



CAHAYA SOVEREIGN AI — STANDARDS COMPLIANCE

ARCHITECTURAL COMPLIANCE MAPPING & SIRIM CERTIFICATION READINESS DOSSIER

Applicant Enterprise: LIBRAE AI LABS SDN. BHD. (1687459-T)	Document Ref: LIB-MRANTI-2026-DOC2
Founder & System Architect: Theenesan VK Kunjaayappan (theenesanvk@librae.work)	Date of Submission: August 2026
Target Facility: MRANTI Park Commercialization Sandbox & Office Residency	Classification: Sovereign Commercial Application Dossier

1. Executive Standards Statement & SIRIM Audit Strategy

This dossier provides a comprehensive, control-by-control architectural mapping of **CAHAYA Sovereign AI (MPOB Edition)** against international standards for Artificial Intelligence Governance (**ISO/IEC 42001:2023 AIMS**), Information Security (**ISO/IEC 27001:2022 ISMS**), Environmental Management (**ISO 14001:2015 EMS**), and Greenhouse Gas Quantification (**ISO 14064-1:2018 GHG**), alongside mandatory Malaysian and European regulatory frameworks (**MSPO 2.0 / MS 2530:2022** and **EUDR 2023/1115**).

KEY ARCHITECTURAL HIGHLIGHT: FORMAL STATUS DECLARATION: *Librae AI Labs Sdn. Bhd. has intentionally engineered CAHAYA's underlying software architecture, data provenance pipelines, and offline cryptographic controls from Day 1 to achieve strict 100% structural alignment with ISO/IEC 42001:2023 and ISO/IEC 27001:2022. The system is currently prepared for formal Third-Party Audit and Certification by SIRIM QAS International upon commencement of our MRANTI residency.*

2. ISO/IEC 42001:2023 Artificial Intelligence Management System (AIMS) Mapping

ISO/IEC 42001:2023 is the world's premier standard for certifying ethical, reliable, and auditable enterprise AI. The table below details how CAHAYA implements the mandatory Annex A controls directly in software architecture:

ISO 42001 Control	Mandate / Requirement	CAHAYA Architectural Implementation & Evidence	Readiness
Annex A.2 AI Risk Assessment & Mitigation	Elimination of AI hallucinations, model drift, and unverified mathematical claims in critical decision pathways.	Complete decoupling of LLM from arithmetic. All agronomic math executes in deterministic Python routines ('formula_bank.py') using certified MPOB / USDA RUSLE equations.	100% Ready
Annex A.5 Data Governance & Lineage (ISO 5259)	Verifiable tracking of all spatial inputs, training weights, and generated outputs with tamper-evident audit trails.	Every ingested boundary (KML/KMZ/Shapefile) and generated PDF is stamped with an immutable SHA-256 hash stored in an append-only ledger ('evidence_ledger.jsonl').	100% Ready
Annex A.6 Sovereign & Third-Party Isolation	Protection against unauthorized external model dependencies, cloud outages, and public network interception.	Air-gapped edge server architecture (Port 8001). Pre-compiled GGUF weights run locally on CPU/GPU via llama.cpp without external API calls or internet tethering.	100% Ready
Annex A.7 AI Transparency & Explainability (XAI)	Auditors must be able to inspect why the AI reached a conclusion, what formulas were applied, and data sources used.	Full Explainable AI (XAI) metadata drawer exposes exact mathematical equations, sensor bands, thresholds, and literature citations (e.g. Corley & Tinker 2003, Huete 2002).	100% Ready
Annex A.9 Human-in-the-Loop Oversight	AI must not execute critical automated agronomic or legal actions without explicit human verification.	Mandatory two-phase execution: CAHAYA prepares structured proposals and requires explicit user 'Approve'/'Proceed' confirmation before generating legal audit packages.	100% Ready

3. ISO/IEC 27001:2022 Information Security Management System (ISMS)

National agricultural spatial databases, estate boundary cadastrals, and yield records represent sensitive commercial assets. CAHAYA's architecture implements ISO/IEC 27001:2022 security controls across four key pillars:

- **Control A.5.15 (Access Control & Multi-Tenancy):** Strict session-level data isolation via `session\_id` tokens. Boundary coordinates and raster tiles uploaded in Session A are strictly partitioned and inaccessible to Session B.
- **Control A.8.20 (Network Security & Sovereign Boundary):** Eliminates third-party API keys and external cloud webhook leaks. The sidecar API runs on local loopback / sovereign private subnets with rate-limiting and input sanitization.
- **Control A.8.24 (Use of Cryptography):** Merkle proof verification for all compliance outputs. PDF documents and spatial GeoJSON datasets embed SHA-256 integrity signatures verifying that files have not been modified post-generation.
- **Control A.8.28 (Secure Coding & Self-Healing Watchdogs):** Zero `sleep()` loops or unhandled exceptions in background threads. System monitored 24/7 by `self\_healing\_sentinel.py` to ensure high availability and auto-recovery under edge power interruptions.

4. Alignment with ESG, Agronomic & Legal Standards

Standard / Regulation	Scope & Legal Objective	CAHAYA Built-In Compliance Engine
MSPO 2.0 (MS 2530:2022)	Principle 4 (Environmental & Biodiversity): Prohibits new planting on peat soils post-2019; mandates annual carbon stock reporting and erosion limits.	Automates SoilGrids 250m peatland identification, computes GUSLE soil loss risk (<10 t/ha/yr limit), and validates HCV buffer zones.
EUDR 2023/1115 (Articles 3, 9 & 10)	Mandates geolocation polygon coordinates for all plots >4 Ha and verifiable proof of zero deforestation after December 31, 2020.	Parses multi-polygon closed rings, matches against Landsat/Sentinel-2 2019-2020 baseline, and issues certified EUDR Deforestation-Free Audit Certificates.
ISO 14064-1:2018 (Scope 1 & 3 GHG)	Principles and requirements for quantification and reporting of greenhouse gas emissions and carbon sequestration.	Executes certified MPOB Corley & Tinker (2003) / Khalid et al. (1999) allometric biomass equations converted to t CO ₂ e under IPCC Tier 2 confidence bands.
ISO 14001:2015 (EMS in Agriculture)	Systematic management of environmental aspects, soil conservation, and water management in estate operations.	Generates dynamic Field Ground-Truthing Checklists (soil core bulk density, Ganoderma foliar trenching, peat water table piezometer calibration).

5. SIRIM QAS International Audit & Certification Roadmap

Upon securing office and sandbox facilities at MRANTI Park, Librae AI Labs will execute the following phased roadmap toward formal SIRIM accreditation:

Milestone Phase	Target Timeline	Key Audit Deliverable / SIRIM Engagement Scope	Target Status
Phase I: Gap Analysis & Dossier Submission	Month 1-2 (MRANTI)	Submit complete CAHAYA software architecture, data lineage logs, and formula verification bank to SIRIM QAS advisory for pre-audit review.	Scheduled
Phase II: Stage 1 Readiness Audit	Month 3-4 (MRANTI)	Formal evaluation of ISO/IEC 42001 AI governance documentation, risk management framework, and ISO/IEC 27001 information security controls.	Scheduled
Phase III: Stage 2 Technical Witness Audit	Month 5-6 (MRANTI)	Live witness testing of edge deployment, mathematical determinism under load, Merkle ledger integrity, and MPOB pilot compliance on MRANTI hardware.	Scheduled
Phase IV: Formal SIRIM Certification Issuance	Month 7 (MRANTI)	Issuance of formal SIRIM QAS Certification for ISO/IEC 42001 (AIMS) and ISO/IEC 27001 (ISMS) — establishing CAHAYA as Malaysia's first certified Sovereign AI.	Target Milestone

6. Standards Governance Attestation

CERTIFICATION ATTESTATION: I hereby confirm that CAHAYA Sovereign AI is structurally aligned with the stated ISO, MSPO, and EUDR standards and is fully prepared for formal SIRIM QAS International audit under our MRANTI residency.	AUTHORIZED SIGNATORY: Theenesan VK Kunjaayappan Founder & System Architect LIBRAE AI LABS SDN. BHD. (1687459-T) theenesanvk@librae.work
--	---