AOS core record contracts - detailed review draft

Document: aos-core-record-contracts-v0-1-review-draft · Source revision or record: v0.11

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.

DEC-105 adopted - 29 October 2026: Current revision 0.11. Operational technical-control reliance requires declared scope/limits and accepted observed enforcement/failure/recovery evidence; build/prototype and G4/live approval gates remain separate. Decision/amendment record (../Supporting-Specifications/aos-dec-105-technical-control-limits-and-evidence-2026-10-29.md). Earlier counts/baselines are dated history; current inventory and annex addendum control catalogue navigation. Existing non-waivable rules and DEC-099-104 retained; all new cases/variants remain planned/unexecuted.

DEC-104 adopted - 29 October 2026: Current revision 0.10. Each mandatory protected-finding category requires assessed technical-failure and implicated-person interference arrangements with an appropriately independent authorised alternative and no implicated sole release gatekeeper. Decision/amendment record (../Supporting-Specifications/aos-dec-104-protected-reporting-and-implicated-recipients-2026-10-29.md). External reporting is conditional on justified lawful authority, not a default. Exact profiles/permissions, protected_finding v0.3 compatibility and actual evidence remain gates; amended wording retains ordinary separate review and cases are planned/unexecuted. Earlier contrary or narrower baselines are history for this scope.

DEC-103 adopted - 29 October 2026: Current revision 0.9. Decision validity/effective time, attributable evidence/authentication, minutes approval and permission to execute are separate. DEC-087 is partly superseded; decision/amendment and legal-source record (../Supporting-Specifications/aos-dec-103-decision-validity-evidence-and-minutes-2026-10-29.md). No universal later-minutes or second decision-record approval gate. Exact instruments/evidence policy, KX-06 v0.3 compatibility and ordinary separate review/readiness gates remain required; cases unexecuted. Earlier contrary wording is historical only where explicitly identified.

DEC-100 adopted - 29 October 2026: Mark approved separate advance-authorised minimum control-metadata access. Current document revision 0.8; this notice supersedes earlier baseline notices for the affected scope only. See the decision and amendment record (../Supporting-Specifications/aos-dec-100-control-metadata-access-2026-10-29.md). DEC-099 remains approved. Requirements remain proposed wording implementing the approved direction; cases remain planned/unexecuted and ordinary separate review/readiness gates apply.

DEC-099 adopted - 29 October 2026: Mark approved the derived-information restriction rule. Current document revision 0.7; earlier functional/editorial baselines below are retained history. The decision and controlled amendment record (../Supporting-Specifications/aos-dec-099-derived-information-restrictions-2026-10-29.md) governs this change. Existing requirement/case/IF identities are retained; amended wording remains subject to the normal separate review and readiness gates. No case execution or operating approval is implied.

Editorial edition - 29 October 2026: Mark authorised documentary corrections D-01-09. This edition reconciles navigation, count/revision pointers, conformance links and historical scope labels; existing technical meanings, requirement/IF/decision identities and proposed/planned status are retained. The internal version below identifies the retained functional baseline; this dated editorial edition identifies the corrected document. See the current document inventory

(../Supporting-Specifications/aos-current-document-inventory-2026-10-29.md) and correction record (../Supporting-Specifications/aos-documentary-corrections-2026-10-29.md). Earlier dated adoption baselines are historical snapshots; exact logical family/view revisions are in Exchange Register §4.

Table row 1
Document control: Working identifier
Value: AOS-REC; controlled drafting annex to AOS-SC, not a new AOS component

Table row 2
Document control: Version / date
Value: 0.11 / 29 October 2026

Table row 3
Document control: Status
Value: Draft for Mark's review; definitions and obligation wording proposed

Table row 4
Document control: Scope
Value: Evidence, authority, data-use, execution and linked assurance records; common exchange version/acknowledgement supplement

Table row 5
Document control: Project owner / baseline approver
Value: Mark Sweeny

Table row 6
Document control: Author
Value: Codex, at Mark's request

Table row 7
Document control: Semantic ownership
Value: AOS-02 common record structures; AOS-02 evidence, AOS-01 authority, AOS-03 data use, AOS-04 execution behaviour with AOS-05 runtime evidence; accountable role appointments remain open

Table row 8
Document control: Independent reviewer
Value: Unassigned; independent project review deferred

Table row 9
Document control: Quality / template basis
Value: AOS-QS v0.1; component template v0.4

Table row 10
Document control: Architecture / map
Value: AOS-00/Map v0.55; DEC-001-105 with their recorded scope/status; originating adoption baselines below are history

Table row 11
Document control: Parent dossier
Value: Shared v0.27; this Core document v0.11; Exchange Register v0.26; Control Coordination v0.3; Protected Reporting and Recovery v0.3

Table row 12
Document control: Approval record
Value: DEC-002 approves ownership; DEC-028-030 approve Q01-03 architectural directions on 4 October. Exact schemas, requirements, profiles and verification results remain proposed/unassessed

Table row 13
Document control: Readiness

Value: Organised drafting annex; no G2/G3/G4 or build/activation claim

Table row 14
Document control: Change history
Value: 0.1 initial four-record draft. 0.2 incorporates DEC-062-066: REC-Q assurance, explicit incomplete assurance, immutable evaluation/later evidence sequence and common version/acknowledgement adoption; previous directions preserved 0.3 - incorporates DEC-067-072 and Control Coordination v0.1, Register v0.2 and component v0.5 adoption; original status/history preserved.

1. Purpose, authority and boundaries

The four records answer different questions: What is the evidence? Is the action within delegated authority? Is this use of the data permitted? What actually happened? Keeping those questions distinct prevents a valid observation, a technical credential or an AI proposal becoming an execution permission.

This annex develops AOS-02-IF-001 and AOS-01-IF-001 without replacing their identifiers. Data-use and execution are the companion subjects in AOS-SC §5; the controlled Kernel Exchange Register v0.1 now allocates proposed AOS-03-IF-001 / REC-D and AOS-04-IF-001 / REC-X. Allocation identifies the logical families; it is not exact-schema approval. REC-E, REC-A, REC-D and REC-X are local record-family references, not invented approved component interfaces. Participating components must ultimately reference the same approved definitions.

For this detailed drafting scope, this annex is the single proposed field/lifecycle definition. AOS-SC retains the seven-contract context, allocation and earlier obligation history. If the annex and parent differ, record and resolve the difference before approving either; a later date is not itself authority to select one. No component implementation is commissioned by creating this document.

Baseline and derivation

The supplied FP v4 and RP v6 remain governing sources. AOS-00 v0.7 §§2-6/8-10 supplies the approved decision directions and still-proposed REQ-001-049. Map v0.4 supplies responsibility boundaries. AOS-QS v0.1 QS-04-23/25-28 supplies record completeness, interface, evidence, uncertainty and readiness obligations. Template v0.3 §§4.3/5-7/9-17/19-21 supplies structure. AOS-SC v0.1 §§3-6/8 supplies the envelope, contract briefs and unresolved P01-12. FP/RP/GT source texts were read during the joint drafting immediately preceding this annex; source versions are unchanged.

Approved constraints include permanent human Mode 2; no AI boardroom observation or real-time capture; purpose-bounded processing; explicit context-specific agent delegation; withholding dependent action when authority is denied/unresolved/unavailable; separately authorised escalation; protected telos and delegation amendment; separate organisational instances; existing-system source ownership; and legible constraint explanations with recorded, reviewed exceptions. The draft translates those directions into proposed detailed semantics. Approval of an architectural direction is not approval of every field or engineering derivation below.

AOS-01 determines authority; AOS-03 determines identity and data use; AOS-04 executes within their controls; AOS-05 supplies enforceable runtime separation and recovery; AOS-02 preserves common meaning and records. AOS-13 tracks internal escalation and AOS-30 records human ownership/decisions. AOS-14 governs external exchange but cannot mint systemwide permissions. GI interprets and prepares; it cannot approve its own reserved judgement or grant itself authority.

2. Reading the field dictionaries

Every field dictionary is a proposed logical schema, independent of transport, database, API or credential format. Field names and value vocabularies are proposed; no code-generated default is authorised. R means required; C means required when its stated condition applies; O means optional and cannot be relied upon for a decision unless supplied and validated. “Reference” means an exact identity/revision reference whose target is governed by its own access policy.

Record-family and organisation profiles must fix unresolved types, cardinalities, value ranges, units, comparison rules and permissions before dependent build. Presence is not truth or valid approval. A referenced record must be resolvable by the control that relies on it; an unauthorised downstream audience may instead receive an approved disclosure projection. A reference does not permit arbitrary retrieval.

2.1 Shared header - applies to REC-E/A/D/X/Q

Table row 1
Field: record_id / revision_id
Cardinality / logical type: R / identity pair
Meaning and validation: Stable logical identity and exact revision. A changed material value creates a new revision; an old determination cannot cover it by implication. Runtime identifier format remains profile-defined.

Table row 2
Field: family / schema_revision
Cardinality / logical type: R / enum plus revision
Meaning and validation: REC-E/A/D/X/Q and exact accepted contract revision. Unsupported revisions produce a defined invalid/unresolved result, not silent coercion.

Table row 3
Field: organisation_instance
Cardinality / logical type: R / instance reference
Meaning and validation: Separate organisational scope. Cross-instance references require an explicitly approved exchange; no shared application authority is inferred.

Table row 4
Field: producer / acting_role
Cardinality / logical type: R / identity and role references
Meaning and validation: Authenticated creator and role at creation; automated actors also link accountable human role. Role membership at the time is evidenced, not assumed from current membership.

Table row 5
Field: created_at / effective_from
Cardinality / logical type: R; C / time values
Meaning and validation: Record creation time; effective time where the record governs a time-dependent state. Neither substitutes for source-event time.

Table row 6
Field: case_id / request_id
Cardinality / logical type: C / references
Meaning and validation: Case linkage where a workflow exists; request linkage for determinations/attempts. A record outside a case states that condition explicitly.

Table row 7
Field: causation_refs
Cardinality / logical type: C / ordered or unordered reference collection
Meaning and validation: Trigger/source records required to explain the record's creation. Order semantics are declared; list order alone is not execution order.

Table row 8
Field: status
Cardinality / logical type: R / family vocabulary
Meaning and validation: Current evidenced status; valid transitions are family-specific. A status label cannot authorise a transition.

Table row 9

Field: access_profile / retention_profile
Cardinality / logical type: R / exact policy references
Meaning and validation: Permitted disclosure and record-class lifecycle. Missing approval prevents using the record for the dependent purpose; quarantine/incident handling needs its own authorised policy.

Table row 10
Field: supersedes / correction_reason
Cardinality / logical type: C / reference plus text/category
Meaning and validation: Required for correction/supersession. Correction cannot silently rewrite the history of an already executed action.

Table row 11
Field: limitations
Cardinality / logical type: R / explicit collection
Meaning and validation: Known missing/conflicting/stale evidence and uncertainty. Empty means no limitation identified by the stated checks, not proof of completeness.

Time value: a calendar date has date precision and calendar context; a timestamp has timezone/offset or an unambiguous time basis, precision and known clock uncertainty. Preserve source precision. Do not invent a midnight timestamp from a promised date. P02 covers comparison semantics and clock tolerance.

Identity: agent identity, deployment identity, model identity, service identity, human principal and accountable human role are different fields where relevant. A model name is not an authenticated actor. Exact verification assurance is profile-defined under P04.

Unavailable / unknown / not applicable / withheld: use a structured value-status, not an ambiguous blank. A required unresolved value prevents a dependent favourable determination. Intentionally withheld data identifies its approved disclosure rule without exposing protected content. A “not applicable” value includes its reason and profile basis.

2.2 Common exchange supplement, v0.2

Every REC family adopts Kernel Exchange Register v0.1 §3 envelope supplements and exact logical types, §4 revision/acknowledgement manifest and §5.2/5.13 compatibility and stage-evidence shapes. Record header and exchange envelope remain distinct views bound to the same exact payload revision. Source revisions retain their original definition metadata. Accepted translations retain both original and translated revisions plus mapping/use-acceptance evidence; they do not rewrite original records. Later execution/acknowledgement evidence is linked as separately versioned records, subject to governed deletion/disclosure, not inserted as if known at original evaluation.

DEC-099 - derived-information restriction rule

Every transformation or combination must preserve the applicable restrictions of its contributing sources. The proposed use of the resulting information must satisfy those restrictions and account for any additional sensitive information the combination reveals. If the system cannot establish the lineage or permitted use sufficiently, it must withhold that use and refer the uncertainty for accountable review.

Applies to summaries, aggregates, embeddings/search indexes, joins, exports and restored derived copies within the declared governed scope. Transformation supplies no wider purpose or permission; conflicting restrictions can prevent the proposed combination. A different treatment requires an evidenced authorised determination under the governing rules, never mere notice or developer discretion. Completed disclosures and unreachable external copies remain explicit limitations with accountable handling; no recall or universal forgetting guarantee is made. AOS-03 REQ-011/012 and the existing necessity, explicit-consent, separate-governance and review-cycle conditions are retained; no new personal-inference exception is created.

AOS-02 owns common lineage/restriction record meaning and the scoped transformation inventory; AOS-03 owns the

independent operation/purpose-specific permitted-use assessment. Producers supply attributable source/transformation evidence; receiving components must establish the current permission for their intended use. An unresolved case retains its accountable review duty. Exact profile definitions, evidence sufficiency, source-combination rules, permitted transformations, destination inventory and enforceable withdrawal/recovery behaviour must be fixed and assessed before dependent implementation reliance. This decision adds no default policy, wire schema or automatic override.

DEC-100 - independent minimum control-metadata access

The organisation shall authorise in advance a separate, tightly bounded permission for its checking services to read only the minimum control information necessary to assess a request. That permission must be verifiable independently of whether the requested business action is allowed. It grants no wider access to resident, employee or other operational information. If the required permission or current control information cannot be verified, the affected action remains withheld and the uncertainty is referred for accountable handling.

The control profile identifies the checking service/identity, approving authority and instrument, organisation, permitted metadata records/fields and read operations, assessment purpose, validity/withdrawal/currentness evidence and accountable review route. A service does not obtain this permission from the business request, a model instruction or a favourable result issued by the other check. AOS-01 owns authority for the checking operation; AOS-03 owns permitted metadata use; AOS-02 preserves controlled records; AOS-05 enforces the declared access boundary. Startup and recovery must establish the advance permission/current state through an independently usable approved verification path; no unbounded bootstrap identity, data access or outage privilege is inferred. Separately permitted service/human fallback retains its own authority and duties. Exact profile, verification mechanism and compatibility/evidence are prerequisites before dependent reliance; this direction supplies no credentials, wire schema or live operating permission.

DEC-103 - separate decision, evidence, minutes and execution

AOS shall distinguish the validity and effective time of a human decision, the provenance/authentication and evidential standing of its record, the separate approval status of minutes, and current permission to execute an action. It shall assess decision validity and sufficient evidence under the organisation’s applicable law, legal form, constitution/registered rules, powers and approved evidence/reliance policy. It shall not universally require later minutes approval to bring a decision into existence, nor require a second board approval of a separate decision record where those applicable arrangements do not require it.

Minutes approval and authentication are evidence events, not universal substitutes for the actual decision process. An authenticated record or extract may support reliance through an authorised evidence route, but neither its signature nor its label can manufacture a decision, cure missing powers/conditions or make disputed evidence conclusive. Preserve actual decision, record, authentication/approval, effective and execution times separately; no automatic backdating. Contradictory, missing or insufficient evidence withholds affected automated reliance for accountable human resolution without declaring that an otherwise valid legal decision does not exist. Organisation-specific additional assurance gates may be adopted, but must be labelled as AOS/organisation reliance policy rather than general law. Separately authorised urgent/service duties remain owned. Minute-taker drafting and Company Secretary stewardship remain distinct; human decision powers, protected constitutional processes, boardroom AI exclusion, current authority/data-use checks and DEC-088/089 remain unchanged.

The approved organisation profile binds legal form/jurisdiction, actual constitution/registered rules and powers, valid decision/record/authentication routes, relevant statutory evidence standing, exact required source/validity conditions and competent evidence-assessment/escalation roles. AI cannot infer unseen deliberation or declare legal validity; record the authorised human assessment and limits. No compulsory extra decision-wording approval is invented. A stricter automated-reliance threshold is explicit policy. KX-06 v0.3 is a revised logical view; exact types, code lists, required/conditional fields and reviewed old/new consumer compatibility must be fixed before dependent use. DEC-087 original text is history to the extent superseded; role separation and protected powers remain.

DEC-105 - declared technical control limits and observed assurance

Operational reliance on implemented technical controls requires explicit scope, limits and failure/recovery behaviour supported by accepted observed evidence. The evidence must cover all enabled action paths within the declared control/threat scope, independently of the acting agent; permission-change enforcement points and timing uncertainty; shared cumulative bounds under concurrency; conservative treatment of unknown effects/reservations; and recovery that applies current restrictions without reviving withdrawn authority or repeating completed effects.

The approved control profile fixes exact functions/paths/dependencies/versions, threat assumptions, effect boundary, currentness and revocation/fencing mechanism, timing/uncertainty bounds and units, accounting scopes/consistency and admission, uncertain exposure/release evidence, recovery source/currentness/completeness, permitted fallback/continuing duty, observability/oracle, assessors and objective acceptance conditions. Timeout, cancellation, worker retirement or failover alone cannot prove no effect, release possibly used capacity or permit consequential repetition. No instantaneous global revocation or recall of an irreversible disclosure is promised. Limits are assessed under actual constraints and powers, not silently accepted as waivers of non-waivable safeguards. Missing/failed evidence blocks affected operational-reliance claims with an owned remedy; separately authorised service/reporting duties remain owned and do not acquire extra permissions.

G3 remains authorisation of a bounded build with fixed scope, explicit dependencies/profiles and required separate review; G4 requires implemented observations, and actual operational approval is separate. An explicitly authorised bounded prototype can investigate the mechanisms before operational assurance exists; this decision itself authorises neither a prototype nor live effects. A failed prototype requires investigation of the implementation, assumptions and alternatives; it is not alone proof of architectural impossibility. Model refusal, a generated explanation, intended configuration, an old checkpoint or retrospective log alone is not evidence that all effect paths were enforced or recovery was current. Actual acceptance must link observations to the exact requirement/local-case/variant/profile and endpoint scope, with limitations and competent assessor disposition.

AOS-05 produces control-boundary/dependency observations and declares the implemented limits with authoritative semantic/control owners. AOS-40 evaluates scoped acceptance and preserves build, implementation-verification and operational approval distinctions. Approved profile/instrument owners determine legitimate settings; accountable human assessors disposition limitations without waiving non-waivable constraints.

3. REC-E - evidence exchange

Existing interface: AOS-02-IF-001. Semantic owner: AOS-02 with relevant domain source stewardship; accountable role-holder appointment open. Producer → consumer: approved source adapter/domain/human input → governed record admission and authorised consumers. Purpose: transfer evidence without losing provenance, meaning, uncertainty or use restrictions.

3.1 Evidence record fields

Table row 1
Field: evidence_kind
Requirement / type: R / enum
Meaning and validation: observation, inference, source_statement or governed_record_reference. Decision/approval records are referenced through their owning contract, not created by relabelling an observation.

Table row 2
Field: subject_refs
Requirement / type: R / typed references
Meaning and validation: Entities to which the evidence applies; identifier namespace and organisation scope explicit. Unknown subject is an admission exception, not a guessed match.

Table row 3
Field: fact_type / payload_schema
Requirement / type: R / semantic key and revision
Meaning and validation: Meaning of the fact and exact payload contract; units/ranges come from the domain profile.

Table row 4
Field: payload_or_reference
Requirement / type: R / one selected form
Meaning and validation: Governed content or exact content reference; chosen disclosure is authorised. Unavailable referenced content is not silently treated as validated.

Table row 5
Field: source_system / source_record_revision
Requirement / type: R / source references
Meaning and validation: Origin and exact source revision. An adapter's receipt timestamp is not a source version.

Table row 6
Field: source_authority_profile
Requirement / type: R / registry reference
Meaning and validation: Which source is authoritative for this fact and purpose; a system may be authoritative for an internal target but not the resident-communicated promise.

Table row 7
Field: occurred_at / observed_at / received_at
Requirement / type: C; C; R / time values
Meaning and validation: Distinguish event, observation and receipt time; at least the time required by the fact profile must be known. Delayed arrival is visible.

Table row 8
Field: collected_for / basis_refs
Requirement / type: R / purpose and approved-basis references
Meaning and validation: Original collection purpose and the governance basis applicable to the data; no assumption that consent is the only possible basis or that possession supplies one.

Table row 9
Field: permitted_uses / restrictions
Requirement / type: R / profile references and conditions
Meaning and validation: Processing, inference and disclosure constraints. They are inputs to a current data-use determination, not an irrevocable licence.

Table row 10
Field: provenance_refs / transformations
Requirement / type: R; C / lineage records
Meaning and validation: Input and transformation lineage; inference cites its evidence/model/configuration and remains inference. Source authenticity and substantive truth are separately assessed.

Table row 11
Field: quality_assessment
Requirement / type: R / profile-shaped result
Meaning and validation: Completeness, currency, conflict, source verification and relevant measurement limitations. A confidence value identifies method/rubric and evaluation status.

Table row 12
Field: related_or_conflicting_evidence
Requirement / type: C / references
Meaning and validation: Known contradiction, correction, corroboration or supersession; its relationship type is explicit.

Table row 13
Field: admission_result
Requirement / type: R / enum and reason
Meaning and validation: accepted, accepted_with_restrictions, rejected or unresolved. Record the validating profile/revision and checks. Restricted storage is not permission for operational use.

Table row 14
Field: impact_review_refs
Requirement / type: C / references
Meaning and validation: Required when correction/conflict affects analyses, determinations, pending actions or recorded outcomes under the approved impact rule.

3.2 Admission and correction

Proposed evidence lifecycle: submitted → validation_pending → accepted / accepted_with_restrictions / rejected / unresolved. Accepted material can later be superseded, disputed, access_restricted or deleted under policy. Those later conditions may coexist; a single enum must not erase a still-relevant restriction. The final encoding may therefore separate admission status from currency/access status.

Admission checks use only the metadata/content accessible under the admission purpose. A denied operational use does not authorise an unrestricted quarantine repository. Quarantine, incident evidence and preservation rights require separately approved permissions and retention rules.

An acceptance acknowledgement names the exact admitted revision and restrictions. It does not certify the source's claim as true. Repeated submission of the same source-event identity and same content is a duplicate, with a link to the original. Same identity with materially different content is a conflict/invalid replay; do not overwrite it as a benign duplicate. Profile-specific content comparison remains P02, rather than mandating a hash algorithm.

Use source revision/effective-time semantics within the entity/fact's declared ordering scope. Receipt order alone never establishes which statement governs. Correction preserves the link to earlier evidence and initiates the defined impact review. Under approved Q02/DEC-029, pause and reassess only pending work materially dependent on corrected or disputed evidence. Preserve completed history and conduct accountable impact review of significant consequences. Unrelated work continues; materiality, dependency mapping and accountable review roles remain to be specified.

3.3 Repair evidence profile - illustrative fields, proposed semantics

Table row 1
Fact: Resident-communicated completion promise
Additional fields and distinction: repair_id; promised_completion_value; precision/calendar context; communicated_at; authorised resident/channel reference; communication evidence; source revision; change authority/evidence where changed. An internal target is a separate fact_type.

Table row 2
Fact: Repair completion
Additional fields and distinction: repair_id; completion state; claimed/verified completion time; source and verification evidence; known disagreement or unresolved partial completion. A “job closed” flag cannot silently equal completed repair without the approved source profile.

Table row 3
Fact: Promise amendment
Additional fields and distinction: earlier promise reference; revised value; source/human authority and resident communication evidence; reason and effective time. Arrival of a later target date is not proof that the resident's promise changed.

Table row 4
Fact: Contact provision
Additional fields and distinction: case/repair reference; named case owner role/holder and accountable team; authorised contact/channel details; attempt/delivery evidence; known unusable-contact limitation. Record references rather than duplicating personal contact data in every log.

DEC-022 fixes the resident-communicated date as the trigger. DEC-036-040 approve comparison, promise-amendment, completion-evidence, uncertainty and partial-scope directions; Operational Profiles v0.1 supplies the current disposition. Actual mappings and evidence-rule detail remain explicit settings; no grace interval or silent reset is implied.

3.4 REC-Q - linked fact assurance (KX-08)

REC-E §3.1 adds required assurance_refs (0..n exact REC-Q references) and required assurance_status (unassessed, partial, disputed, validated_for_purpose). An empty collection requires explicit unassessed/no-access basis; it is never truth certification. Origin, admission, assurance and intended-use suitability are separate. REC-Q uses the §2 header plus the following single common definition.

Table row 1
Field: fact_revision / fact_scope
Cardinality / logical type: R ref; R scope
Meaning and validation: Exact evidence/fact revision and assessed fields/claim; a changed fact cannot inherit validation silently.

Table row 2
Field: assessment_status
Cardinality / logical type: R enum
Meaning and validation: unassessed, partial, disputed, validated_for_purpose; interpreted for the stated scope/method, never generic truth.

Table row 3
Field: supporting_evidence
Cardinality / logical type: R 0..n refs
Meaning and validation: Exact evidence revisions; empty only with explicit unassessed/absent-evidence reason.

Table row 4
Field: method / criteria / method_version
Cardinality / logical type: C exact refs
Meaning and validation: Required where assessment/validation performed; for unassessed record explicit not-applicable reason. A confidence number cannot substitute.

Table row 5
Field: validator_identity
Cardinality / logical type: C ref
Meaning and validation: Actual human/service validator where validation occurred; absence/unknown explicitly visible.

Table row 6
Field: accountable_role
Cardinality / logical type: R ref
Meaning and validation: Role accountable for the assessment/status assertion, including unassessed/disputed records. Appointment evidence is a commissioned dependency.

Table row 7
Field: assessed_at / applies_at
Cardinality / logical type: R time; C time
Meaning and validation: Assessment/status-recording time and fact-period applicability where distinct. Preserve precision/clock limits.

Table row 8
Field: purpose_scope
Cardinality / logical type: R scope
Meaning and validation: Intended purpose and context covered; validation for one purpose does not validate all uses.

Table row 9
Field: currentness_profile / currency
Cardinality / logical type: R ref; R value
Meaning and validation: Required freshness criteria and known currentness/expiry limitations. Exact time bounds commissioned.

Table row 10
Field: limitations / coverage
Cardinality / logical type: R collections
Meaning and validation: Missing, stale or conflicting support and assessed/excluded coverage; empty does not prove completeness.

Table row 11
Field: competing_assessments / disagreement
Cardinality / logical type: C refs; C classified text
Meaning and validation: Required for known conflicting relevant assessments; retain each exact revision and differing scope/method. No latest-arrival precedence.

Table row 12
Field: assurance_lifecycle
Cardinality / logical type: R enum
Meaning and validation: current, superseded, withdrawn, restricted; separate from assessment status. Corrected/withdrawn assurance remains governed history, not a continuing suitability grant.

Table row 13
Field: correction_or_withdrawal_basis
Cardinality / logical type: C ref
Meaning and validation: Required for supersession/withdrawal; restrictions/deletion use approved lifecycle, with no hidden payload copies.

Multiple REC-Q assessments may apply to one fact revision. A consumer's suitability record is required when assurance affects its conclusion/action: exact fact and assessment refs, intended purpose, required-assurance profile, result (suitable, unsuitable, unresolved), checked currentness/conflicts/limitations, evaluator/date and reason. It is a consumer evaluation under KX-01/08, not another independent source of fact truth. Inaccessible material evidence or unmet required assurance yields unresolved/unsuitable reliance; an independently permitted referral can still report the limitation. Projections retain permitted supporting references, scope and limitations.

DEC-062/063 approve these directions; fields remain proposed. KXR-03/04 and KXV-02/06 in the register supply requirement/case allocation. Origin provenance_refs and quality_assessment remain present; they cannot silently stand in for this chain.

4. REC-A - authority determination

Existing interface: AOS-01-IF-001. Semantic owner: AOS-01. Producer → consumer: authorised authority control → executor and other controls. Purpose: establish permission for a specific proposed action in the current domain, context and conditions. GI's interpretation may inform the case; it cannot be the sole authority grant.

4.1 Action request - shared input to REC-A, REC-D and REC-X

Table row 1
Field: action_request_id / revision
Requirement / type: R / identity pair
Meaning and validation: Exact proposed action; material change requires reassessment.

Table row 2

Field: actor / principal / accountable_role
Requirement / type: R; C; R / references
Meaning and validation: Acting identity, delegating human/organisational principal where applicable, and accountable human role. Identity verification and delegation linkage remain distinct.

Table row 3
Field: action_type / target_refs
Requirement / type: R / semantic type and references
Meaning and validation: Defined operation and target scope; “send”, “change”, “approve” or “read” without scope is insufficient.

Table row 4
Field: material_parameters
Requirement / type: R / typed profile
Meaning and validation: Data/payload revision, destination, amount/unit, scope, channel, timing and other values relevant to this action. Exact relevant-field list is defined by the action profile, not left to model judgement.

Table row 5
Field: domain / purpose / context_refs
Requirement / type: R / defined references
Meaning and validation: Domain and authorised purpose, current contextual facts and conditions; changes may invalidate permission.

Table row 6
Field: delegation / instrument_refs
Requirement / type: R / exact revisions
Meaning and validation: Claimed authority and approved organisational instruments; absence is not inferred permission.

Table row 7
Field: consequential_classification
Requirement / type: R / profile result
Meaning and validation: Classification under the organisation's approved schedule; unresolved/unapproved classification cannot enable the affected capability.

Table row 8
Field: human_decision_refs
Requirement / type: C / exact approved records
Meaning and validation: Required when reserved or action-specific approval applies. A draft or an approval of another revision is insufficient.

Table row 9
Field: requested_effect / preconditions
Requirement / type: R / action-profile values
Meaning and validation: Observable proposed effect and necessary conditions; distinguish preparation from external commitment.

Table row 10
Field: related_attempts
Requirement / type: C / references
Meaning and validation: Prior execution, retry or reconciliation context; a new request must not hide an unknown prior effect.

Requests to the control functions themselves need approved access and data-use scopes. Evaluation cannot bootstrap its right to inspect unrestricted personal data from the action it is evaluating.

4.2 Authority result fields

Table row 1
Field: request_binding

Requirement / type: R / exact request revision and bound-field values/references
Meaning and validation: Defines the action/context covered. Binding is semantic here; implementation integrity protection remains AOS-05 work.

Table row 2
Field: determination
Requirement / type: R / enum
Meaning and validation: allow, deny or unresolved. “Unresolved” includes missing/conflicting required authority facts; operational unavailability is recorded separately as a control-call failure, not a fabricated determination.

Table row 3
Field: authority_basis
Requirement / type: R / exact instrument/delegation references
Meaning and validation: Applicable permissions, prohibitions, reserved decisions and conditions actually evaluated. For unresolved results, identify which required basis is unavailable.

Table row 4
Field: policy_state_refs
Requirement / type: R / current-state evidence
Meaning and validation: Versions and applicable suspension/revocation restrictions examined; a policy document's revision alone does not prove no later suspension exists.

Table row 5
Field: applicable_conditions
Requirement / type: R / structured conditions
Meaning and validation: Explicit obligations for the exact action; unknown required condition is not satisfied.

Table row 6
Field: validity / invalidation_triggers
Requirement / type: R / action-profile terms
Meaning and validation: Effective start, expiry if prescribed, permissible context and events that invalidate permission. No invented lifetime or indefinite cache licence.

Table row 7
Field: execution_checkpoint_rule
Requirement / type: R / approved profile reference
Meaning and validation: Where current authority is confirmed relative to actual effect, and how interruption/change races are handled. DEC-028/067 direction is approved; Control Coordination v0.1 §3 defines the logical checkpoint/race protocol; actual boundary/freshness/tolerance values remain commissioned. A timestamp is not enforcement proof.

Table row 8
Field: data_use_link
Requirement / type: C / request/result reference
Meaning and validation: Relevant data-use determination and operation scope where personal/restricted data is used. A valid link does not mean its result is permit.

Table row 9
Field: explanation
Requirement / type: R / structured statement
Meaning and validation: Constraint meaning, authority basis and separately authorised escalation route; default supplied under DEC-027.

Table row 10
Field: explanation_exception
Requirement / type: C / controlled record
Meaning and validation: Security/privacy/feasibility reason, disclosure scope, required reviewer/authority and review/effectiveness evidence. An exception does not change deny to allow.

Table row 11
Field: evaluator / evaluation_evidence
Requirement / type: R / control identity and evidence references
Meaning and validation: What evaluated the request and which rules/input revisions were used; contemporaneous evidence, not private chain-of-thought.

4.3 Use and invalidation

Proposed lifecycle: requested → evaluated → allow / deny / unresolved. A favourable determination is subsequently valid, expired, invalidated or already used under the action profile. “Used” is not proof of effect, and reuse rights are never inferred from its status.

Dependent execution requires an allow for the exact action/context and satisfaction of all current conditions. Deny, unresolved, unavailable, expired, revoked, unsupported profile or mismatched request withholds the dependent action. A separately permitted internal referral or safety fallback may proceed; it must have its own current permissions and does not create emergency authority for the original action.

Approved Q01/DEC-028 requires current authority and data-use validation at the last enforceable point before a consequential effect; the actual boundary and handling of changes during irreversible action remain to be specified. Pending work affected by changed delegation, suspension, actor role, material context or governing policy is reassessed. A change after an irreversible effect cannot retroactively prevent it; retain the ordering/effect evidence and follow the approved incident/follow-up route. No claim of instant global revocation or invulnerable enforcement follows from this lifecycle.

Human approval must correspond to the underlying powers and exact decision/action scope. A human override of analysis cannot override that person's authority limits. Telos amendment stays board-only; schedule amendment retains executive proposal, Committee review and board sign-off; suspension and reinstatement use the approved operational schedule.

5. REC-D - data-use determination

Catalogue identifier: proposed AOS-03-IF-001 / KX-03; schema wording remains proposed. Semantic owner: AOS-03. Producer → consumer: authorised identity/access/data-use control → producer/admission, analytical component, executor or disclosure control. Purpose: decide whether this actor may perform this operation/inference on these data for this purpose, under the approved basis and restrictions.

5.1 Data-use request and result fields

Table row 1
Field: data_use_request_id / revision
Requirement / type: R / identity pair
Meaning and validation: Exact scope evaluated; may be linked to an action request without becoming the same record.

Table row 2
Field: actor / acting_role / assurance_refs
Requirement / type: R / references
Meaning and validation: Authenticated identity, relevant role and assurance evidence. Service access is not unlimited organisational permission.

Table row 3
Field: data_scope / revision_selector
Requirement / type: R / typed references
Meaning and validation: Fields/entities/datasets and selected revisions, or explicit permitted dynamic-selection rule. “All UDL data” is not

a default scope.

Table row 4
Field: operation / inference_type
Requirement / type: R; C / enums or governed semantic keys
Meaning and validation: collection, read, transformation, inference, disclosure, retention, correction or deletion; exact profile-defined meaning. An inference operation declares what it proposes to infer.

Table row 5
Field: purpose / collection_purpose_refs
Requirement / type: R / purpose references
Meaning and validation: Requested use compared with original purposes and restrictions. New governance approval is needed where applicable; technical availability supplies none.

Table row 6
Field: basis_refs / consent_state_refs
Requirement / type: R; C / exact governance records
Meaning and validation: Approved processing basis; current consent scope/state if that basis depends on consent. The contract makes no unverified legal-basis finding.

Table row 7
Field: recipient / onward_use / location_profile
Requirement / type: C / references
Meaning and validation: Required for disclosure/external processing; recipient, permitted onward use and approved location/access arrangements. No blanket UK-only or overseas permission is inferred.

Table row 8
Field: sensitivity / information_barriers
Requirement / type: R / profile values
Meaning and validation: Applicable classification, field-level limits and resident/workforce/domain separation. Unclassified required data remains unresolved.

Table row 9
Field: result
Requirement / type: R / enum
Meaning and validation: permit, deny or unresolved. A failed control call is unavailable and provides no permit result.

Table row 10
Field: permitted_scope / conditions
Requirement / type: R / scoped values
Meaning and validation: Exact authorised operation, data, purpose, disclosure and further-use constraints. A narrowed scope is a different checked request/result, not a quiet edit of the original.

Table row 11
Field: policy_state / validity / invalidation
Requirement / type: R / profile references
Meaning and validation: Checked policy/basis/consent versions and current restrictions; approved expiry and invalidation rules.

Table row 12
Field: explanation / exception_ref
Requirement / type: R; C / structured explanation and reference
Meaning and validation: Meaning, basis and referral route by default; reviewed exception under DEC-027 where applicable.

Table row 13
Field: evaluator / evaluation_evidence
Requirement / type: R / control and evidence refs
Meaning and validation: Verified input/rule versions and the actual result. A source saying “consent obtained” without required scope/state evidence is not validation.

5.2 Processing and onward use

Proposed lifecycle: requested → evaluated → permit / deny / unresolved, followed by valid / expired / invalidated for reliance on the result. Authority and data use are separate checks: permitted data processing does not grant authority to commit an organisation, and an authorised action does not enlarge consent or processing scope.

Evaluate both against independently approved instruments. REC-A and REC-D can reference the same request/context; neither derives its favourable result solely from the other's favourable result. At execution the required results are combined. The evaluation sequence, dependencies and minimal permitted metadata access are fixed in the action/data-use profile so there is no circular permission bootstrap.

Receiving components check their proposed use. Derived records retain source-purpose and restriction lineage; a transformation, summary, embedding or cross-domain join cannot erase restrictions. Where further use is separately approved, preserve the new basis and its relationship to the original obligations rather than relabelling historical consent.

Consent withdrawal, expiry or correction invalidates uses dependent on that consent under the approved profile. It does not automatically erase an independent retention obligation, authorise a welfare exception, undo completed processing or permit all alternate uses. The permitted stopping, deletion/restriction, downstream notification and evidence retention paths must be governed. DEC-051 settles the bounded human welfare-protocol direction; actual board instruments, verified basis and exceptional-inference constraints remain D05/P05. Refer conflicts; no default override.

Asset-condition monitoring cannot silently become occupancy/routine monitoring. Resident-assistant access cannot silently become enterprise profiling. People/process data cannot inherit new performance/surveillance uses because an analysis is operationally convenient. Those are receiving-operation checks as well as data-design obligations.

5.3 Original evaluation and later evidence - DEC-064

evaluator/evaluation_evidence records contemporaneous request, actual input/instrument revisions, method/control version, result and conditions. Permission issuance cannot require proof of future execution. The original REC-A/REC-D revision is immutable as historical evidence, subject to authorised correction, supersession and lifecycle rules. A change creates a new revision, not a rewrite of the original evaluation.

A separately versioned evidence link identifies the exact original determination, exact REC-X attempt, checkpoint evidence, actual enforcement/effect evidence and known limitations. It records link_state (pending, evidenced, withheld, indeterminate) and actual observation time. Pending/absent evidence cannot prove enforcement. For denied/withheld work preserve the blocker and available control observations; absence of effect is claimed only when evidenced. REC-X §6.1 consumes these exact links. REC-A and REC-D independently evaluate approved instruments; minimal approved metadata access avoids circular bootstrap. Control Coordination v0.1 §3 now defines the logical snapshot/check/race handling; implementation and numerical operating values remain commissioned.

6. REC-X - execution attempt and observed result

REC-X / CHECK ownership clarification - 29 October 2026: AOS-04 owns the enclosing REC-X execution meaning; AOS-05 owns/supplies the runtime combined CHECK evidence. The existing REC-X.final_control_check references CHECK, while observed effects are recorded separately. AOS-02 supplies common structure/custody. See the current Exchange Register §4 (aos-kernel-exchange-register-v0-1.md) for family/view revisions and owners. No field, owner or runtime obligation is changed by this cross-reference.

Catalogue identifier: proposed AOS-04-IF-001 / KX-04; schema wording remains proposed. Semantic owner: AOS-04 for execution contract; AOS-05 supplies runtime evidence and AOS-02 the shared structure. Producer → consumer: bounded executor/runtime control → governed records, AOS-13/14 workflow reconciliation, authorised humans and oversight. Purpose: reconstruct what was attempted and observed, including prevention, partial effect and uncertainty.

6.1 Execution fields

Table row 1
Field: execution_id / attempt_id
Requirement / type: R / identity pair
Meaning and validation: One logical execution and distinct attempts. A retry references the same intended effect and prior attempt unless an authorised new action is created.

Table row 2
Field: action_request_ref / bound_action
Requirement / type: R / exact revision and profile values
Meaning and validation: The requested action actually attempted; material target/payload/context changes require new checks.

Table row 3
Field: executor / deployment / model_tool_refs
Requirement / type: R; R; C / exact references
Meaning and validation: Acting executor and deployed configuration; relevant model/tool versions where used. A deployment capability is not a delegation.

Table row 4
Field: authority_result / data_use_results
Requirement / type: R; C / exact references
Meaning and validation: Authority allow and applicable permit records, or the failure/blocking evidence when execution was withheld.

Table row 5
Field: final_control_check
Requirement / type: R / evidence reference
Meaning and validation: Current versions, conditions and checkpoint result examined under the approved profile. Control Coordination v0.1 §3 CHECK supplies logical binding/fencing/reservation composition; selected P03 mechanisms/values and executed evidence remain prerequisites to conformant execution.

Table row 6
Field: intended_effect / affected_targets
Requirement / type: R / action-profile values
Meaning and validation: Observable intended operation and its defined scope. Distinguish dispatch, acceptance and external effect.

Table row 7
Field: duplicate_key / ordering_scope
Requirement / type: R / profile-defined identity/scope
Meaning and validation: Same-effect attempt identity and per-case/entity ordering terms. No universal exactly-once or total-order guarantee is inferred.

Table row 8
Field: pre_effect_record_ref
Requirement / type: C / runtime evidence
Meaning and validation: Required for consequential actions under the proposed reconstructability rule: intended action and control checkpoint recorded before the effect boundary. P09 fixes unavailable-audit fallback.

Table row 9
Field: started_at / effect_boundary_at / finished_at
Requirement / type: C / time values

Meaning and validation: Observed execution timing; absent timestamp records why it is unknown, rather than fabricating order.

Table row 10
Field: attempt_state
Requirement / type: R / enum
Meaning and validation: prepared, withheld, running, dispatched, awaiting_evidence, concluded or interrupted. States describe the attempt, not the case's human disposition.

Table row 11
Field: observed_effect
Requirement / type: R / enum plus detail
Meaning and validation: none_confirmed, full_confirmed, partial_confirmed or indeterminate. Full confirmation means the defined technical effect, not all service/governance obligations completed.

Table row 12
Field: effect_evidence / limitations
Requirement / type: R / governed refs and uncertainty
Meaning and validation: Actual receipts/source outcome evidence and what they establish. A successful API response may prove only acceptance.

Table row 13
Field: failure / interruption_reason
Requirement / type: C / classified record
Meaning and validation: Failed control, invalid input, runtime outage, remote rejection, permission invalidation or other defined event; distinguish known failure from unknown effect.

Table row 14
Field: reconciliation_state / next_action_ref
Requirement / type: C / status and reference
Meaning and validation: Required for partial/unknown result or unresolved obligation; owner, permitted query/follow-up, deadline and disposition path. Unknown external state cannot become “failed, safe to retry” without evidence.

Table row 15
Field: closure / obligations_remaining
Requirement / type: C; R / governed record
Meaning and validation: Attempt closure authority/reason where relevant; remaining case/contact/remediation duties, even after technical effect is confirmed.

6.2 Attempt, effect and case states

Proposed normal route: prepared → current controls confirmed → running → dispatched/awaiting_evidence → concluded. Before the effect, denial or invalidation produces withheld. A crash can produce interrupted with indeterminate effect; interruption is not evidence that nothing happened.

Attempt state, observed effect and case lifecycle are separate axes. A concluded attempt may have a known failure, partial result or explicitly unresolved outcome. A transport acknowledgement can conclude a dispatch attempt while actual effect remains indeterminate and reconciliation stays open. Human receipt/ownership/disposition and resident contact requirements live in escalation/decision contracts and remain visible through references.

Before a consequential repeat, establish the prior attempt's possible effect under an authorised reconciliation route. Approved Q03/DEC-030 blocks automatic consequential repetition until an approved action profile establishes permitted continuation without duplication or compounding, or an authorised human decides the permitted next action. Status queries are distinct actions requiring permission. Timeout indicates uncertainty rather than failure; accountable handoff owner, deadline and cover remain to be specified. Such a decision cannot waive foundational constraints or claim to reverse an irreversible disclosure. Compensation, cancellation and repair are distinct actions needing their own authority/data-use checks.

If the required record/enforcement capability is unavailable before the effect, withhold the dependent automated action and use the approved separately authorised fallback. A validated alternative recording boundary may be part of the eventual platform design, but “we will log it later” is not a conformant default. Human safety responsibility continues through the approved fallback; this draft supplies no unavailable-record emergency permission.

After restart, load actual policy/suspension state, reconcile attempts and revalidate affected work before continuation. Restoring an old checkpoint or model configuration cannot restore suspended authority. If the effect is already confirmed, avoid repeating it; record separately any remaining notification, ownership or case-closure failure.

7. Cross-record validation and failure matrix

Table row 1
Condition: Missing required field or unknown contract revision
Proposed response: Reject invalid submission or return unresolved determination; no favourable coercion
Evidence / accountable handoff: Validation result identifies field/profile/revision without unnecessary sensitive disclosure

Table row 2
Condition: Same source identity, different content
Proposed response: Preserve conflict; no silent overwrite or benign duplicate acknowledgement
Evidence / accountable handoff: Source steward review through authorised route; original/candidate revisions retained under policy

Table row 3
Condition: Evidence admitted, receiving use denied
Proposed response: Keep admission and denial distinct; receiving processing withheld
Evidence / accountable handoff: REC-E restrictions and REC-D deny; approved custody/retention separately assessed

Table row 4
Condition: Authority allows, data use denies/unresolved/unavailable
Proposed response: Withhold dependent operation
Evidence / accountable handoff: Both results and blocker recorded; independently authorised fallback assessed separately

Table row 5
Condition: Data use permits, authority denies/unresolved/unavailable
Proposed response: Withhold dependent action
Evidence / accountable handoff: Processing permission cannot substitute for action authority

Table row 6
Condition: Request changes after favourable determinations
Proposed response: Create revised request and re-evaluate material binding
Evidence / accountable handoff: Earlier result retained but not applied to changed target/purpose/payload

Table row 7
Condition: Delegation suspended or actor role changed while queued
Proposed response: Invalidate affected reliance and reassess before dependent execution
Evidence / accountable handoff: Current-state and pending-work links; no administrator-only reinstatement

Table row 8
Condition: Consent withdrawn during pending inference/disclosure
Proposed response: Stop dependent continuation at the approved enforcement boundary; handle retained/derived records under policy
Evidence / accountable handoff: Downstream invalidation/notification evidence; legal basis and retention conflict referred

Table row 9
Condition: Known external dispatch but unknown effect
Proposed response: Preserve indeterminate; authorised reconciliation; no blind consequential repeat
Evidence / accountable handoff: REC-X attempt, AOS-14 exchange/outcome refs and unresolved owner/deadline

Table row 10
Condition: One effect confirmed, next stage fails
Proposed response: Record confirmed effect plus open failed stage; do not replay completed stage indiscriminately
Evidence / accountable handoff: Distinct attempts and case obligations; accountable review/follow-up

Table row 11
Condition: Escalation delivered but no human ownership
Proposed response: Escalation remains open; approved cover/deadline path
Evidence / accountable handoff: AOS-13 delivery and AOS-30 ownership separately evidenced

Table row 12
Condition: Constraint explanation would expose protected material
Proposed response: Supply approved limited explanation or recorded reviewed exception
Evidence / accountable handoff: DEC-027 exception evidence; permission/prohibition unchanged

Table row 13
Condition: Recovery sees incompatible/stale records
Proposed response: Reconcile versions and block affected continuation
Evidence / accountable handoff: Compatibility decision and restored-policy evidence; neither success nor authority inferred

Delivery semantics are profile-specific. Transport retries do not guarantee business-effect idempotence. Rejection/denial explanations, acknowledgements, invalidation events and reconciliation queries are themselves governed records/actions. Their audiences, disclosure and delivery permissions must be defined; a blanket diagnostic route is not created here.

8. Proposed obligation and source register

REC-R01-R24 are local draft obligations, not newly approved component REQ numbers. Their component allocation is identified below; retain these derivation links when final records are assigned. All have origin v0.1, 4 October, status proposed, release scope logical record-contract drafting; implementation slice unselected, and project baseline approver Mark. Operational authority/data-use/retention instruments require the relevant commissioning authority. Role appointments are open. Parent REQs are still proposed AOS-00 v0.7 wording; DEC directions have their recorded approval standing.

Each row supplies statement, category, exact parent/source locator, rationale, responsible specification, blocking profile/issue and planned verification. QS-08 metadata is shared through this paragraph rather than repeated. “Shall” below is proposed mandatory wording; no approval is inferred.

Table row 1
ID: REC-R01
Proposed obligation: Each record shall identify its exact organisation and accepted schema revision.
Level/category; source and rationale: Interface/identity; REQ-021/035 and QS-12; avoid scope/version ambiguity
Owner / blockers: 02/03/05; P01/P02
Planned case: REC-V01

Table row 2
ID: REC-R02
Proposed obligation: An admitted evidence revision shall retain its source-revision provenance reference.
Level/category; source and rationale: Interface/evidence; REQ-012/036, QS-13/19; reconstruct origin
Owner / blockers: 02; P02/P08
Planned case: REC-V02

Table row 3
ID: REC-R03
Proposed obligation: A receiving component shall distinguish admitted source evidence from validated truth and inference.
Level/category; source and rationale: Component/evidence; AOS-SC §4.1, FP6/QS-18; prevent false certainty

Owner / blockers: 02/domain consumer; P02/P11
Planned case: REC-V02

Table row 4
ID: REC-R04
Proposed obligation: An evidence correction shall identify the earlier revision and its correction basis.
Level/category; source and rationale: Interface/correction; QS-13 and AOS-00 §5.2 lifecycle; preserve history
Owner / blockers: 02; P02/P08
Planned case: REC-V03

Table row 5
ID: REC-R05
Proposed obligation: A materially conflicting replay under the same source-event identity shall not overwrite the original as a duplicate.
Level/category; source and rationale: Interface/integrity; QS-12 engineering derivation; prevent concealed contradiction
Owner / blockers: 02/05; P02
Planned case: REC-V03

Table row 6
ID: REC-R06
Proposed obligation: An authority result shall bind to the exact action revision and material context it evaluates.
Level/category; source and rationale: Interface/authority; REQ-006, SC-R04; prohibit action substitution
Owner / blockers: 01; P03/P07
Planned case: REC-V04

Table row 7
ID: REC-R07
Proposed obligation: An executor shall withhold dependent action on denied, unresolved or unavailable authority.
Level/category; source and rationale: Component/authority; DEC-003/REQ-007, SC-R05; no implied grant
Owner / blockers: 04/05; P03/P09
Planned case: REC-V04

Table row 8
ID: REC-R08
Proposed obligation: A pending action affected by invalidated authority shall require a valid determination before continuation.
Level/category; source and rationale: Component/revocation; REQ-006/040, SC-R06; avoid stale permission
Owner / blockers: 01/04/05; P03/Q01
Planned case: REC-V05

Table row 9
ID: REC-R09
Proposed obligation: A human decision reference used for execution shall identify the exact attributed record, decision-maker powers and sufficient validity/evidence under the applicable organisation policy; authentication and minutes approval shall remain separate from the decision and current execution permission, without a universal subsequent approval gate (DEC-103).
Level/category; source and rationale: Interface/governance; DEC-008/087/REQ-024; no Chair draft or unrelated approval
Owner / blockers: 01/30; P07
Planned case: REC-V06

Table row 10
ID: REC-R10
Proposed obligation: A required constraint explanation shall include meaning, authority basis and referral route unless a recorded reviewed exception applies.
Level/category; source and rationale: Interface/explanation; DEC-027/FAR-R-002, SC-R19; legible control
Owner / blockers: 01/03/04/05; P10
Planned case: REC-V07

Table row 11
ID: REC-R11
Proposed obligation: A data-use result shall identify the exact data, operation and purpose it permits or refuses.

Level/category; source and rationale: Interface/privacy; REQ-004, RP domain 9 purpose principle, SC-R03; bounded use
Owner / blockers: 03; P04/P05
Planned case: REC-V08

Table row 12
ID: REC-R12
Proposed obligation: A receiving component shall withhold an inference outside its current permitted scope.
Level/category; source and rationale: Component/privacy; RP domain 9 sensing-purpose principle; avoid new inference by availability
Owner / blockers: 03/domain consumer; P05
Planned case: REC-V08

Table row 13
ID: REC-R13
Proposed obligation: A derived record shall retain the lineage of applicable source-purpose and use restrictions.
Level/category; source and rationale: Interface/privacy; REQ-004/QS-13 engineering derivation; prevent laundering through transformation
Owner / blockers: 02/03; P02/P05/P08
Planned case: REC-V09

Table row 14
ID: REC-R14
Proposed obligation: Consent-dependent pending processing shall cease reliance on consent after its applicable invalidation boundary.
Level/category; source and rationale: Component/privacy; Map §3 AOS-03 consent withdrawal and QS-13; no continued invalid basis
Owner / blockers: 03/04/05; P03/P05
Planned case: REC-V09

Table row 15
ID: REC-R15
Proposed obligation: An executor shall require both favourable current authority and all applicable data-use determinations before dependent effect.
Level/category; source and rationale: Component/enforcement; DEC-005/REQ-040; independent checks compose
Owner / blockers: 01/03/04/05; P03/P07
Planned case: REC-V10

Table row 16
ID: REC-R16
Proposed obligation: A consequential executor shall record the intended action and control-checkpoint evidence before the defined effect boundary.
Level/category; source and rationale: Component/evidence; REQ-012, RP domain 7 audit principle, QS-19 engineering derivation; no unrecorded consequence
Owner / blockers: 04/05/02; P03/P09/Q01
Planned case: REC-V11

Table row 17
ID: REC-R17
Proposed obligation: An execution record shall distinguish attempted dispatch from evidence of actual effect.
Level/category; source and rationale: Interface/outcome; REQ-012/QS-14/19, SC-R17; no false success
Owner / blockers: 04/14/02; P02/P09
Planned case: REC-V12

Table row 18
ID: REC-R18
Proposed obligation: An execution record shall represent an unknown effect as indeterminate.
Level/category; source and rationale: Interface/uncertainty; FP6 and AOS-14 ISS-005/SC-R17; no fabricated success/failure
Owner / blockers: 04/14/02; P02/P09
Planned case: REC-V12

Table row 19

ID: REC-R19
Proposed obligation: A consequential repeat shall require prior possible effect to be reconciled under an approved action profile.
Level/category; source and rationale: Component/recovery; AOS-00 §8, SC-R18; avoid duplicate consequence
Owner / blockers: 04/05/13/14; P09/Q03
Planned case: REC-V13

Table row 20
ID: REC-R20
Proposed obligation: Restart shall not reinstate authority suspended under the operational schedule.
Level/category; source and rationale: Component/authority; DEC-025/REQ-048, SC-R15; no stale restoration
Owner / blockers: 01/04/05; P03/P07
Planned case: REC-V05

Table row 21
ID: REC-R21
Proposed obligation: Technical-effect confirmation shall not close a case whose required human ownership or follow-up remains unevidenced.
Level/category; source and rationale: Component/accountability; REQ-010, RP domain 1 feedback, SC-R07/08; complete accountability
Owner / blockers: 13/30; P06
Planned case: REC-V14

Table row 22
ID: REC-R22
Proposed obligation: The overdue-repair comparison shall use the resident-communicated completion promise, rather than an internal target.
Level/category; source and rationale: Component/domain; DEC-022/REQ-042; preserve the chosen trigger
Owner / blockers: 02/10/13; P02/P06
Planned case: REC-V14

Table row 23
ID: REC-R23
Proposed obligation: The overdue-repair workflow shall retain evidence of contact provision for both named owner and accountable team.
Level/category; source and rationale: Component/domain; DEC-023/026, REQ-044; usable resident route
Owner / blockers: 11/13/30; P05/P06
Planned case: REC-V14

Table row 24
ID: REC-R24
Proposed obligation: A protected authority amendment shall not activate through an execution record alone.
Level/category; source and rationale: Component/constitutional control; DEC-024/025, REQ-045/046; records cannot manufacture approval
Owner / blockers: 01/04/05/30; P03/P07
Planned case: REC-V06

Source applicability and limits

FP1-4/6/8 inform purpose, human authority, structural constraints, legibility and uncertainty; FP5/10 inform interruption, correction and interactions; FP7 informs the resident contact/contestability path. FP9 informs purpose-first design, not a compliance certificate. RP domains 1/2/3/4/5/6/7/8/9 apply through closure, permanent human judgement, correct allocation, decision evidence, blind spots, purpose, audit, explicit delegation and sensing limits. This annex does not complete individual RP allocation or resolve broader ethical/governance mechanisms.

GT M1.2/7/8/10/11/13 and M2.3/4/8/9/12/13/15 remain relevant assessment references. Planned technical cases do not establish human judgement quality, ethical effectiveness, no-exit legitimacy or full GT conformance. The full source-traceability

matrix must be updated against approved component requirements later; no row is promoted to confirmed by this draft.

9. Planned verification catalogue

REC-V01-V14 are planned and unexecuted. The relevant AOS-40 technical/governance assessor reviews results; role/qualification appointments are unresolved. Fixtures use synthetic identities and repair records, approved test profiles and declared record/contract/instrument versions. No live resident/employee information or permissions are assumed.

Evidence common to all executions: case ID, fixture/profile/version manifest, inputs, procedure, expected and observed outputs, control/record references, time/sequence limitations, assessor/date and failures. Numerical parameters below refer to approved fixture profiles; this draft supplies none. Human judgement assessment is separately retained.

Table row 1
Case / linked obligations: REC-V01 / R01
Method; precondition and procedure: Test/inspection; supply matching, unsupported and cross-instance record revisions
Expected result and evidence: Only approved compatible scope accepted; invalid scope/revision explicitly rejected/unresolved; no silent field conversion. Retain input/validator/compatibility records.

Table row 2
Case / linked obligations: REC-V02 / R02/03
Method; precondition and procedure: Test/inspection; source observation, unverified source statement and model-derived inference share a subject
Expected result and evidence: Distinct kind/authority/quality and exact provenance remain reconstructable; admission cannot mark all as truth. Retain lineage and consumer display/use records.

Table row 3
Case / linked obligations: REC-V03 / R04/05
Method; precondition and procedure: Test; correction, reversed arrival, exact duplicate and same-ID different-content replay
Expected result and evidence: Earlier evidence preserved according to retention policy; correction/conflict identified; no silent overwrite. Retain source identities, impact-review links and validation results.

Table row 4
Case / linked obligations: REC-V04 / R06/07
Method; precondition and procedure: Test; valid exact request, changed target/purpose/payload, deny/unresolved/unavailable control
Expected result and evidence: Only current exact allow can proceed; other actions withheld; separate escalation evaluated on its own permission. Retain request bindings, control results and observed-effect record.

Table row 5
Case / linked obligations: REC-V05 / R08/20
Method; precondition and procedure: Test and race analysis; queue permitted request, suspend delegation, delay propagation, interrupt/restart and attempt stale rollback
Expected result and evidence: At approved P03 checkpoint, affected pending work cannot execute/reinstate stale permission. Boundary/order limitations are visible. Retain current-state, checkpoint and recovery evidence; case blocked until P03 fixed.

Table row 6
Case / linked obligations: REC-V06 / R09/24
Method; precondition and procedure: Test/inspection; valid decision with pending minutes and sufficient attributed evidence; wrong role/revision, unsupported or contradicted authentication, board-only telos change and incomplete schedule change
Expected result and evidence: Check actual powers/process/evidence and effectiveness independently of minutes approval; no universal record-approval gate, conclusive signature or executor-created authority. Preserve protected amendment process, current controls, exact records/assessments and actual history. Planned, not executed.

Table row 7
Case / linked obligations: REC-V07 / R10
Method; precondition and procedure: Inspection/test; ordinary denial, sensitive security explanation, missing exception review
Expected result and evidence: Default explanation present; valid exception limits disclosure without changing prohibition; unreviewed

exception cannot satisfy explanation obligation. Retain explanation/exception/authority records.

Table row 8
Case / linked obligations: REC-V08 / R11/12
Method; precondition and procedure: Test; repair-support use then occupancy inference, employee performance use, wider disclosure
Expected result and evidence: Each requested data/operation/purpose evaluated; out-of-scope inference/disclosure withheld, including downstream join. Retain request/basis/restriction/result evidence.

Table row 9
Case / linked obligations: REC-V09 / R13/14
Method; precondition and procedure: Test/inspection; derive summary, change purpose and invalidate consent while pending
Expected result and evidence: Restriction lineage persists; affected continuation stops at approved boundary; retained evidence/deletion handled under distinct basis, never blanket deletion or continued use. Retain downstream invalidation and lifecycle records.

Table row 10
Case / linked obligations: REC-V10 / R15
Method; precondition and procedure: Test; authority allow/data-use deny, opposite combination, both favourable with missing condition, both favourable and all conditions evidenced
Expected result and evidence: Neither favourable result substitutes for the other; only exact request satisfying both current sets passes effect boundary. Retain evaluations and checkpoint result.

Table row 11
Case / linked obligations: REC-V11 / R16
Method; precondition and procedure: Test/analysis; consequential action with functioning record boundary, record-store outage and approved alternative fallback
Expected result and evidence: Intended action/checkpoint recorded before effect; unavailable required recording withholds dependent automation; authorised fallback has its own evidence. Retain boundary timing and failure traces.

Table row 12
Case / linked obligations: REC-V12 / R17/18
Method; precondition and procedure: Test; accepted API dispatch but no external effect evidence, known rejection and partial completion
Expected result and evidence: Dispatch/full/partial/indeterminate states distinguishable; unknown not called successful or failed; defined effect evidence determines classification. Retain receipts/source queries and limitations.

Table row 13
Case / linked obligations: REC-V13 / R19
Method; precondition and procedure: Test/analysis; unknown prior effect, authorised reconciliation, confirmed duplicate, partial effect and proposed repeat
Expected result and evidence: No blind consequential repeat; authorised query/next action separate; continuation matches approved profile/human authority. Retain attempt correlation, reconciliation and fresh determinations.

Table row 14
Case / linked obligations: REC-V14 / R21-23
Method; precondition and procedure: End-to-end demonstration; synthetic on-time/overdue/missing-date cases; unavailable owner, delivery without acknowledgement, then permitted team cover and resident notification
Expected result and evidence: Overdue uses communicated promise; missing/contradictory date does not invent trigger; human ownership and both contact routes evidenced; no closure from transport success alone. Retain evidence, determination, execution, escalation, delivery and disposition chain.

10. Overdue-repair example - connected records

This is a symbolic walkthrough, not an execution record. Dates, channels, role assignments and response windows come from an approved synthetic fixture profile.

Table row 1

Step: 1. Receive promise/completion evidence
Records and checks: REC-E-PROMISE-1 and REC-E-COMPLETION-1 reference source revisions, communicated date, completion state and restrictions
What remains observable: An internal target is a different fact; source verification and completeness visible

Table row 2
Step: 2. Assess overdue condition
Records and checks: AOS-13 uses approved date precision/comparison and source-authority profile; changed/missing/conflicting promise triggers defined exception
What remains observable: Detection is a derived finding, not authority to amend the promise

Table row 3
Step: 3. Request internal escalation
Records and checks: ACTION-ESCALATE-1; REC-A-ESCALATE-1; REC-D-ESCALATE-1 where restricted data is used
What remains observable: Named route/recipient, permitted minimum disclosure and current delegation independently checked

Table row 4
Step: 4. Execute routing
Records and checks: REC-X-ESCALATE-1 plus AOS-13-IF-001 lifecycle records
What remains observable: Dispatch, delivery, human acknowledgement and owner are separate; no acknowledgement leaves a tracked exception

Table row 5
Step: 5. Provide resident contacts
Records and checks: Separate ACTION-CONTACT-1, applicable REC-A/D and REC-X records; AOS-11/14 roles depend on approved boundary/channel profile
What remains observable: Named case-owner and accountable-team details, actual contact delivery and unusable-contact limitation retained

Table row 6
Step: 6. Human disposition and repair outcome
Records and checks: AOS-30 approved decision/disposition; linked actual repair completion evidence; separately permitted follow-up
What remains observable: No machine resolution of reserved value conflict; completed repair, informed resident and case closure remain distinct

Table row 7
Step: 7. Closure/review
Records and checks: AOS-13 applies approved closure conditions; AOS-25 can review recurring failure/unknown effects under permitted purpose
What remains observable: Failed stages and unresolved outcomes remain visible; workflow performance does not prove good governance

If escalation succeeds but resident notification fails, retain the successful routing and open contact failure. If contact dispatch might have occurred before a crash, reconcile its effect before a duplicate consequential send. If a promised date is corrected after escalation, preserve the earlier finding and assess affected pending actions under the adopted correction policy; do not erase the history or silently extend the promise.

11. Decision pack and remaining profiles

Mark approved all three recommended directions on 4 October 2026 (“All three agreed”), including the qualifications below, recorded as AOS-00-DEC-028-030 in architecture v0.8 and Map v0.5. These are architectural direction approvals. Exact technical mechanisms, schemas, requirement wording, time limits and role permissions still need specification and approval; no verification case or readiness gate is promoted.

Table row 1

Decision: Q01 - Final authority/data-use check
Approved direction: Require current authority/data-use validation at the last enforceable point before the consequential effect; earlier checks support planning but cannot be the sole basis after material change. Define how changes during an irreversible action are recorded/handled.
Alternative considered / not adopted: Permit reliance on a cached determination within an approved validity window. This reduces control calls but requires explicit bounds, invalidation and residual race-risk acceptance; neither option proves instantaneous revocation.
Affected records and obligations: REC-A/D/X; R08/15/16/20; P03/P09

Table row 2
Decision: Q02 - Evidence correction impact
Approved direction: Corrections/conflicts that affect material action inputs place affected pending work into reassessment before continuation; completed effects retain history and significant consequences get an accountable impact review. Unrelated work continues.
Alternative considered / not adopted: Merely flag the correction while pending work proceeds. This avoids pauses but risks acting on evidence already known to be disputed; materiality classification/authority must be specified.
Affected records and obligations: REC-E/A/D/X; R04/06/08; P02/P03

Table row 3
Decision: Q03 - Unknown/partial consequential effect
Approved direction: Block automatic consequential repetition until an approved reconciliation/continuation profile establishes permitted continuation without duplication or compounding, or an authorised human determines the permitted next action. Record an unresolved outcome explicitly if certainty cannot be recovered.
Alternative considered / not adopted: Automatically repeat after timeout or declare failed. This improves apparent completion speed but can duplicate commitments, disclosures or notifications; timeout alone is not evidence that the first effect did not occur.
Affected records and obligations: REC-X and AOS-13/14; R17-19; P09

“Last enforceable point” in approved Q01 identifies the required control boundary, not an approved numerical latency or instantaneous revocation guarantee. The enforceable checkpoint, freshness and race limits must be fixed under P03. Q02 needs a material-input dependency map; Q03 needs action-specific reconciliation and retry profiles, separately authorised status queries, and a human handoff owner, deadline and cover. None permits an unapproved human or technical administrator to enlarge delegation.

Configuration and specification gaps - all unresolved

Table row 1
Gap: Contract role appointment/change procedure
Required content and owner: P01; AOS-02 and semantic owners; named human roles, cross-component impact/approval and version compatibility
Effect: Blocks contract baseline/build where accountability absent; ownership direction itself settled

Table row 2
Gap: Fact/source/time profile
Required content and owner: P02; AOS-02 with Asset/Process: record keys/types/units, authoritative promise/completion source, date comparison/change rules, conflict/duplicate ordering
Effect: Blocks overdue predicate and interoperable record build

Table row 3
Gap: Enforcement/race profile
Required content and owner: P03/P12; AOS-01/03/04/05: context binding, current-state checks, invalidation, checkpoints, propagation and independent bypass threat model
Effect: Blocks consequential execution and revocation assurance

Table row 4
Gap: Identity and external trust profile
Required content and owner: P04; AOS-03/14: principal/delegation evidence, authenticity, acceptable currency and claim semantics proportionate to exchange

Effect: Blocks dependent trusted exchange; federation remains deferred

Table row 5
Gap: Data-use profile
Required content and owner: P05/P08; AOS-03 with resident/workforce/professional/governance participants: purposes, consent/basis, inference/disclosure, retention/deletion, derived-data and location rules
Effect: Blocks dependent processing; no legal basis or welfare priority invented

Table row 6
Gap: Action/schedule profile
Required content and owner: P07; AOS-01/20/30 and commissioning authority: consequential classification, permissions/prohibitions, reserved human approval and suspension/reinstatement
Effect: Blocks action capability and protected activation

Table row 7
Gap: Handoff/contact/closure profile
Required content and owner: P06; AOS-13/30/11: accountable receipt, deadline/cover, resident channel/contact validity, permitted unresolved closure
Effect: Blocks end-to-end escalation/notification completion claims

Table row 8
Gap: Recovery and evidence profile
Required content and owner: P09; AOS-04/05/13/14: record boundary, availability, reconciliation, retry/fallback/rollback permissions and limits
Effect: Blocks outcome/recovery conformance; no default retry count or timeout

Table row 9
Gap: Explanation profile
Required content and owner: P10; AOS-01/03/04/05: permitted default disclosure, exception reason/reviewer/authority and evidence
Effect: Blocks explanation interface approval; exceptions never waive controls

Table row 10
Gap: Analytical/review profile
Required content and owner: P11; AOS-20-25/30: uncertainty rubric, canonical state and human review/decision evidence
Effect: Blocks quality/governance conclusions beyond captured facts

Appointing roles, setting thresholds and resolving resident/workforce/legal matters are not all Mark-only decisions. The architecture specifies which approved organisational instruments must supply them; actual organisations approve their own valid configuration within non-waivable constraints. Synthetic proof-of-concept settings will be labelled fixtures, not sector defaults.

12. Author review, readiness and next work

Table row 1
Review area: Record scope and identity
Author assessment and limitation: Four connected families defined; existing evidence/authority IFs preserved; companion IF allocation explicit vacancy

Table row 2
Review area: Semantics and field coverage
Author assessment and limitation: Logical types, cardinality, validation, ordering, acknowledgements, correction, revocation, retries and failure developed; operational profiles still unresolved

Table row 3
Review area: Requirement/source records
Author assessment and limitation: Twenty-four draft obligations linked to exact source/parent locators, owners, blockers and fourteen

planned cases; component REQ/VER allocation unfinished

Table row 4
Review area: Human and constitutional boundaries
Author assessment and limitation: Recorded decisions preserved; underlying human powers required; no boardroom input route or self-issued grant

Table row 5
Review area: Design adequacy
Author assessment and limitation: Draft exposes circular permission bootstrap, stale authority, purpose expansion, evidence conflict and unknown-effect risks; actual enforcement/operating capacity not established

Table row 6
Review area: Source completeness
Author assessment and limitation: Selected FP/RP/GT application given; complete individual disposition and traceability matrix update remain future component work

Table row 7
Review area: Readiness and assurance
Author assessment and limitation: No executed verification or independent review; no G2/G3/G4; authorised build scope absent

This is a drafting annex rather than four full component specifications. Proposed component-template mapping: purpose/sources/responsibilities §1; semantic/state/data/authority/failure/evidence §§2-7; requirements and applicability §8; acceptance §9; workflow §10; issues/dependencies §11; review/change/handover §12. Formal tailoring and complete component-template adoption remain to be reviewed; the mapping does not waive omissions.

Builder stop conditions: unresolved profiles implementing approved Q01-03, or a profile that materially changes the approved dependent behaviour; missing lawful/approved processing basis; unavailable current permissions; unsupported schema/scope; ambiguous resident promise; unknown prior effect; absent approved accountable handoff; missing protected amendment evidence; no required execution record boundary; or a source conflict requiring governance resolution. Do not turn a field placeholder, model inference, profile example or generated explanation into permission.

Next starting point: action 3 logical control coordination adopted; next action 4 is protected reporting and recovery (KR-04/05), subject to instruction. Scope-specific profiles, non-kernel adoption and independent/executed evidence remain open.

Approval addendum, 4 October: original drafting baseline above remains AOS-00 v0.7 / Map v0.4; current decision disposition is AOS-00 v0.8 DEC-028-030 / Map v0.5. REC-R01-24 remain proposed and REC-V01-14 remain planned. Component drafting must complete explicit obligation and verification coverage for the approved directions, including evidence-correction dependencies.

Operational profile annex, 5 October: Operational Profiles v0.1 (aos-operational-profiles-v0-1-review-draft.md) develops approved DEC-031-035 under AOS-00 v0.9 / Map v0.6. It is the proposed profile drafting reference, complementing the existing shared/core record definitions without duplicating or approving their schemas. Earlier drafting baselines remain historical. Profile wording/values and component adoption remain open; no SC/REC obligation or case status is promoted.

Date/evidence and channel disposition, 5 October: DEC-036-041 under AOS-00 v0.10 / Map v0.7 approve the five date/evidence recommendations and require resident-agreed channel(s). Operational Profiles v0.1 supplies the current proposed detail and cases. For resident communication, the action/determination/execution chain must carry or resolve the applicable channel-agreement revision and selected channel(s); promise/contact evidence must preserve communication via those channels. Organisation permission alone is insufficient evidence of resident agreement. Exact conditional fields/validation and component adoption remain proposed; current SC/REC obligations/cases retain their status.

Initial component allocation, 5 October: AOS-01 v0.1 (aos-01-authority-constitutional-controls-and-change.md) derives proposed general authority requirements and planned cases, preserving AOS-01-IF-001/REC-A. This is initial allocation, not adoption/approval of executable schemas or complete source traceability. Shared definitions remain authoritative drafting

references; other components must adopt their respective obligations. Process-specific fixture decisions do not define general delegation policy.

AOS-02 initial component allocation, 5 October: AOS-02 v0.1 (aos-02-unified-data-layer-and-shared-records.md) now allocates common-definition/semantic-owner, evidence/source/identity/time/lineage/correction/access/outcome and compatibility obligations, preserving AOS-02-IF-001/REC-E. Existing common family schemas remain the single proposed detailed definitions; component baseline and producer/consumer adoption remain open. HACT is a referenced sector alignment candidate; exact field mappings/version and conformance are not inferred. No SC/REC status is promoted.

AOS-03 initial component allocation, 5 October: AOS-03 v0.1 (aos-03-identity-access-consent-and-data-use.md) now allocates proposed identity/capacity, exact purpose/basis/use, consent/change, inference/barrier, disclosure/projection and lifecycle/location obligations around the existing REC-D definition. No competing schema or approved IF number is introduced. Five design questions Q01-Q05 await Mark. Common schemas remain the single proposed detailed definitions; exact reciprocal adoption and commissioning are open. No SC/REC requirement status or readiness promotion. Next: resolve the five AOS-03 choices and develop shared-schema/consumer coverage.

AOS-03 approved direction disposition, 5 October: Mark agreed Q01-Q05, recorded as DEC-049-053 in AOS-00 v0.13. AOS-03 v0.2 incorporates all five; earlier pending-choice notes are historical. Exact shared schemas/consumer adoption and commissioning remain open. Next AOS-04; no SC/REC requirement status or readiness promotion.

6 October current disposition: DEC-062-066 approved; this v0.2 and Kernel Exchange Register v0.1 (aos-kernel-exchange-register-v0-1.md) are adopted as proposed logical definitions by AOS-01-05 v0.4. Existing REC-R01-24 and REC-V01-14 retain proposed/planned status; new KXR/KXV links carry action-2 refinements. Earlier dated next-step/component versions are historical. No executable schema, executed case or readiness approval.

Action-3 current supplement, 6 October 2026

Kernel Control Coordination v0.1 (aos-kernel-control-coordination-v0-1.md) and Kernel Exchange Register v0.2 define approved DEC-067-072 at logical record/protocol level. AOS-01-05 v0.5 adopt this v0.3 against AOS-00/Map v0.17. Earlier versions and pending-profile notes remain drafting history; current logical protocols are supplemented as follows.

Table row 1
Existing family/view: REC-A / authority / KX-02
Current common fields/protocol and boundary: Exact current-source/restriction evidence and context refs; CHECK consumes original result with current authority state, not a rewrite of original evaluation.

Table row 2
Existing family/view: REC-D / use / KX-03
Current common fields/protocol and boundary: Exact identity/basis/consent/current restriction sources, independently evaluated original decision; CHECK verifies current receiving use and permissible notification scope.

Table row 3
Existing family/view: REC-X / execution / KX-04
Current common fields/protocol and boundary: final_control_check references CHECK; actual request/attempt/arguments/current version vector/pre-effect evidence plus ACC/RSV where bounded; withheld reason links WHD, unknown effect retains reservation, later evidence remains distinct.

Table row 4
Existing family/view: Policy activation / KX-05
Current common fields/protocol and boundary: ACT required-member compatible applied vector and restriction-priority fence; approval alone cannot prove activation.

Table row 5
Existing family/view: Evidence/assurance correction / KX-13
Current common fields/protocol and boundary: CHG dependent target/application/no-material-dependency/owned unresolved records;

history/assurance retained under permitted lifecycle.

Table row 6
Existing family/view: Task/lifecycle / KX-16
Current common fields/protocol and boundary: Linked effect/group/profile and BRK resumption/reconciliation; no auto-replay or cancellation-based capacity release.

Table row 7
Existing family/view: Escalation / KX-07, acknowledgement / KX-21
Current common fields/protocol and boundary: WHD operational owner, minimal permitted notification, deadline/cover, actual responsibility acceptance, failed-delivery exception, traceable coalescing and appropriate resident-agreed-channel update through responsible workflow.

Annex §§3-9 are the single logical field/transition/acceptance definitions; each required compound value is typed under its common header/schema. Changed KX families name revision 0.2, ACC/RSV/WHD KX-24/25/26 revision 0.1. All original SC/REC obligation/case statuses stay proposed/planned; KCR/KCV provide new action-3 source and case links. Role appointments, effect estimation/group/period/numerical settings, actual concurrent accounting/fencing, wire schemas, independently usable reporting route/human capacity, recovered authoritative-state proof and executed conformance remain open. Recovery/protected reporting are action 4.

Action-4 current supplement, 6 October 2026

Baseline at this dated adoption step: AOS-00/Map v0.18; AOS-01-05 v0.6; Core/Shared v0.4; Exchange Register v0.3; Control Coordination v0.2. Protected Reporting and Recovery v0.1 (aos-kernel-protected-reporting-and-recovery-v0-1.md) §§2-8 supplies the single reporting/recovery dictionary and protocols under approved DEC-073-078. REC-E/A/D/X/Q retain original evidence/evaluation meaning; reports bind advance authority/use and recipient verification, while recovery binds complete current authoritative sources, applied lifecycle dispositions, isolated validated configuration, effect/reservation reconciliation and scoped acceptance. Protected-copy integrity alone cannot establish currentness or completeness.

KX-19 protected_finding v0.2, KX-20 recovery v0.2 and KX-26 WHD v0.2 add exactly the annex §5 fields. All original IF/CON IDs remain; relevant producer/consumer views and role ownership are §§2/5. Receipt/validation, human responsibility acceptance, actual release/application and service completion are separate statuses. No future full-schema conformity is inferred from adopting this logical supplement. Annex §6 cases and component additions trace every direction; §7 references primary standards with derivation/AOS-choice distinctions and ISO clause verification limits. Historical action-3 versions and former open action-4 notes remain dated history; this supplement is current.

Common research adoption - 6 October 2026

Baseline at this dated adoption step: AOS-00/Map v0.22, DEC-001-086; AOS-01-05 v0.7; AOS-14 v0.3; AOS-20 v0.2; Shared v0.6/Core v0.5/Register v0.5; source matrix v0.7; template v0.4. AOS-02 v0.7 §6.6 is the single proposed profile/run/finding/disposition logical definition; AOS-04 v0.7 CON-009 owns behaviour/profile meaning. Exchange Register v0.5 §13 (aos-kernel-exchange-register-v0-1.md) declares RSVIEW-0.1, exact component adoption, common owner/producer/consumer links and gated wire/profile work. It supersedes earlier candidate-definition/adoption-pending statements at the documentary logical level. No new approved IF/REC family or alternative field dictionary is introduced.

Research evidence/assurance links use REC-E/Q; authority/use/task/effect links use REC-A/D/X. Finding assessment, canonical GI analysis, agent recommendation, empowered human disposition and separate amendment/activation records retain different meanings. AOS-20 v0.2 §6.2 supplies GI-specific assessment qualifiers; the Boundary charter maps its recommendation vocabulary into finding content rather than human decision status. Current checks, staged acknowledgement, deduplication/material correction, licensing/privacy/lifecycle and controlled recovery remain inherited. Missing required fields/permissions/versions produce invalid/unresolved reliance, never favourable coercion or guessed defaults.

Component-level REQ/VER coverage and source traceability are Register §13 and source matrix v0.7 §11. Detailed non-kernel drafting/consumer adoption, exact executable types/cardinalities/units/version compatibility, approved profile values/roles/quality criteria and executed assurance remain owned prerequisites. No source finding, charter change, live agent activation or readiness is approved by these references.

AOS-30 functional alignment - 7 October 2026

Under DEC-103 and current AOS-30 §§5/6.2/10.3, decision validity/effective time, record authentication/evidence, minutes approval and permission to execute are distinct. Reliance uses sufficient attributable evidence assessed under the actual organisation’s legal form, instruments and approved evidence policy; a valid decision may precede minutes approval. A Chair-authenticated record or extract may be evidence through an authorised route, but no signature, draft or extract alone creates decision authority or resolves conflicting evidence. No universal second approval of exact decision wording is imposed where applicable arrangements do not require it. Minute-taker drafting and Company Secretary stewardship remain distinct; non-board decisions use their applicable empowered route. Current authority/data-use/conditions and observed effects remain separate. Missing or disputed sufficient evidence blocks affected automated reliance for accountable resolution, not a declaration of legal invalidity.

Existing KX-06 logical v0.2 participation is aligned in AOS-01-05 v0.8/AOS-20 v0.3/AOS-30 v0.3 and Register v0.8 §15. AOS-30 conditionally receives KX-13/AOS-02 corrections affecting preparation/account/outcome review; GI updates canonical analysis and AOS-30 obtains human review without silent approved-record rewrite or effect reversal. Functional CR30-01-03 findings closed; executable schema compatibility is later implementation work. Earlier dated AOS-30 adoption-pending/next-drafting statements are superseded for existing functional drafts. Existing obligation/case identifiers and statuses remain.

Historical opening status notices - retained provenance

These are dated drafting snapshots, including their then-current versions, totals, completion statements and next tasks. They do not define today's baseline or work queue. The present document retains its proposed/planned status; approved directions retain their recorded scope. Use the current inventory, adopted README and live to-do list for orientation; authoritative requirement and decision text remains in its named sections.

Historical status notice - AOS-30 alignment - 7 October 2026: functional drafting and consistency alignment complete under Mark’s instruction. AOS-00/Map v0.25, DEC-001-089; AOS-01-05 v0.8, AOS-14 v0.4, AOS-20 v0.3 and AOS-30 v0.3; Shared v0.9/Core v0.6/Exchange Register v0.8; source matrix v0.9 and template v0.4 unchanged; Control Coordination v0.2/Protected Reporting and Recovery v0.1 unchanged. Earlier dated baseline/adoption/next-step entries are history. CR30-01-03 are closed at the functional-document level; implementation/commissioning evidence remains separate. No new DEC/REQ/VER/IF identifier or operating power is introduced.

DEC-104 current protected-finding interpretation - 29 October 2026

Each mandatory protected-finding category shall have an approved reporting arrangement assessed against both technical failure and interference by implicated people. The profile shall identify the intended recipient, possible conflicts and an appropriately independent authorised alternative; an implicated person shall not be the sole gatekeeper deciding whether the required finding reaches its authorised audience.

Authority/use permissions, minimum report content, recipient verification, custody, route/change dependencies, tracking ownership, acceptance, cover and escalation are established in advance. An external route is included where justified and lawfully authorised; external reporting is not a universal default and a finding creates no extra disclosure power. Planned exercises address failed infrastructure, unavailable/implicated recipients, apparent alternatives controlled by the same implicated gatekeeper and attempted suppression. Missing adequate arrangements remain an explicit owned gap, prevent claims of operational protected-reporting assurance and withhold affected dependent reliance under existing gates; they do not create

false delivery, ownership transfer or blanket shutdown of separately authorised service. Original tracking duty persists until actual scoped acceptance.

Protected Reporting and Recovery v0.2 §5 defines KX-19 protected_finding v0.3: its existing class/profile and route/dependency evidence now explicitly includes technical failure, implicated recipient/release/custody control, approved conflict disposition and appropriately independent authorised alternative. The original v0.2 adoption records above are historical for this view; recovery v0.2, KX-26 v0.2 and other distinct subviews retain their separate revisions. Profiles/wire mappings, accepted exact old/new semantic compatibility and actual endpoint/control evidence must be approved before affected reliance; old consumers are not silently upgraded.