/systems/{id}`	ADMIN+	Pillar VIII (COB notify)	10/hour
POST	`/api/v1/decisions/`	SERVICE	Pillar VIII (HITL check)	1000/min (bulk)
GET	`/api/v1/decisions/{id}`	OPERATOR+	Pillar VI	200/15min
GET	`/api/v1/decisions/{id}/verify`	PUBLIC	Pillar VI (Merkle verification)	100/15min
GET	`/api/v1/audit/events`	OPERATOR+	Pillar VI	100/15min
POST	`/api/v1/audit/events/{id}/review`	OPERATOR+	Pillar VIII	100/15min
GET	`/api/v1/audit/merkle/root`	OPERATOR+	Pillar VI	200/15min
POST	`/api/v1/audit/export`	ADMIN+	Pillar VI	10/hour
POST	`/api/v1/compliance/check`	ADMIN+	Pillar VI (SA AI Policy check)	20/hour
GET	`/api/v1/compliance/report/{id}`	OPERATOR+	Pillar VI	50/hour
POST	`/api/v1/bias/scan`	ADMIN+	Pillar I (s9 RSA)	10/hour
GET	`/api/v1/bias/alerts`	OPERATOR+	Pillar I	200/15min
GET	`/api/v1/oversight/queue`	ADMIN+	Pillar VIII	200/15min

Method	Endpoint	Auth Level	Constitutional Pillar	Rate Limit
POST	`/api/v1/oversight/review`	ADMIN+	Pillar VIII	100/15min
GET	`/api/v1/lineage/{system_id}`	OPERATOR+	Pillar VI	100/15min
GET	`/api/v1/sovereignty/status`	OPERATOR+	Pillar III	200/15min
POST	`/api/v1/sovereignty/verify`	ADMIN+	Pillar III	5/hour
GET	`/api/v1/workforce/`	SETHS_HEAD+	Pillar XII	100/15min
GET	`/api/v1/admin/users`	SUPER_ADMIN	Pillar XI	50/hour
PUT	`/api/v1/admin/users/{id}/role`	SUPER_ADMIN	Pillar XI (dual control log)	10/hour
GET	`/health`	None	Pillar III (sovereignty header)	Unlimited
GET	`/health/ready`	None	N/A	Unlimited

APPENDIX C

PROCUREMENT NOTES & LOCAL ADAPTATION

ZA sovereign preference · Vendor neutrality · FX exposure · VAT

Vendor Neutrality

Do not lock the specification to a single OEM unless the client procurement environment demands it. Define equivalence by CPU class, RAM, storage endurance, NIC speed, PSU redundancy, support SLA, TPM 2.0 capability, and signed firmware availability.

Local Sovereign Preference

For ZA sovereign deployments, prefer data-centre operators and support contracts that keep hardware replacement, logistics, and spare part holding within ZA jurisdiction. This directly supports SA AI Policy Pillar 05 (Cultural Preservation and International Integration).

Cold Spares Policy

Buy spare disks, NICs, PSUs, fans, and at least one spare server per critical node class for sovereign or air-gapped environments where vendor lead time is a strategic risk. Budget R1.2M for cold spares.

Budget Priority Order

Do NOT underbuild HSM redundancy, PostgreSQL HA, Kafka quorum, or Cassandra immutable audit storage. These are non-negotiable. Reduce OpenSearch and GPU analytics capacity first if budget is constrained. The immutable audit store is the core of the constitutional mandate.

FX Exposure

Server, HSM, and networking hardware is predominantly USD-priced. The budget model assumes R17.18/$ (SARB 23 March 2026). A forward hedge or budget buffer of 10–15% is recommended for multi-year procurement cycles to protect against ZAR/USD movement.

VAT Treatment

All capex, staffing, and opex figures in this document are ex VAT. Add 15% VAT for cash-flow and budget submission purposes. VAT registration must be in place before hardware procurement begins.

Replace Estimates with Quotes

Server, HSM, storage, staffing, co-location, connectivity, and implementation costs are planning assumptions only. Replace with distributor quotes, HR pay band confirmations, and facility operator pricing before any procurement authorisation is sought.

CIDB & B-BBEE

All construction and infrastructure contracts for SDU facility build-out and data centre fit-out must comply with CIDB grading requirements and target Level 1 B-BBEE suppliers where available. Procurement documentation must support PFMA compliance for government-partnered projects.

APPENDIX D

GLOSSARY OF KEY TERMS

Technical definitions for all concepts referenced in this whitepaper

Term	Definition
AES-256-GCM	Advanced Encryption Standard with 256-bit key in Galois/Counter Mode. Provides authenticated encryption. Quantum-secure as
Air-gap	Physical isolation of a computer system from any unsecured network. Data transfer requires physical media under dual-officer co
Cassandra WORM	Apache Cassandra configured with Write-Once-Read-Many semantics — no UPDATE or DELETE operations permitted on audit
CRYSTALS-Kyber (ML-KEM)	NIST FIPS 203 post-quantum Key Encapsulation Mechanism. Based on Module Learning With Errors (M-LWE) problem. Replac
CRYSTALS-Dilithium (ML-DSA)	NIST FIPS 204 post-quantum Digital Signature Algorithm. Based on Module-LWE and Module-SIS problems. Replaces RSA/EC
DEC/KEK/Master Key Hierarchy	Three-tier key hierarchy: Data Encryption Keys (90d rotation) wrapped by Key Encryption Keys (annual) wrapped by Master Key
Edge Governance Node	Compact 1–3 node appliance deployed at disconnected sites. Runs local registry mirror, audit cache, reviewer queue, and expor
Embedded Governance Fabric	The set of SDK, sidecar, host agent, gateway, and edge attachment points that embed UDOC governance into AI applications —
FIPS 140-3 Level 3	NIST Federal Information Processing Standard for cryptographic modules. Level 3 requires physical tamper-evidence and identit
Harvest-now-decrypt-later	Attack where adversary collects encrypted data today intending to decrypt using quantum computers in the future. Defeated by P
HMAC-SHA256	Hash-based Message Authentication Code using SHA-256. Used for Phase 1 audit event signing. Replaced by CRYSTALS-Dilit
HSM	Hardware Security Module. Dedicated hardware device for secure cryptographic key generation, storage, and operations. Keys n
Kubernetes Patroni	Patroni is a high-availability solution for PostgreSQL. Manages leader election via etcd DCS and performs automatic failover to s
Merkle Tree	Binary tree where each node is a cryptographic hash of its children. Root hash published every 15 minutes. Any modification to a
mTLS	Mutual Transport Layer Security. Both client and server present certificates for authentication. Mandatory for all inter-service traf
NIST PQC	National Institute of Standards and Technology Post-Quantum Cryptography. Standardisation process that produced FIPS 203 (
OPA / Rego	Open Policy Agent — policy-as-code engine. Rego is its policy language. Used for hot-reloadable constitutional policy enforceme
POPIA Section 26	Protection of Personal Information Act — Section 26 defines Special Personal Information categories: health, sexual orientation,
POPIA Section 57	Requires prior authorisation from the Information Regulator before processing criminal behaviour information. Applies to S.E.T.H
QKD	Quantum Key Distribution. Uses quantum mechanical principles (photon states) to generate and distribute encryption keys with i
Replication Factor (RF)	Number of copies of data maintained across Cassandra or Kafka nodes. RF=3 means any 2 nodes can fail without data loss. Ca
RPO	Recovery Point Objective. Maximum acceptable data loss measured in time. UDOC backbone target: 1-hour RPO via continuous
RTO	Recovery Time Objective. Maximum acceptable downtime. UDOC backbone target: 4-hour RTO at platform level with <30s data
SA AI Policy GG54477	Draft South Africa National Artificial Intelligence Policy published in Government Gazette No.54477, 10 April 2026. 86 pages. Pu
SPD	Statistical Parity Difference. Key bias metric: |P(positive outcome|group A) - P(positive outcome|group B)|. UDOC threshold: 0.05
SPHINCS+	Stateless hash-based signature scheme. NIST FIPS 205. Used for long-term archive signing where stateful schemes (Dilithium)
TPM 2.0	Trusted Platform Module version 2.0. Hardware chip providing secure key generation, remote attestation, and measured boot. R
Ubuntu AI Principle	Nguni philosophy emphasising interdependence and community. Adopted in SA AI Policy as guiding framework for AI developme
WORM	Write Once Read Many. Storage architecture preventing modification or deletion of written data. Used for Cassandra audit cluste

Term	Definition
Zero Trust	Security model that requires continuous verification of every entity attempting to access resources. No implicit trust based on net

DOCUMENT CONTROL & CERTIFICATION

Version history · Approval authority

Document	UDOC Full Technical Whitepaper — Software, Hardware & Quantum Architecture
Version	v2.0
Published	10 April 2026
Classification	CONFIDENTIAL — INSTITUTIONAL & SOVEREIGN DISTRIBUTION ONLY
Gazette Alignment	SA Draft AI Policy GG No.54477 — 10 April 2026
Author	Sashin J. Singh — Founder & Systems Architect — G.O.D.S Holdings (Pty) Ltd
Review Authority	Constitutional Oversight Board (COB) — G.O.D.S Holdings
Contact	info@gods.systems · www.gods.systems · Johannesburg, South Africa
Next Review	On publication of final SA National AI Policy (expected 2026/2027)

G.O.D.S Holdings (Pty) Ltd · Johannesburg, South Africa · 2026 info@gods.systems · www.gods.systems Sashin J. Singh — Founder & Systems Architect CONFIDENTIAL — FOR INSTITUTIONAL REVIEW ONLY This document constitutes the complete technical specification for the UDOC Sovereign AI Governance Platform. All costs are planning estimates — replace with vendor and HR quotes before procurement. All cryptographic specifications are aligned to NIST standards as at April 2026. The platform is aligned to the SA Draft National AI Policy (Government Gazette No.54477) as published 10 April 2026 — subject to update upon finalisation of the national policy in 2026/2027.