Adaptive Operating System - specification suite

Document: aos-readme · Source revision or record: Adopted orientation, 29 October 2026

AOS Specifications v1.0 · Edition dated 3 November 2026

Original architecture and specifications: Mark Sweeny, Governance Intelligence. © 2026 Mark Sweeny.

AOS-authored material is licensed under Creative Commons Attribution 4.0 International (CC BY 4.0).
https://creativecommons.org/licenses/by/4.0/

Preserve third-party credits. Referenced external works remain subject to their own terms.

Canonical collection: https://www.governanceintelligence.co.uk/aos

Publication copy with editorial notices, public references and disclosure edits where applicable.

Expanded README adopted by Mark Sweeny · 29 October 2026

Status: adopted orientation and navigation text. Individual specifications, approved decisions and AOS-QS retain their own authority and readiness gates. Adoption clarifies the suite's purpose and current maturity; it does not amend technical requirements or resolve the substantive questions identified in the 29 October deliverability review.

What this suite is for

The Adaptive Operating System (AOS) describes how an organisation can use AI across its work while preserving human authority, accountability, evidence and the ability to challenge how the organisation fulfils its purpose. Its initial context is UK social housing, with scope and jurisdiction governed by the individual specifications and recorded decisions.

The suite translates that architecture into component responsibilities, shared logical records and exchanges, authority and data-use rules, failure and recovery behaviour, human decision points and planned acceptance cases. Its technical specifications are written primarily for AI coding agents and the people who commission, supervise, integrate and assess their work. The explanatory material also supports suppliers and other interested readers.

The project objective is a coherent specification suite from which an AI coding agent can build and test an authorised scope without inventing material architectural or governance decisions. The present suite is a functional review draft towards that objective. Completing functional drafting does not establish readiness to build every component.

What is specified, and what remains to be done

The component and common-contract documents define proposed behaviour and obligations at a logical level. They include record fields, relationships, lifecycle conditions, permissions, ownership, acknowledgement stages and failure rules. They are more detailed than a conceptual description. They do not yet supply a complete, approved, executable integration package for a deployed AOS.

For a selected implementation, further work must bind the relevant requirements to exact compatible schemas, supported operations, endpoints, organisation instruments, approved profile values, named responsible people, evaluation methods and evidence. The scope must identify its dependencies, exclusions and unresolved questions. Material unresolved decisions must be referred to the appropriate authority; a coding agent cannot make them true by choosing a convenient default.

No AOS software test execution, whole-system implementation verification or successful institutional operation is established by these documents. Separate website software checks and a limited research-agent pilot do not establish those claims for the architecture. The suite also does not constitute a statutory compliance opinion, independent human assurance, procurement approval or a certification scheme.

How the architecture fits together

Table row 1
Part: Kernel, AOS-01-05
Responsibility: Authority and change; shared data and records; identity and permitted use; agent behaviour and lifecycle; platform enforcement, resilience and recovery.

Table row 2
Part: Sensing domains, AOS-10-14
Responsibility: Asset, Resident, People, Process and Boundary evidence and their specialist responsibilities. Process coordinates operations; Boundary governs external exchange.

Table row 3
Part: Governance Intelligence, AOS-20-25
Responsibility: Corpus, synthesis, interpretation, options, artefact assessment, presentation, oversight and learning within permitted scope.

Table row 4
Part: Governance Hub, AOS-30
Responsibility: Software support for empowered human decisions, responsibility acceptance, records and follow-through. The actual governing people and bodies retain their authority.

Table row 5
Part: Acceptance and assurance, AOS-40
Responsibility: Planned component-to-system assessment, evidence requirements, readiness and commissioning.

These are allocations of responsibility, not a requirement to buy or deploy one product per component. One product can support several functions; several products and human procedures can realise one function. “Unified data” means governed shared meaning and exchange, without prescribing one physical database.

Governance Intelligence contributes positively by bringing evidence together, identifying patterns and tensions, examining alternatives, preparing explanations and making neglected purpose concerns visible. Empowered humans judge competing goods and decide what to do. The quality of that contribution requires evaluation; neither a plausible report nor a quiet dashboard proves effective governance.

What an implementer may decide

The specifications describe required behaviour while leaving justified implementation discretion. A database, transport, policy engine, programming language, model provider or deployment arrangement can be selected where the choice preserves the required semantics, controls and accepted scope. These choices still require review where their consequences affect security, data use, compatibility or assurance.

Organisation-specific authority, permitted processing, consequential-action classifications, operating limits, human-reserved decisions, protected recipients and role appointments must be authorised by the relevant organisation. They are not merely developer preferences. Approved profiles require the validation, ownership and failure behaviour specified by the suite; a blank parameter is not zero risk or unlimited permission.

An implementer must stop and refer a material ambiguity about authority, ownership, permitted inference, source meaning, human judgement, restriction inheritance or acceptance. A technology choice that would require weakening a prohibition or transferring a responsibility is an architectural/governance change, even if expressed as configuration.

Reading status and evidence correctly

Table row 1
Wording or record: Approved architectural direction
What it establishes: A recorded project decision within its stated scope; exact requirement wording, implementation and operating authority may remain separate.

Table row 2
Wording or record: Proposed requirement
What it establishes: Reviewable normative wording; “shall” does not itself confer approval.

Table row 3
Wording or record: Planned verification case
What it establishes: An intended assessment and expected evidence; no execution or pass is implied.

Table row 4
Wording or record: Author consistency or documentary closure
What it establishes: Completion of a stated drafting/checking task within its recorded limits.

Table row 5
Wording or record: G3 - ready for authorised build
What it establishes: Under AOS-QS, competent separate quality/design review, fixed dependencies, resolved blocking findings and an approved bounded build scope.

Table row 6
Wording or record: G4 - implementation verified
What it establishes: Actual evidence against the specified baseline and scope. It does not itself authorise live operation or prove organisational effectiveness.

Table row 7
Wording or record: Operational/institutional assurance
What it establishes: Competent assessment of actual powers, people, service conditions, legal/domain duties and outcomes; some claims require longitudinal evidence.

Project custody, independent project review and an adopting organisation's operational roles are different responsibilities. An unappointed required role remains a dependency. The architecture's Change Constitution is a draft proposal for review; it has not been adopted merely because it was written. A second AI assessment is useful challenge and does not supply independent human assurance.

Counts require similar care. A requirement catalogue can include retained historical or deferred identities. Reciprocal producer and consumer obligations are not independent statistical samples. Parent cases, variants, local cases and observed endpoint results are different units. A coverage claim must name the exact active scope, method, baseline and evidence rather than rely on a total.

Distinctions that must survive implementation

An observation is not an inference; an inference is not a recommendation; a recommendation is not authority. Permission to use data does not confer permission to act. Delivery does not prove validation, accepted human responsibility, actual effect or fulfilment.

Records can therefore carry several independent states. Boundary admission can be permitted while downstream data use is withheld. Quarantine is a custody state, escalation is a routing state, and neither grants authority. The applicable contract defines the mapping; a generic “approved” flag cannot replace it.

Ownership is similarly layered. For exchange-related obligations, Boundary recognises the obligation, AOS-02 governs its shared record semantics, Process tracks accepted responsibility and fulfilment, and AOS-30 supports empowered human disposition. This does not give every participating component ownership of the same meaning. The current common register and approved decisions govern exact allocation.

The architecture requires independently enforceable controls within an explicitly assessed perimeter and threat scope. It does not establish instantaneous global revocation, control of every off-system human action, recall of disclosed information, or immunity from every privileged infrastructure actor. Declared limits must have consequences for allowed operation and assurance claims. They cannot be hidden in a disclaimer while the same guarantee is claimed elsewhere.

Purpose and use restrictions apply to derived information where the relevant rules require them. Transformation or aggregation does not by itself make information safe or grant a new purpose. The required derivation, disclosure-risk and downstream-control rules must be explicit for the implemented scope. Human referral likewise requires real empowered capacity; authentication, acceptance clicks and signatures do not prove substantive judgement.

Start here and find the controlling documents

Begin with the project objective (project-objective.md), system architecture and decision register (aos-00.md), specification map (specification-map.md) and specification quality standard (specification-quality-standard.md). Then read the relevant component specifications together with their shared contracts and acceptance material.

Table row 1
Location: 00 Foundations (../index.html#section-00-foundations)
Contents and purpose: Architectural rules and source traceability.

Table row 2
Location: 01 Reference Architecture (../index.html#section-01-reference-architecture)
Contents and purpose: The 18 component specifications and AOS-40 variants/coverage annex.

Table row 3
Location: 02 Architectural Contracts (../index.html#section-02-architectural-contracts)
Contents and purpose: Shared/Core records, Exchange Register, Control Coordination, Protected Reporting and Recovery, Operational Profiles, Contract Model and Extension/Conformance specification.

Table row 4
Location: 03 Governance of AOS (../index.html#section-03-governance-of-aos)
Contents and purpose: Proposed Change Constitution.

Table row 5
Location: Reference implementation context (../Supporting-Specifications/readme-reference-implementations.md)
Contents and purpose: First-demonstration context.

Table row 6
Location: 05 Ecosystem (../index.html#section-05-ecosystem)
Contents and purpose: Supplier alignment briefing.

Table row 7
Location: Issues register (../Supporting-Specifications/architecture-issues-register.md) and research charter (../Supporting-Specifications/aos-14-boundary-research-agent.md)
Contents and purpose: Common issues register and Boundary research-agent charter; component issues also remain in their

documents.

Table row 8
Location: 90 Architecture Records (../index.html#section-90-architecture-records)
Contents and purpose: Dated assessments, findings, dispositions and design rationale. Read their stated scope and later disposition.

Table row 9
Location: V0.1 (../index.html#section-v0-1)
Contents and purpose: Live AOS-00, map, quality standard, objective, historical source summary and selected source documents under a historical folder name.

Table row 10
Location: Phase 2 (deferred under DEC-097 and DEC-098)
Contents and purpose: Deferred applications: CAP-01 Trade-Off Divergence, CAP-02 Risk Register Assessment and RI-001 Living Specification.

V0.1 is a historical path, not a frozen release. Filenames containing v0.1 or review-draft can contain later internal revisions. Use the document's internal control record, applicable decision and the current document inventory (../Supporting-Specifications/aos-current-document-inventory-2026-10-29.md); do not infer status from a filename, folder or modification date. Where current statements conflict, record the conflict and obtain resolution rather than silently selecting one.

Under DEC-097/098, the three Phase 2 applications are deferred. Their retained IDs and source history do not create current-core acceptance obligations. General risk, independent challenge, human judgement and protected reporting remain in scope. The overdue-repair example is the first selected demonstration context; it is not the source of universal architectural rules.

Reading the suite as a supplier

Use the supplier alignment briefing (../Supporting-Specifications/aos-supplier-alignment-briefing-v0-1.md) and Extension, architectural fit and scoped conformance (aos-extension-and-conformance-specification-v0-1.md) to map a product's contribution, retained responsibilities, required exchanges, evidence and gaps.

Architectural contribution mapping can precede a deployed API. Logical contract alignment requires assessed meanings and translations. Verified interoperability requires actual compatible implementations and observations. None establishes whole-AOS certification. An illustrative product mapping is not an assessment of a supplier, product version or configuration. Existing-system data availability and effect-control capability must be established rather than assumed.

How to repeat an independent review

Supply a dated package inventory with exact document identities, internal versions, status and hashes. Include AOS-00 and its decision register, the map, objective, quality standard, governing controlled sources, component specifications, common contracts, acceptance annex, source traceability and applicable scope/deferred-status records. Identify unavailable documents explicitly. Internal conversations are unnecessary to interpret a complete public package.

Ask the reviewer to distinguish:

1. An unresolved material architectural/governance decision.
2. A contradiction, ambiguous definition, broken allocation or document-control defect.
3. Implementation or organisation-specific preparation already identified by the suite.
4. A proposition requiring experiments, competent human assessment or operational evidence.
5. A misunderstanding or missing explanation, supported by the actual controlling passage.

For each finding, request the exact document/version/section, evidence, consequence, confidence and proposed remedy. Ask

what the suite supplies today, whether it is sufficient for its stated review stage, and what remains before an authorised build. A declaration that something is “implementation detail” is insufficient if it leaves a material governing decision for the developer to invent.

Evaluate architectural obligations, specification quality, technical feasibility, build readiness and institutional effectiveness separately. Where the existing requirement is clear but untested, report the missing evidence rather than describing the requirement as absent. Where a guarantee is infeasible or ambiguous, challenge the guarantee directly. This README is orientation, not a defence against valid criticism.

A kernel feasibility experiment can test enforcement, records, races and recovery. A demonstration of AOS's wider proposition also needs evidence about Governance Intelligence's contribution to human understanding and decisions. Neither a synthetic slice nor an AI review can establish long-term organisational effectiveness.

Documentary correction edition - 29 October 2026

Mark authorised D-01-09 from the deliverability review. The correction record (../Supporting-Specifications/aos-documentary-corrections-2026-10-29.md) identifies the changes and retained limitations. The current document inventory (../Supporting-Specifications/aos-current-document-inventory-2026-10-29.md) distinguishes functional baselines, the dated editorial edition and catalogue counts. Substantive questions from the review remain separately unresolved.

Decision evidence and minutes - DEC-103, 29 October 2026

AOS distinguishes a decision’s validity/effective time, attributable record evidence/authentication, separate minutes approval and current permission to act. It imposes no universal rule that later approval of minutes creates a board decision, and no universal second board approval of separate record wording. Actual legal form, governing instruments and an approved evidence/reliance policy govern the required proof; an authenticated record may carry evidential weight without becoming conclusive or authority-creating. Missing/disputed sufficient evidence prevents affected automated reliance with accountable review; it does not itself erase a legally valid decision. Any stricter automated-reliance gate must be labelled as policy. See DEC-103 (../Supporting-Specifications/aos-dec-103-decision-validity-evidence-and-minutes-2026-10-29.md).

Protected reporting - DEC-104, 29 October 2026

Each mandatory protected-finding category requires an approved arrangement assessed against both technical failure and implicated-person interference. An implicated person cannot be the sole gatekeeper for its required authorised audience. Appropriately independent alternatives, permissions, minimal content, recipient verification, custody and continuing ownership must be established in advance and tested; an external route is included only where justified and lawfully authorised. Missing adequate arrangements remain owned gaps and prevent operational-assurance claims. See DEC-104 (../Supporting-Specifications/aos-dec-104-protected-reporting-and-implicated-recipients-2026-10-29.md).

Technical-control assurance - DEC-105, 29 October 2026

Operational reliance on technical controls requires declared scope/limits and accepted observations of enforcement paths, revocation timing/uncertainty, cumulative admission, conservative unknown effects and current-state recovery without revived permissions or repeated effects. Build/prototype authorisation is separate from implemented evidence and live approval. An experiment may establish the mechanism or expose a candidate failure; narrative assurances and a test-only pass do not supply operational assurance. See DEC-105 (../Supporting-Specifications/aos-dec-105-technical-control-limits-and-evidence-2026-10-29.md).