AOS-03 - Identity, access, consent and data use

Document: aos-03-identity-access-consent-and-data-use · Source revision or record: v0.12

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-104 adopted - 29 October 2026: Current revision 0.12. 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 0.11. 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 DEC-087 is partly superseded; decision/amendment and legal-source record (../Supporting-Specifications/aos-dec-103-decision-validity-evidence-and-minutes-2026-10-29.md).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 0.10; 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 0.9; 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: Version / date

Value: 0.12 / 29 October 2026

Table row 2
Document control: Status
Value: Review draft; proposed component obligations; five general design directions approved

Table row 3
Document control: Architecture baseline
Value: AOS-00/Map v0.25, DEC-001-089; AOS-30 functional alignment 7 October 2026

Table row 4
Document control: Source baseline
Value: Foundational Principles v4; AOS Reasoning Principles v6; Governance Intelligence Tests, controlled supplied set

Table row 5
Document control: Accountable owner / custodian
Value: Identity and information-governance stewardship required; organisational appointments open

Table row 6
Document control: Project baseline approver
Value: Mark Sweeny

Table row 7
Document control: Organisation approvers
Value: Empowered governance, privacy, security, resident and workforce authorities under approved instruments; exact powers/appointments open

Table row 8
Document control: Author
Value: Codex, at Mark’s request

Table row 9
Document control: Reviewer
Value: Independent project reviewer unassigned; review deferred

Table row 10
Document control: Quality / template
Value: AOS-QS v0.1; component template v0.4

Table row 11
Document control: Release scope
Value: General logical component specification; no implementation slice authorised

Table row 12
Document control: Gate / approval evidence
Value: Author-reviewed draft; no G2/G3/G4, build, activation or legal-conformance claim

Table row 13
Document control: Dependencies
Value: 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; Control Coordination v0.2/protected reporting-recovery v0.1 unchanged; non-kernel and wire/commissioning adoption open

Table row 14
Document control: Change history
Value: 0.1 initial draft. 0.2 incorporates Mark’s approval of Q01-Q05 on 5 October as DEC-049-053; exact component wording and readiness remain subject to review. 0.3 - 6 October: common decision-baseline/status/interface reconciliation (KR-09 label portion),

preserves historical approvals and proposed/planned records; register formatting repaired where applicable (KR-10); see §19.1. 0.4 - DEC-062-066 common exchange adoption; five new proposed adoption REQs/six planned cases; AOS-03 REQ-040 sequencing clarified where applicable. 0.5 - DEC-067-072 control coordination/withholding notification; eight proposed REQs/eight planned cases and reciprocal source/field adoption; original records preserved. 0.6 - DEC-073-078 protected reporting/recovery and standards provenance; six proposed REQs/six planned VERs; prior records preserved. Current revision incorporates DEC-086 common research inheritance and reciprocal logical adoption, 6 October 2026; prior decision/record statuses retained. 7 October - authorised AOS-30 functional adoption, Chair/board approval propagation and material-correction alignment; no new identifiers or operating power.

Current catalogue inventory - editorial reconciliation, 29 October 2026

The normative tables contain 69 retained numbered requirement records and 52 planned verification case identities. These are catalogue counts, not independent obligations, active-scope coverage, executed tests or accepted results. Earlier totals in dated adoption supplements describe those steps only. The current document inventory (../Supporting-Specifications/aos-current-document-inventory-2026-10-29.md) records the suite baseline and count method.

1. Purpose and scope

1.1 Purpose

AOS-03 makes the use of information answerable to people, purpose and permission. It establishes who is acting, in what capacity, which information and operation they may use, for which purpose, under which basis and conditions, and what happens when those conditions change.

1.2 Architectural problem

Authentication can prove access to a credential without proving a legitimate purpose. A system can be authorised to perform a repair task without being authorised to infer a resident’s routines. A summary, embedding or joined dataset can expose information that no source was permitted to disclose. Consent can become a blanket label, especially where a resident cannot change landlord or an employee fears consequences for refusing.

Without AOS-03, integration increases technical access faster than accountable permission. Organisational authority and privacy constraints become conflated, and an apparently helpful assistant can become an unapproved observation mechanism.

1.3 Intended outcome

Every controlled processing boundary can establish an exact, current permitted-use result for the proposed actor, data, operation, purpose and recipient. Affected people can understand and challenge material uses through accessible human routes. Restrictions survive transformation and transfer. Missing evidence, unresolved conflict or unavailable controls cannot produce permission by implication.

1.4 Scope

Human, service and agent identity assurance; acting roles and representation; purpose/basis registration; access and inference decisions; consent records and lifecycle; information barriers; disclosure projections; governed retention/deletion and rights handling; location/access assessment; currentness/invalidation; constraint explanations and accountable review.

The reusable specification is derived from principles. Contrasting scenarios test its adequacy; one repair process does not define the general policy. England anchors the initial jurisdiction-specific mapping, separately from the reusable core.

1.5 Exclusions

AOS-01 owns organisational authority, delegation and constitutional policy change. AOS-02 owns common structures, entity/source mappings and records. AOS-04 owns bounded agent behaviour; AOS-05 enforceable runtime separation. Domain components define their legitimate sensing/service needs; AOS-13/30 route and record human responsibility. AOS-14 governs external exchange; GI interprets and prepares rather than granting itself access. AOS-40 assesses assurance.

This specification neither chooses an identity vendor nor creates a federated identity system. It does not decide legal bases for every housing process, prescribe universal consent, allocate a default retention period, or authorise emergency exceptions. It specifies the evidence and control needed for those decisions.

2. Authority and sources

2.1 Source hierarchy and exact derivation locators

FP v4 and RP v6 govern; architecture DEC directions have their recorded approval standing. Parent requirement wording, shared schemas and all component REQs below remain proposed. GT supplies governance assessment criteria. External guidance informs jurisdictional assessment and cannot waive an AOS constraint. Books are explanatory; research and working notes are proposals.

The following source keys are local traceability references, not invented controlled-source requirement IDs. Parent IDs use prefix AOS-00.

Table row 1
Key: S01
Version / exact locator: FP v4 principles 1-4, 7-8; RP v6 domain 2 “Mode 2 is permanently human” and “The boardroom is a Mode 2 deliberative space”
Application: Purpose, human judgement, deliberative privacy and no-exit obligation

Table row 2
Key: S02
Version / exact locator: RP v6 domain 9 “Sensing must not exceed its declared purpose”
Application: Declared purpose and structural inference limits

Table row 3
Key: S03
Version / exact locator: RP v6 domain 9 “The boundary between observing an asset and monitoring a behaviour”
Application: Asset/behaviour separation at design, processing, storage and action

Table row 4
Key: S04
Version / exact locator: RP v6 domain 9 “Where behavioural inference from sensing data is genuinely necessary”
Application: Demonstrated necessity, explicit consent, separate governance and regular review

Table row 5
Key: S05
Version / exact locator: RP v6 domain 9 “The purpose limitation principle applies across all intelligence layers”
Application: Workforce/process/boundary and cross-layer expansion limits

Table row 6
Key: S06
Version / exact locator: RP v6 domain 6 “Where the organisation’s welfare obligation to residents and its consent architecture pull in opposing directions”
Application: Deliberate board determination of welfare/consent hierarchy; no default override

Table row 7
Key: S07
Version / exact locator: RP v6 domain 7 three principles beginning “If you cannot audit it”, “The architecture must be more transparent” and “Transparency obligations extend”
Application: Reconstruction, affected-person transparency and visible uncertainty

Table row 8
Key: S08
Version / exact locator: RP v6 domain 8 explicit/contextual delegation, external commitments/contact/sensitive-data principle, internal escalation distinction and protected audience principle
Application: Independent controls, bounded handoff and no quiet suppression

Table row 9
Key: S09
Version / exact locator: AOS-00 v0.12 DEC-002/005/008/014/016/020; REQ-004/008/021/030/031/035/037/040
Application: Owners, common definitions, organisation isolation, England mapping and location assessment

Table row 10
Key: S10
Version / exact locator: AOS-00 v0.12 DEC-027-030/033-034/041-047
Application: Explanations, current checks, selective reassessment, reconciliation, channel agreement, delegation and governed history

Table row 11
Key: S11
Version / exact locator: Shared Contracts v0.1 §§3-5, SC-R03/05/06/15; Core Records v0.1 §§2/5, REC-D and REC-R11-14/23
Application: Exact request binding, purpose inheritance, lifecycle and independent checks

Table row 12
Key: S12
Version / exact locator: AOS-01 v0.2 §§4/6/7; AOS-02 v0.2 §§3.1/4/6/9
Application: Authority/data-use separation; origin versus assurance; governed projections and lifecycle

Table row 13
Key: S13
Version / exact locator: AOS-QS v0.1 QS-04-19/21/24-28; component template v0.4 §§4/6/15/20/21
Application: Requirement quality, contract semantics, evaluation, evidence and readiness

Table row 14
Key: S14
Version / exact locator: GT supplied controlled text M1.1-14 and M2.1-15
Application: Applicability and organisational assessment in §8

Table row 15
Key: S15
Version / exact locator: AOS-00 v0.13 DEC-049-053; Mark’s approval 5 October (“Agree all 5”)
Application: Approved Q01-Q05 directions; exact commissioning and normative wording remain open

2.2 External references consulted 5 October 2026

Table row 1
Ref / primary source: EXT-P01 - ICO: How do we ensure lawfulness in AI? (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/), consent/contract/special-category sections
Finding and limit: Distinguishes purposes and processing bases; consent withdrawal needs accommodation; a basis for service delivery does not automatically cover model development

Table row 2
Ref / primary source: EXT-P02 - ICO: Special category data (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/special-category-data/), “At a glance” and inference discussion
Finding and limit: Article 6 basis and additional Article 9 condition are distinct; intentional sensitive inference can require additional protection. Scope-specific legal assessment remains required

Table row 3
Ref / primary source: EXT-P03 - ICO: How do we ensure individual rights in our AI systems? (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-individual-rights-in-our-ai-systems/), rights and meaningful human input sections
Finding and limit: Rights need operational routes; merely recording a human involvement does not establish meaningful review

Table row 4
Ref / primary source: EXT-P04 - ICO: What is the impact of Article 22 on fairness? (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-is-the-impact-of-article-22-of-the-uk-gdpr-on-fairness/), opening notice
Finding and limit: Guidance explicitly under review following Data (Use and Access) Act changes. This draft does not treat its older rule summary as a verified current legal baseline

These are limited reference checks, not a complete assessment of current legislation, commencement, safeguarding powers, equality duties or housing obligations. Organisation legal/privacy owners must verify exact applicable provisions, guidance currency, scope and approval evidence before commissioning. AOS’s permanent human Mode 2 commitment remains independent of what legislation might permit.

HACT alignment remains under AOS-02 DEC-048. A compatible sector field definition supplies shared meaning; it does not supply a processing basis, consent or disclosure permission. Exact adopted release/mappings remain open in AOS-02.

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-104 - protected reporting under failure and implicated-person interference

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.

The organisation’s profile binds each required finding class to normal/alternate authorised audiences, conflict criteria/evidence and accountable assessment, disclosure basis/minimal payload, independently verifiable recipients/permissions, credentials/custody and route/reconfiguration controls, failure/compromise assumptions, tracking/cover/escalation, human fallback, evidence and review triggers. Test both infrastructure/common-dependency independence and organisational release/recipient/custody control; neither implies the other. No administrator, executive sign-off or report-validation step may silently remove a required duty. The declared threat/governance scope and residual limitations must be visible: this is not an unlimited guarantee against every holder of legal/constitutional change powers. Inadequacy returns to an empowered accountable reviewer; the reporting agent cannot invent a recipient or grant itself onward-disclosure authority.

3. Responsibilities and boundaries

Table row 1
Responsibility: Actor assurance
AOS-03 owns: Identity, acting role, representation scope, verification evidence and currency
Shared / institutional responsibility: AOS-02 preserves entity mappings; empowered humans establish appointments/representation;

AOS-05 authenticates and isolates

Table row 2
Responsibility: Permitted-use semantics
AOS-03 owns: Actor/data/operation/purpose/basis/recipient/location decision and conditions
Shared / institutional responsibility: Governance/privacy owners approve policy and legal findings; AOS-01 approves organisational powers

Table row 3
Responsibility: Consent lifecycle
AOS-03 owns: Scope, person/representative, notice and expression evidence, change/withdrawal/expiry
Shared / institutional responsibility: AOS-11/12/30 deliver accessible interaction; AOS-02 common records

Table row 4
Responsibility: Barriers / inference limits
AOS-03 owns: Data-design separation and receiving-use restrictions
Shared / institutional responsibility: Domains declare capabilities; AOS-04/05 enforce; AOS-02 preserves lineage

Table row 5
Responsibility: Transparency / rights
AOS-03 owns: Permitted explanatory projection, reason for restriction and review route
Shared / institutional responsibility: AOS-24 presentation; AOS-30 accountable review; professional owners resolve privacy/rights conflict

Table row 6
Responsibility: Lifecycle / locations
AOS-03 owns: Approved purpose-specific retention/deletion/disclosure and assessed locations
Shared / institutional responsibility: AOS-02 executes common record lifecycle; AOS-05 backups/runtime/provider paths; AOS-14 counterparty exchange

Table row 7
Responsibility: Monitoring
AOS-03 owns: Permission drift, suspicious scope expansion, blocked uses and exceptions
Shared / institutional responsibility: AOS-25/40 oversight; AOS-13/30 human ownership and outcome

Trust boundaries: unauthenticated input; credential versus actor; identity versus representation; domain versus domain; private assistance versus enterprise records; source versus inference; requester versus independent control; internal versus external audience; organisation versus organisation; service delivery versus model development; current processing versus retained history.

An approved policy establishes the rule. A concrete decision establishes its application to this request. Evidence of enforcement establishes that the actual processing respected the decision. Those are separate assurance claims.

3.1 Component-owned external research

Under DEC-086, AOS-03 owns the relevance and substantive implications of external research into its own function/specification, inheriting AOS-04 v0.7 §§3.1/5.1/6.6/10.8 (CON-009), AOS-02 v0.7 §6.6 (CON-007) and AOS-01 v0.7 §§6.6/10.8. Shared agents/collection infrastructure may serve distinct profiles; Boundary does not become the substantive research owner for every component. Internal operational monitoring and GI organisational sensing remain separate. Research observes, analyses, challenges and proposes; it cannot amend specifications, expand tools/powers, approve deployment or reopen DEC-018.

Table row 1
Controlled profile allocation: Remit/questions/baseline
Component-specific meaning / owner and gate: Does external evidence expose incomplete, incorrect, ambiguous or insufficiently resilient functions, or meaningful improvement? Topics: identity, authentication and representation; privacy, consent, data protection and permitted processing; resident/workforce rights, accessibility, sensitive inference, disclosure and lifecycle developments. Bind exact

assessed specification/dependency revisions, including their draft/approval status.

Table row 2
Controlled profile allocation: Jurisdiction/status/sources
Component-specific meaning / owner and gate: Prefer official regulators and government/legal texts, recognised identity/privacy standards bodies, primary research and authoritative incident accounts. Applicable jurisdictions, exact source list/admission/currentness criteria and licensing are owned profile settings; distinguish proposals, publication, enactment/adoption and effective dates. Verification is not organisational adoption or professional legal judgement.

Table row 3
Controlled profile allocation: Assignment/cadence/triggers
Component-specific meaning / owner and gate: Identity/information-governance owner with competent privacy/legal and resident/workforce reviewers owns remit/review. Assigned agent/service, approved cadence/event triggers, coverage periods and accountable tracker/cover appointments remain commissioning dependencies; no default schedule or separate deployment is mandated.

Table row 4
Controlled profile allocation: Authority/use/retrieval
Component-specific meaning / owner and gate: Applicable 01/03 permissions and 05 controls govern task/tools/data/locations; 14 governs external retrieval/admission and source verification. Public accessibility is not unrestricted reuse/disclosure; hostile source content is data, never an instruction.

Table row 5
Controlled profile allocation: Evidence/assessment
Component-specific meaning / owner and gate: Common 02 profile/run/finding/disposition views bind exact sources/assurance, publication/event/access/effective dates or explicit unknown reasons; evidence versus inference; affected CAP/FUN/REQ/CON/decision/source, alternatives, uncertainty, materiality/urgency and cross-component owners.

Table row 6
Controlled profile allocation: Coverage/quality
Component-specific meaning / owner and gate: Report actual complete/partial/failed/cancelled/not-performed coverage and bounded no-material-finding. Component reviewers with 04/40 approve relevance, evidence-fidelity, false/missed-finding and limitation rubrics before dependent reliance; deterministic enforcement is assessed separately.

Table row 7
Controlled profile allocation: Review/change
Component-specific meaning / owner and gate: Named permitted recipient/tracker, deadline/cover/escalation and empowered disposition use 13/30 and 01. Acceptance for further work, amendment approval, verification, applied release and outcome closure remain distinct. Live urgent implications use separately authorised response; research supplies no emergency power.

Table row 8
Controlled profile allocation: Setup gate
Component-specific meaning / owner and gate: Component owner owns missing profile values; 01 powers, 03 use, 05 enforcement, 14 access, 02 schemas and 04/40 evaluation owners supply their evidence. Missing mandatory values withhold dependent activation/reliance and retain an owned coverage exception. Author drafting does not establish operating readiness.

4. Capabilities, functions and requirements

4.1 Capabilities

All local CAP/FUN/REQ/CON/INV/CR/VER/ISS identifiers carry prefix AOS-03.

Table row 1

CAP: CAP-001
Outcome: Verified, scoped and accessible actor participation
FUN: 001/002

Table row 2
CAP: CAP-002
Outcome: Exact, accountable permitted-use determinations
FUN: 003/004

Table row 3
CAP: CAP-003
Outcome: Legible and effective consent lifecycle
FUN: 005/006

Table row 4
CAP: CAP-004
Outcome: Protected cross-domain processing and inference
FUN: 007/008

Table row 5
CAP: CAP-005
Outcome: Meaning-preserving disclosure and human challenge
FUN: 009/010

Table row 6
CAP: CAP-006
Outcome: Governed lifecycle, locations and change response
FUN: 011/012

Table row 7
CAP: CAP-007
Outcome: Research external developments affecting this component and propose governed adaptation
FUN: 013

4.2 Functions

Table row 1
FUN / trigger: 001 - Actor access or changed credentials
Inputs and behaviour: Verify organisation, actor, assurance evidence and required currentness under approved risk profile
Output / authority / uncertainty and failure: Verified/unverified/unresolved identity. Unverified actor cannot gain protected access; authorised public/assisted service assessed separately

Table row 2
FUN / trigger: 002 - Role or representation claim
Inputs and behaviour: Resolve current role/powers and specific represented person/principal; distinguish person, household, agent, service and deployment
Output / authority / uncertainty and failure: Scoped acting capacity. Tenancy/address/household membership alone cannot grant representation

Table row 3
FUN / trigger: 003 - Proposed processing
Inputs and behaviour: Bind exact actor, data revisions/selection, operation/inference, purpose, basis, audience, locations and current policies
Output / authority / uncertainty and failure: REC-D permit/deny/unresolved; missing required evidence is unresolved; control failure is unavailable

Table row 4
FUN / trigger: 004 - Reliance at a processing boundary
Inputs and behaviour: Validate scope/versions/conditions at approved last-enforceable checkpoint independently of requesting intelligence
Output / authority / uncertainty and failure: Checked permit or withheld processing; actual race/currentness evidence recorded

Table row 5
FUN / trigger: 005 - Consent offered, changed or renewed
Inputs and behaviour: Present accessible notice; record actual expression and scoped choices by appropriately verified person/representative
Output / authority / uncertainty and failure: Evidence-linked consent state. Silence, ongoing tenancy or technical acceptance does not supply consent

Table row 6
FUN / trigger: 006 - Withdrawal, expiry or invalidation
Inputs and behaviour: Identify dependent purposes, pending work and downstream derived artefacts; apply approved stopping/lifecycle rules
Output / authority / uncertainty and failure: Invalidation and disposition evidence; independent uses assessed separately, not silently re-labelled

Table row 7
FUN / trigger: 007 - Sensing or inference design/use
Inputs and behaviour: Check declared purpose, necessity, asset/behaviour separation and permitted inference; assess cross-layer joins
Output / authority / uncertainty and failure: Permitted bounded operation or blocked design/use; unexpected inference surfaces a design gap

Table row 8
FUN / trigger: 008 - Cross-domain/private-to-enterprise transfer
Inputs and behaviour: Check receiving purpose and disclosure, preserve restrictions/lineage; private boundary follows Q02 under the approved direction
Output / authority / uncertainty and failure: Approved projection or withheld transfer; receipt never broadens permission

Table row 9
FUN / trigger: 009 - Explanation/disclosure request
Inputs and behaviour: Assess requester/audience, sensitivity and assurance chain; produce permitted meaningful projection
Output / authority / uncertainty and failure: Explanation with evidence/limitations and review route; restricted details follow recorded exception policy

Table row 10
FUN / trigger: 010 - Rights, challenge or welfare/consent conflict
Inputs and behaviour: Route minimal permitted evidence to empowered human; track acknowledgement and outcome
Output / authority / uncertainty and failure: Pending/resolved disposition under approved powers; no automatic values adjudication or emergency permission

Table row 11
FUN / trigger: 011 - Retention/deletion/location change
Inputs and behaviour: Assess applicable class policy, independent duties, actual copies/providers/access locations and approved disposition
Output / authority / uncertainty and failure: Governed lifecycle/change result; conflict referred, unapproved new use/location withheld

Table row 12
FUN / trigger: 012 - Rule/model/role/correction change
Inputs and behaviour: Find materially affected pending uses and evaluate changed conditions; retain historical effect evidence
Output / authority / uncertainty and failure: Reassessment, version/impact record and approval-dependent activation; no automatic policy expansion

Table row 13

FUN / trigger: 013 - External research
Inputs and behaviour: Approved profile and external event/cycle; retrieve through 14 and assess exact component baseline
Output / authority / uncertainty and failure: Common coverage/finding and tracked human review; no self-amendment

4.3 Requirement register

Every row is a proposed, independently assessable obligation, originated in v0.1 on 5 October 2026. Scope is the whole logical component; dependent build/activation is unselected. Category codes: C = component behaviour, I = interface, D = design constraint; S = source-derived, E = engineering derivation. Sources are exact keys in §2, with finer locators where shown. Rationale is the last phrase in the source column.

Accountable component owner: organisational identity/information-governance steward, appointment open. Project baseline approver: Mark. Legal/policy approval remains with the empowered organisational owners; code deployment does not supply that approval. Each row inherits these metadata and this change history. §16/17 contain unresolved dependencies; §15 supplies planned acceptance. Q-dependent rows implement approved design directions DEC-049-053; the exact proposed obligation wording and detailed commissioning remain unapproved.

Table row 1
REQ: 001
Proposed obligation: Protected processing shall require actor identity assurance meeting the approved operation-risk profile.
Category / source / rationale: C/E; S09/S11, Q01; prevent credential-only permission
FUN / dependencies: 001; CON-001; ISS-001
VER: 001

Table row 2
REQ: 002
Proposed obligation: An acting role shall be validated for the specific organisation and current request context.
Category / source / rationale: C/S; S08/S09; no role or tenant-scope inheritance
FUN / dependencies: 002; CON-001
VER: 002

Table row 3
REQ: 003
Proposed obligation: Representation of another person shall require evidence of authority for the specific represented person and operation.
Category / source / rationale: C/E; S01/S11; no household-wide assumed consent
FUN / dependencies: 002; ISS-006
VER: 002

Table row 4
REQ: 004
Proposed obligation: A data-use request shall identify the exact data scope, operation and proposed purpose.
Category / source / rationale: I/S; S02/S11 REC-R11; bounded processing
FUN / dependencies: 003; CON-002
VER: 003

Table row 5
REQ: 005
Proposed obligation: A permitted-use result shall identify the approved processing-basis evidence applicable to that operation.
Category / source / rationale: I/E; S11 REC-D §5.1, EXT-P01; basis is evidenced not asserted
FUN / dependencies: 003; ISS-007
VER: 003

Table row 6
REQ: 006

Proposed obligation: A processing permission shall remain distinct from the organisational authority required for an associated action.
Category / source / rationale: C/S; S09 DEC-005, S11 §5.2; neither check grants the other
FUN / dependencies: 003/004; AOS-01
VER: 004

Table row 7
REQ: 007
Proposed obligation: Dependent processing shall be withheld when its required use result is denied, unresolved or unavailable.
Category / source / rationale: C/E; S02/S10 DEC-028, S11 SC-R03; no permissive failure
FUN / dependencies: 004; AOS-04/05
VER: 004/005

Table row 8
REQ: 008
Proposed obligation: Reliance on a permit shall validate its current scope, conditions and policy state at the approved last-enforceable processing boundary.
Category / source / rationale: C/S; S10 DEC-028, S11; bounded currentness
FUN / dependencies: 004; ISS-008
VER: 005

Table row 9
REQ: 009
Proposed obligation: A receiving component shall evaluate its proposed use rather than inherit permission from source admission or sending authority.
Category / source / rationale: C/S; S05, S09 REQ-004; receiving purpose matters
FUN / dependencies: 003/008; CON-002
VER: 006

Table row 10
REQ: 010
Proposed obligation: A permitted-use assessment of transformed or combined information shall establish its contributing-source lineage, satisfy all applicable source-use restrictions and account for additional sensitive information the combination reveals; insufficient lineage or permitted-use evidence shall withhold the affected use and refer the uncertainty for accountable review.
Category / source / rationale: I/S; S05/S11 REC-R13; DEC-099 approved direction; prevent transformation laundering
FUN / dependencies: 007/008; CON-004; AOS-02
VER: 006/007

Table row 11
REQ: 011
Proposed obligation: Asset-condition sensing shall be separated from personal behavioural inference at data design, processing, storage and action boundaries.
Category / source / rationale: D/S; S03; absolute category separation
FUN / dependencies: 007; ISS-009
VER: 007

Table row 12
REQ: 012
Proposed obligation: Resident behavioural inference from sensing shall require demonstrated necessity, explicit consent, separate governance and a defined review cycle.
Category / source / rationale: C/S; S04; convenience is insufficient
FUN / dependencies: 007; ISS-003/009
VER: 008

Table row 13
REQ: 013
Proposed obligation: A cross-layer purpose expansion shall require explicit consent-based authorisation under the governing RP scope.
Category / source / rationale: C/S; S05; no silent workforce/process profiling
FUN / dependencies: 007/008; ISS-004/007

VER: 009

Table row 14
REQ: 014
Proposed obligation: A consent record shall identify the person, exact scope, applicable notice revision and evidence of the actual expression of consent.
Category / source / rationale: I/E; S01/S04/S11; reconstruct the choice
FUN / dependencies: 005; CON-003; ISS-006
VER: 010

Table row 15
REQ: 015
Proposed obligation: Silence, non-engagement, tenancy continuity or absence of complaint shall not be recorded as consent.
Category / source / rationale: C/S; S01 FP7; no-exit is not assent
FUN / dependencies: 005; AOS-11/12
VER: 010

Table row 16
REQ: 016
Proposed obligation: Consent management shall provide accessible human-assisted routes for giving, reviewing and withdrawing consent.
Category / source / rationale: C/E; S01 FP4/7, EXT-P01; usable choice
FUN / dependencies: 005/006; Q01/Q04
VER: 011

Table row 17
REQ: 017
Proposed obligation: Consent withdrawal or expiry shall invalidate dependent pending uses under the approved enforcement profile.
Category / source / rationale: C/S; S10 DEC-028, S11 §5.2; effective withdrawal
FUN / dependencies: 006; CON-003; ISS-008
VER: 012

Table row 18
REQ: 018
Proposed obligation: A separate retained or continuing use after consent withdrawal shall require its own approved basis and scoped determination.
Category / source / rationale: C/E; S11 §5.2, S10 DEC-047; no silent basis switch
FUN / dependencies: 006/011; ISS-007/010
VER: 012/013

Table row 19
REQ: 019
Proposed obligation: A welfare exception shall not be activated solely by an agent’s classification of concern.
Category / source / rationale: C/S; S06/S08; no invented emergency powers
FUN / dependencies: 010; Q03; ISS-003
VER: 014

Table row 20
REQ: 020
Proposed obligation: A welfare-versus-consent conflict shall be referred through an explicitly authorised route to an empowered human under a documented board-approved hierarchy.
Category / source / rationale: C/S; S06, S10 DEC-033/034; accountable conflict resolution
FUN / dependencies: 010; Q03; AOS-01/13/30
VER: 014

Table row 21
REQ: 021
Proposed obligation: Resident communication shall use the channel or channels agreed with that resident for the communication

concerned.
Category / source / rationale: C/S; S10 DEC-041; permission is not channel agreement
FUN / dependencies: 009; AOS-11/14; ISS-011
VER: 015

Table row 22
REQ: 022
Proposed obligation: Private resident-assistant content shall remain outside enterprise use unless a specific authorised sharing or exception route is established.
Category / source / rationale: D/E; S01/S02, Q02; private support cannot imply observation
FUN / dependencies: 008; Q02; ISS-002
VER: 016

Table row 23
REQ: 023
Proposed obligation: Optional-use refusal or withdrawal shall not trigger adverse service or employment consequences attributable to that refusal.
Category / source / rationale: D/E; S01 FP7, Q04; make choice credible
FUN / dependencies: 005/006; ISS-004
VER: 017

Table row 24
REQ: 024
Proposed obligation: Disclosure shall be limited to the permitted recipient, content scope, onward use and assessed processing/access locations.
Category / source / rationale: C/S; S08/S09 DEC-020, S11 REC-D; destination matters
FUN / dependencies: 009/011; CON-005; ISS-012
VER: 018

Table row 25
REQ: 025
Proposed obligation: An explanatory projection shall preserve the material meaning, uncertainty and approval status of the decision or evidence disclosed.
Category / source / rationale: I/S; S07/S12; disclosure cannot become a misleading summary
FUN / dependencies: 009; CON-005; Q05
VER: 019

Table row 26
REQ: 026
Proposed obligation: An explanatory projection shall retain a permitted account of the source of assurance for facts material to the explanation.
Category / source / rationale: I/S; S10 DEC-046, S12 §3.1; origin is not assurance
FUN / dependencies: 009; Q05; AOS-02/24
VER: 019

Table row 27
REQ: 027
Proposed obligation: A constraint explanation shall state its meaning, authority basis and referral route unless an approved recorded exception applies.
Category / source / rationale: I/S; S10 DEC-027; legible constraints
FUN / dependencies: 009/010; ISS-005
VER: 019/020

Table row 28
REQ: 028
Proposed obligation: A restricted explanation shall record the reason and accountable review route without waiving the underlying control.
Category / source / rationale: C/S; S10 DEC-027, Q05; restriction is reviewable

FUN / dependencies: 009/010; ISS-005
VER: 020

Table row 29
REQ: 029
Proposed obligation: Privacy review shall not remove a protected finding’s required audience obligation through ordinary configuration.
Category / source / rationale: D/S; S08 RP8 protected audience; no quiet suppression
FUN / dependencies: 009/010; AOS-01/25; ISS-005
VER: 020

Table row 30
REQ: 030
Proposed obligation: Retention, correction, restriction and deletion shall follow the approved record-class lifecycle policy.
Category / source / rationale: C/S; S10 DEC-047, S12; history and minimisation governed
FUN / dependencies: 011; CON-006; ISS-010
VER: 013

Table row 31
REQ: 031
Proposed obligation: A deletion disposition shall not preserve hidden content copies outside the approved lifecycle policy.
Category / source / rationale: D/S; S10 DEC-047; minimal disposition is not shadow retention
FUN / dependencies: 011; AOS-02/05; ISS-010
VER: 013/021

Table row 32
REQ: 032
Proposed obligation: A new or changed storage, processing, backup or access-location arrangement shall require assessment and explicit approval before its dependent use.
Category / source / rationale: D/S; S09 DEC-020; actual providers/support paths matter
FUN / dependencies: 011; CON-006; ISS-012
VER: 018/021

Table row 33
REQ: 033
Proposed obligation: Organisational data and permissions shall remain isolated from other organisational AOS instances.
Category / source / rationale: D/S; S09 DEC-014/REQ-035; no cross-organisation inherited scope
FUN / dependencies: 001/004; AOS-02/05
VER: 022

Table row 34
REQ: 034
Proposed obligation: A rights request or permitted-use challenge shall have a recorded accountable human route and disposition state.
Category / source / rationale: C/E; S01/S07, EXT-P03; request is not fulfilled by receipt
FUN / dependencies: 010; AOS-13/30; ISS-006
VER: 011

Table row 35
REQ: 035
Proposed obligation: A permission-affecting correction shall trigger reassessment of materially dependent pending work under the approved impact profile.
Category / source / rationale: C/S; S10 DEC-029; selective pending-work review
FUN / dependencies: 012; CON-004; ISS-008
VER: 023

Table row 36
REQ: 036
Proposed obligation: A completed processing effect shall retain its historical basis and known consequence without retrospective permission rewriting.

Category / source / rationale: C/S; S10 DEC-029/047, S11; correction is not history erasure
FUN / dependencies: 012; AOS-02; ISS-010
VER: 023

Table row 37
REQ: 037
Proposed obligation: Unknown disclosure effect shall remain indeterminate pending authorised reconciliation before consequential repetition.
Category / source / rationale: C/S; S10 DEC-030; avoid duplicate exposure
FUN / dependencies: 009/012; AOS-14/05
VER: 024

Table row 38
REQ: 038
Proposed obligation: A model, tool or retrieved-content output shall not grant or expand a data-use policy or consent scope.
Category / source / rationale: D/E; S02/S08/S09 DEC-005/031; model output is not permission
FUN / dependencies: 003/004/012; AOS-04/05
VER: 025

Table row 39
REQ: 039
Proposed obligation: Personal data use for model training or provider service improvement shall require a separately assessed and approved purpose and processing arrangement.
Category / source / rationale: D/E; S02/S05, EXT-P01; delivery permission cannot cover training
FUN / dependencies: 007/011; ISS-007/012
VER: 009/018

Table row 40
REQ: 040
Proposed obligation: A data-use determination shall retain the exact request revision, checked instruments, evaluator, result, conditions and contemporaneous evaluation evidence.
Category / source / rationale: I/S; S07/S11 REC-D; DEC-064 clarifies original evaluation before later enforcement
FUN / dependencies: 003/004; AOS-02/05; Core v0.2 §5.3
VER: 003/005

Table row 41
REQ: 041
Proposed obligation: Sensitive-data processing shall require verified additional conditions and safeguards applicable to its assessed category and jurisdiction.
Category / source / rationale: C/E; S08, EXT-P02; no missing category protection
FUN / dependencies: 003/007; ISS-007/009
VER: 008/009

Table row 42
REQ: 042
Proposed obligation: AOS-03 shall reject a permission or consent configuration that enables AI presence, observation or live capture in boardroom deliberation.
Category / source / rationale: D/S; S01 RP2, S09 REQ-008/031; consent cannot waive core
FUN / dependencies: 003/012; AOS-01/24/30
VER: 025

Table row 43
REQ: 043
Proposed obligation: Each component exchange shall reference the common definition, exact revision and profiles allocated to its CON in the Kernel Exchange Register.
Category / source / rationale: I/S; KXR-01/08; DEC-002/065; QS-12/21
FUN / dependencies: §6.3/§19.2; AOS-02 with semantic owner; register v0.1
VER: 026/030

Table row 44
REQ: 044
Proposed obligation: A receiving exchange shall reject or hold unresolved an unsupported revision unless an explicitly reviewed translation preserves required meaning and restrictions and declares accepted loss.
Category / source / rationale: I/S; KXR-02/07; DEC-065; FP4/6; RP9
FUN / dependencies: §6.3/§19.2; AOS-02 with semantic owner; register v0.1
VER: 026

Table row 45
REQ: 045
Proposed obligation: Reliance on a fact for a conclusion or action shall evaluate its linked assurance against the required profile for that exact fact revision and intended use.
Category / source / rationale: I/S; KXR-04; DEC-062/063; FP4/6; RP7
FUN / dependencies: §6.3/§19.2; AOS-02 with semantic owner; register v0.1
VER: 027/031

Table row 46
REQ: 046
Proposed obligation: An exchange acknowledgement shall identify its actually evidenced stage without implying subsequent application, human responsibility or effect.
Category / source / rationale: I/S; KXR-06; DEC-066; RP1; GT M1.13
FUN / dependencies: §6.3/§19.2; AOS-02 with semantic owner; register v0.1
VER: 029

Table row 47
REQ: 047
Proposed obligation: A checkpoint or later enforcement/effect record shall link to the exact original permission-evaluation revision without rewriting its original result or presenting a pending evidence link as enforcement proof.
Category / source / rationale: I/S; KXR-05; DEC-064; RP7 auditability
FUN / dependencies: §6.3/§19.2; AOS-02 with semantic owner; register v0.1
VER: 028

Table row 48
REQ: 048
Proposed obligation: The data-use service shall supply current identity, basis, consent and restriction evidence for the exact operation-bound checkpoint.
Category / source / rationale: I/S; DEC-067; KCR-01; FP4/5/6/7/10; RP1/7/8/9
FUN / dependencies: §6.4/§19.3; AOS-01-05 respective owner; Control Coordination v0.1
VER: 032/033

Table row 49
REQ: 049
Proposed obligation: A changed use-policy configuration shall not supply favourable reliance until required dependencies evidence compatible applied state.
Category / source / rationale: I/S; DEC-068; KCR-02; FP4/5/6/7/10; RP1/7/8/9
FUN / dependencies: §6.4/§19.3; AOS-01-05 respective owner; Control Coordination v0.1
VER: 033

Table row 50
REQ: 050
Proposed obligation: A consent or use restriction change shall track materially dependent receiving application or an owned unresolved exception.
Category / source / rationale: I/S; DEC-069; KCR-03; FP4/5/6/7/10; RP1/7/8/9
FUN / dependencies: §6.4/§19.3; AOS-01-05 respective owner; Control Coordination v0.1
VER: 034/035

Table row 51

REQ: 051
Proposed obligation: Cumulative grouping and measurement shall remain within approved processing purposes and information barriers.
Category / source / rationale: I/S; DEC-070; KCR-04; FP4/5/6/7/10; RP1/7/8/9
FUN / dependencies: §6.4/§19.3; AOS-01-05 respective owner; Control Coordination v0.1
VER: 036/037

Table row 52
REQ: 052
Proposed obligation: Data-use permission for a bounded operation shall not substitute for authoritative reservation of the required shared capacity.
Category / source / rationale: I/S; DEC-071; KCR-05; FP4/5/6/7/10; RP1/7/8/9
FUN / dependencies: §6.4/§19.3; AOS-01-05 respective owner; Control Coordination v0.1
VER: 036

Table row 53
REQ: 053
Proposed obligation: Uncertain disclosure or processing effects shall retain their bounded exposure pending authorised reconciliation rather than being assumed absent.
Category / source / rationale: I/S; DEC-071; KCR-06; FP4/5/6/7/10; RP1/7/8/9
FUN / dependencies: §6.4/§19.3; AOS-01-05 respective owner; Control Coordination v0.1
VER: 037

Table row 54
REQ: 054
Proposed obligation: Withholding notifications and appropriate resident updates shall use separately permitted audiences, minimal content and resident-agreed channels where applicable.
Category / source / rationale: I/S; DEC-071; KCR-07; FP4/5/6/7/10; RP1/7/8/9
FUN / dependencies: §6.4/§19.3; AOS-01-05 respective owner; Control Coordination v0.1
VER: 038/039

Table row 55
REQ: 055
Proposed obligation: Resumption of braked processing shall require current valid use conditions and reconciled dependencies without restarting withdrawn uses.
Category / source / rationale: I/S; DEC-072; KCR-08; FP4/5/6/7/10; RP1/7/8/9
FUN / dependencies: §6.4/§19.3; AOS-01-05 respective owner; Control Coordination v0.1
VER: 035/039

Table row 56
REQ: 056
Proposed obligation: Use governance shall define advance independently verifiable permissions, minimal payload and normal/appropriately independent alternative audiences for each mandatory protected-finding class, without an implicated sole release gatekeeper or implied external disclosure power.
Category / source / rationale: I/S; DEC-073/104; KPR-01; STD-05 CP-8/CP-8(2)/(3), IR-6/IR-8; STD-01/02/03/04 scope alignment
FUN / dependencies: §6.5/§19.4; Protected Reporting and Recovery v0.2; AOS-03-CON-002/003/004/005/006/007
VER: 040

Table row 57
REQ: 057
Proposed obligation: Minimum failure-reporting use permission shall be approved in advance and bind purpose, data scope, independently verifiable recipients and validity without emergency expansion.
Category / source / rationale: I/S; DEC-074; KPR-02; STD-05 AC-6; STD-03/04 scope alignment
FUN / dependencies: §6.5/§19.4; Protected Reporting and Recovery v0.1; AOS-03-CON-002/003/004/005/006/007
VER: 041

Table row 58
REQ: 058
Proposed obligation: Protected handoff and affected-resident updates shall use permitted minimal content and agreed channels,

retaining an owned unresolved duty when delivery or acceptance fails.
Category / source / rationale: I/S; DEC-075; KPR-03; STD-05 IR-6/IR-8; STD-01 scope alignment; AOS-specific acceptance/continuing duty
FUN / dependencies: §6.5/§19.4; Protected Reporting and Recovery v0.1; AOS-03-CON-002/003/004/005/006/007
VER: 042

Table row 59
REQ: 059
Proposed obligation: Recovery shall prove complete current identity, consent/basis, use restrictions and deletion dispositions for affected scope rather than rely on a protected but stale copy.
Category / source / rationale: I/S; DEC-076; KPR-04; STD-05 CP-9/CP-9(1), AU-9; STD-02/03/04 scope alignment; AOS-specific currentness/completeness
FUN / dependencies: §6.5/§19.4; Protected Reporting and Recovery v0.1; AOS-03-CON-002/003/004/005/006/007
VER: 043

Table row 60
REQ: 060
Proposed obligation: Restored data shall remain isolated from normal processing until current restrictions/deletions are applied and any unknown disclosure effects are reconciled conservatively.
Category / source / rationale: I/S; DEC-077; KPR-05; STD-05 CP-10/CP-10(2)/(4)/(6); STD-01/02 scope alignment; AOS-specific current restriction/effect gate
FUN / dependencies: §6.5/§19.4; Protected Reporting and Recovery v0.1; AOS-03-CON-002/003/004/005/006/007
VER: 044

Table row 61
REQ: 061
Proposed obligation: Scoped release shall require accepted current use evidence and applicable human acceptance; automatic failover shall not bypass current processing restrictions.
Category / source / rationale: I/S; DEC-078; KPR-06; STD-05 CP-4/CP-4(4); STD-01/02 scope alignment; AOS-specific release/duty gate
FUN / dependencies: §6.5/§19.4; Protected Reporting and Recovery v0.1; AOS-03-CON-002/003/004/005/006/007
VER: 045

4.4 External-research adoption requirements

New AOS-03-REQ-062-068 originate in v0.7, 6 October 2026; proposed logical component wording, accountable semantic/component owner per §3.1, project approver Mark, organisational instruments/appointments open. No prior REQ is retired or promoted.

Table row 1
REQ: 062
Proposed independently verifiable obligation: The component shall bind its external-research task to a controlled component-specific profile inheriting AOS-04-CON-009 and the exact assessed baseline/status.
Derivation / function / contract: DEC-086; AOS-03-CAP-007/FUN-013/CON-008; common 04/02/01 inheritance
Planned VER: 046

Table row 2
REQ: 063
Proposed independently verifiable obligation: Research retrieval, processing and disclosure shall use AOS-14-governed access with current applicable AOS-01/03 determinations and independently enforced AOS-05 controls.
Derivation / function / contract: DEC-086; AOS-03-CAP-007/FUN-013/CON-008; common 04/02/01 inheritance
Planned VER: 047

Table row 3
REQ: 064

Proposed independently verifiable obligation: The component shall produce and consume AOS-02 §6.6 profile/run/finding/disposition views with linked evidence, assurance, legal/standards applicability/status and explicit coverage limitations.
Derivation / function / contract: DEC-086; AOS-03-CAP-007/FUN-013/CON-008; common 04/02/01 inheritance
Planned VER: 048

Table row 4
REQ: 065
Proposed independently verifiable obligation: Shared retrieval, duplicate coalescing and source/baseline correction shall retain each affected component's assessment, accountable review duty and recorded reassessment.
Derivation / function / contract: DEC-086; AOS-03-CAP-007/FUN-013/CON-008; common 04/02/01 inheritance
Planned VER: 049

Table row 5
REQ: 066
Proposed independently verifiable obligation: Research review shall retain an accountable handoff and empowered exact-revision disposition, with separately authorised urgent handling and no implied amendment or release approval.
Derivation / function / contract: DEC-086; AOS-03-CAP-007/FUN-013/CON-008; common 04/02/01 inheritance
Planned VER: 050

Table row 6
REQ: 067
Proposed independently verifiable obligation: Dependent research reliance shall require accepted component relevance/evidence-fidelity and false/missed-finding evaluation criteria, assessed separately from deterministic control enforcement.
Derivation / function / contract: DEC-086; AOS-03-CAP-007/FUN-013/CON-008; common 04/02/01 inheritance
Planned VER: 051

Table row 7
REQ: 068
Proposed independently verifiable obligation: Missing mandatory profile settings, denied access, failed coverage or delivery shall remain owned exceptions rather than favourable coverage, substituted permissions or completed review.
Derivation / function / contract: DEC-086; AOS-03-CAP-007/FUN-013/CON-008; common 04/02/01 inheritance
Planned VER: 046

Table row 8
REQ: 069
Proposed independently verifiable obligation: The data-use control shall access the control metadata needed to assess a request only through a separately established, advance-authorised minimum-access permission verifiable independently of the requested business action's outcome.
Derivation / function / contract: C/I; DEC-100; independent bootstrap without implied business/data permission
Planned VER: CON-001/002; DEC-100 approved control profile and verification gate
Additional field: 052

5. State model

Identity assurance, representation, consent, permit currency and lifecycle disposition are orthogonal. An authenticated actor can have expired representation; a current consent can cover an operation that the agent lacks authority to execute; withdrawal does not imply that every retained record can be deleted.

Table row 1
Governed object / transition: Identity: claimed → verified / unverified / unresolved
Entry evidence and authority: Approved assurance profile, actual verification and organisation context
Permitted outcome / failure semantics: Verified for stated operation class; insufficient assurance withholds protected access, not all public/assisted service

Table row 2

Governed object / transition: Role/representation: pending → valid → expired / withdrawn / unresolved
Entry evidence and authority: Empowered source and effective scope/time; approval evidence
Permitted outcome / failure semantics: Cannot represent unrelated household members or inherit a service account’s unrestricted rights

Table row 3
Governed object / transition: Consent: not established → active / refused → changed / withdrawn / expired
Entry evidence and authority: Accessible notice, actual expression, person/representative and scope
Permitted outcome / failure semantics: State change never manufactures a new processing basis; no universal consent expiry is invented

Table row 4
Governed object / transition: Use request: submitted → evaluated → permit / deny / unresolved
Entry evidence and authority: Exact request and current approved instruments
Permitted outcome / failure semantics: Unavailable is an operational failure, not a favourable result; narrowed scope requires a checked revised request

Table row 5
Governed object / transition: Permit: valid → used / expired / invalidated
Entry evidence and authority: Currentness/enforcement checkpoint
Permitted outcome / failure semantics: Old permit cannot cover changed purpose, recipient or operation; effect already beyond checkpoint requires incident review

Table row 6
Governed object / transition: Challenge: received → human owned → assessed → disposition / follow-up
Entry evidence and authority: Verified requester where required; separately authorised route and role
Permitted outcome / failure semantics: Delivery is not ownership or resolution; deadlines/cover commissioned, not supplied by this draft

Table row 7
Governed object / transition: Lifecycle: retained → restricted / deletion pending → disposed
Entry evidence and authority: Class policy, legal/privacy assessment and authorised disposition
Permitted outcome / failure semantics: Conflicts remain unresolved and dependent use withheld; authorised custody assessed separately

Table row 8
Governed object / transition: Disclosure attempt: prepared → dispatched → confirmed / partial / indeterminate
Entry evidence and authority: Independent use and action checks; actual transport/effect evidence
Permitted outcome / failure semantics: No reply is not proof of failure; reconciliation itself requires permission

Closed consent requests and challenges retain only permitted evidence. Restart, cache restoration or administrator credential reset cannot reactivate withdrawn permission. A lawful historical processing event is not made unlawful merely by a later withdrawal, nor does its history permit future reuse.

6. Semantic contracts and interfaces

6.1 Catalogue

REC-D in Core Records §5 remains the single proposed detailed data-use definition. This draft allocates its semantic responsibilities and adds no competing field dictionary. The consulted initial catalogue had no AOS-03 IF; the current register allocates proposed AOS-03-IF-001 to existing REC-D. CON IDs are component contract references, not claims that new IFs were approved.

Table row 1
CON: CON-001 - Identity and capacity

Owner / producers → consumers: AOS-03; identity/role/representation authorities → AOS-01/02/04/05/14/30
Meaning / controlled definition: Organisation, actor, acting role, represented principal/person, scope, assurance method/evidence, effective state and limitations; common shape AOS-02, exact profile pending

Table row 2
CON: CON-002 - Permitted-use determination
Owner / producers → consumers: AOS-03; control ↔ all processing consumers
Meaning / controlled definition: REC-D: actor/data/revisions/operation/inference/purpose/basis/recipient/locations, result/conditions/explanation, versions/currentness/invalidation and evaluator; Core Records §5

Table row 3
CON: CON-003 - Consent and change
Owner / producers → consumers: AOS-03; person/representative through AOS-11/12/30 → controls/dependency consumers
Meaning / controlled definition: Exact scope and notice, actual expression, accessible route, revision/effective time, withdrawal/expiry/change and delivery/processing evidence; schema pending

Table row 4
CON: CON-004 - Restriction and impact lineage
Owner / producers → consumers: AOS-02 common lineage, AOS-03 use semantics; source/correction/consent controls → affected components
Meaning / controlled definition: Original and derived scopes, materially affected pending uses, change basis/version, reassessment and downstream acknowledgement; REC-E/D links, exact dependency profile pending

Table row 5
CON: CON-005 - Disclosure and explanation
Owner / producers → consumers: AOS-03 permission, AOS-02 source meaning, AOS-24 rendering, AOS-14 external exchange
Meaning / controlled definition: Exact audience/purpose, permitted content/provenance/assurance projection, restrictions/limitations/review reference, dispatch/effect state; parent AOS-14-IF-001 and canonical AOS-20-IF-001 preserved

Table row 6
CON: CON-006 - Lifecycle and location approval
Owner / producers → consumers: AOS-03 policy, AOS-02 record structure, AOS-05 physical/runtime lifecycle
Meaning / controlled definition: Class/purpose/copy inventory, retention/restriction/deletion basis, assessed locations/providers/support, disposition evidence and unresolved conflict; profile pending

Table row 7
CON: CON-007 - Human conflict, rights and exception
Owner / producers → consumers: AOS-03 use constraints, AOS-01 decision powers, AOS-13/30 handoff/disposition
Meaning / controlled definition: Minimal authorised referral, named accountable role, approved hierarchy/instrument and actual decision/outcome; parent AOS-13-IF-001/AOS-30-IF-001 preserved

AOS-01-IF-001/002 and AOS-02-IF-001 retain their identifiers and authoritative meanings. Under DEC-100, permission checks use separately advance-authorised minimum control-metadata access, verifiable independently of the requested business action. REC-A and REC-D cannot create favourable permissions for one another from the business request. AOS-03 REQ-069 / VER-052 and AOS-01 REQ-069 / VER-045 define the reciprocal obligation/planned evidence; an implemented non-circular bootstrap remains to be demonstrated before dependent reliance.

6.2 Required semantics and unresolved profile settings

Every contract identifies accepted revision, organisation, request/record identities, actor/capacity and causal references. Data selectors distinguish fixed revisions from explicitly approved dynamic selection. Code lists distinguish permit, deny, unresolved, unavailable, unknown, withheld and not applicable; absence is never true/false consent. Units are non-applicable to categorical decisions, but time values retain precision, effective/receipt times and calendar context; scope-specific numeric thresholds need approved units/ranges.

Producers and consumers validate mandatory/conditional fields and unresolved references. Unsupported versions return incompatible/unresolved, without permissive conversion. Exact fields/types/cardinalities/value sets remain shared-schema work; they are build blockers where relied upon.

Timing and expiry use commissioned risk/purpose profiles. Acknowledgement distinguishes technical receipt, applied invalidation, human responsibility and actual effect. Change ordering uses consent/policy/request revisions and defined causal scope; latest arrival does not defeat an effective withdrawal. Same-identity conflicting content is a conflict, not a harmless replay.

Retries cannot broaden a purpose, switch basis or duplicate a consequential disclosure. Unknown effect is reconciled before permitted repetition. Revocation/withdrawal/currentness profiles specify the actual checkpoint, propagation delay, caches, pending work, reconnection and restart behaviour; no instant global cancellation or recall of already delivered information is claimed.

6.3 Reciprocal common-definition adoption, 6 October 2026

AOS-03 adopts Kernel Exchange Register v0.1 (aos-kernel-exchange-register-v0-1.md) §§3-6 at revision 0.1, Core Record Contracts v0.2 and Shared Contracts v0.2 as its single proposed logical definitions. Each local CON retains its identifier and purpose; the register §6 names every produced/consumed family and reciprocal kernel end. No alternative local fields override them. Producers name exact revisions/profiles; receivers validate matching meaning, authorised access and compatibility. Proposed AOS-03-IF-001/REC-D and AOS-04-IF-001/REC-X are catalogue allocations, not schema approval. Required acknowledgement stages and rejection/partial/unresolved responses follow KX-21; actual effect remains REC-X.

DEC-062-066 are approved detailed directions. Organisation role appointments, vocabulary/threshold/unit profiles, executable wire schemas, current-control/propagation and recovery mechanisms, and non-kernel endpoint adoption remain explicit dependencies. Earlier §6 descriptions of pending schema work are resolved only at this common logical level; commissioning and build evidence remain open.

6.4 Action-3 reciprocal coordination adoption

AOS-03 adopts Kernel Control Coordination v0.1 (aos-kernel-control-coordination-v0-1.md) §§2-10, Kernel Exchange Register v0.2 and Core/Shared v0.3 as the single proposed logical checkpoint/activation/change/account/reservation/withholding/resume definitions. Original CON IDs remain stable; Register §10 and Control Coordination §9 extend their common family views. Existing §6.3/§19.2 versions identify action-2 history; current declared definition revisions use Register v0.2 §4/§10, never an inferred version conversion.

AOS-01 supplies current authority/restrictions and powers; AOS-03 supplies identity/use/basis/consent; AOS-04 supplies exact task/effect/grouping/demand; AOS-05 gates actual effects and maintains authoritative account/reservation/applied state; AOS-02 supplies common dependency/assurance/account evidence. KX-24 ACC and KX-25 RSV are produced authoritatively by AOS-05 and consumed by AOS-01/02/03/04/05 only within permitted scope; KX-26 WHD is a continuing-duty view from service/execution workflow with AOS-05 blocker evidence, not an automatic notification exemption. Exact dependent CON allocation is the annex §9 table.

Every relevant change tracks receiving application or a reasoned no-material-dependency/owned unresolved result. Withholding creates an accountable separately authorised notification, human responsibility acknowledgement/cover/escalation, traceable coalescing and appropriate resident workflow update through resident-agreed channels. If delivery fails, the duty remains owned. Acknowledged handoff is not service completion. Independent reporting route/current recovered-state proof remain action 4; no claim of delivery capacity here.

6.5 Action-4 protected reporting and recovery adoption

AOS-03 adopts Protected Reporting and Recovery v0.1 (aos-kernel-protected-reporting-and-recovery-v0-1.md) §§2-8 as the

single proposed logical specification under approved DEC-073-078. Current baseline: AOS-00/Map v0.18; AOS-01-05 v0.6; Core/Shared v0.4; Exchange Register v0.3; Control Coordination v0.2. Existing CON/IF identifiers remain; AOS-03-CON-002/003/004/005/006/007 consume/produce the annex §5 views. KX-19 protected finding, KX-20 recovery and KX-26 continuing duty use their newly declared revisions in Register v0.3. Older action-2/3 declarations remain historical and require explicit reviewed compatibility, never automatic conversion.

The common envelope, REC-E/A/D/X/Q and CHECK/ACT/CHG/ACC/RSV/WHD remain distinct. Protected reporting adds separately approved route/permission/recipient/custody and human responsibility evidence; recovery adds authoritative currentness/completeness, isolation/reconciliation and scoped empowered release. Custody, technical receipt, system availability and accepted responsibility are different results. Operational role appointments, deadlines, accepted source mechanisms and actual fallbacks remain commissioning dependencies with no invented default.

Annex §7 records dated primary standards references and per-rule provenance. STD-05 control principles are design sources; ISO references are verified edition/scope alignments pending licensed clause verification. AOS approval is not ISO conformance or certification. AOS-specific no-revival, uncertainty retention, agreed resident channels and acknowledged continuing duty are expressly distinguished from standard-derived principles.

6.6 Common research adoption

AOS-03-CON-008 references AOS-04 v0.7 §§3.1/5.1/6.6/10.8 (CON-009), AOS-02 v0.7 §6.6 (CON-007) and AOS-01 v0.7 §§6.6/10.8. 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. No new approved IF/REC identifier is created. AOS-02 §6.6 is the single proposed logical view definition; this component supplies the remit/finding semantics, 04 behaviour, 14 access/admission evidence, 03 permitted-use decisions, 05 observed enforcement, 13 tracked handoff and 30/01 empowered disposition/change. Profiles/agents → permitted 02 custody/component reviewers; decisions → exact finding/change follow-up. Register v0.5 §13 records exact producer/consumer adoption and logical supporting-view revision RSVIEW-0.1. Wire types/cardinalities/units, mappings and approved compatible schema manifests remain gated shared-schema work, not inferred from logical adoption.

Profile/run/finding/disposition states inherit AOS-04 §5.1; neither run completion, source verification nor proposal acceptance establishes approval/application/compliance. Existing staged acknowledgement, current checks, correction/revocation, recovery, privacy/licensing and source-lifecycle duties apply to raw and derived research.

6.7 AOS-30 decision-record participation - 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.

CON-001/007 establish acting capacity and permitted human review; neither a verified Chair identity nor processing permission turns draft approval into board approval. No executable schema change is made; the existing logical KX-06 v0.3 meaning is explicitly adopted. Existing REQ/VER identifiers and proposed/planned statuses are preserved.

7. Authority and decision boundaries

Within approved instruments, deterministic controls may validate identity/current roles, compare exact scope, apply current

purpose rules, issue bounded results and invalidate dependent permits. They cannot invent legal bases, approve their own exceptions, treat predicted welfare as emergency authority, reinterpret a constitutional prohibition, or decide incommensurable values.

The board determines the welfare/consent hierarchy with professional advice and defined thresholds, transparency duties and review cycle. Operational humans act only under the powers this confers. Neither board policy nor a human label makes otherwise impermissible processing lawful. If lawful basis and AOS principles conflict, the affected capability remains withheld pending authorised resolution; do not silently relax a governing RP principle.

Applicable prohibitions block the affected processing. Approved precedence may resolve policy conflict; unresolved conflict goes to empowered humans under DEC-044. Separately authorised internal escalation remains possible, with only permitted data and route. A lost data-use service does not grant emergency permission.

Resident-agreed communication channels, consent to an inference, authority to act for another person and legal processing basis are separate objects. An agreement to receive repair messages by email does not authorise health profiling or permit a private assistant transcript to enter the enterprise layer.

8. Reasoning principles applied

8.1 FP applicability

Table row 1
FP v4: 1 - Telos, purpose and function
Component treatment / limitation: Registered purposes relate to organisational commitments; operational usefulness cannot enlarge them. REQ-004/009/038

Table row 2
FP v4: 2 - Human Mode 2
Component treatment / limitation: Human welfare/privacy adjudication and challenged use. REQ-019/020; actual quality requires organisational review

Table row 3
FP v4: 3 - Architectural integrity
Component treatment / limitation: Independently enforced barriers, model/provider terms and permission controls. REQ-007/011/038/039/042

Table row 4
FP v4: 4 - Radical transparency
Component treatment / limitation: Meaningful disclosure, assurance provenance and reviewable restriction. REQ-025-028

Table row 5
FP v4: 5 - Structural imperfection
Component treatment / limitation: Unknown evidence/control failure/recovery designed explicitly. REQ-007/037; §11

Table row 6
FP v4: 6 - Epistemic humility
Component treatment / limitation: Unresolved identity/basis/assurance cannot be converted to permission. REQ-001/005/007/025

Table row 7
FP v4: 7 - No-exit obligation
Component treatment / limitation: Silence is not consent; accessible routes and proposed credible refusal. REQ-015/016/023; Q04

Table row 8
FP v4: 8 - Constitutional mediation

Component treatment / limitation: Welfare hierarchy and policy changes remain governed human decisions. REQ-020/038

Table row 9
FP v4: 9 - Compliance as consequence
Component treatment / limitation: Principle-first design followed by scope-specific legal validation. §§1/2/15; no current legal-conformance finding

Table row 10
FP v4: 10 - Complexity/emergence
Component treatment / limitation: Cross-layer joins and accumulated drift tested, including longitudinal review. REQ-010/013/035; §15

8.2 RP applicability

All nine domains have a component relationship. Domain 1 closes challenges/invalidation loops with named human accountability; domain 2 preserves Mode 2 and unobserved boardroom deliberation; domain 3 keeps shared controls distinct from the 1+5 intelligences and defines permitted handoff; domain 4 prevents data restrictions creating falsely complete analysis and leaves option-generation method to AOS-22; domain 5 makes unknown/withheld evidence legible; domain 6 governs welfare conflicts, equity, no-exit and provider values; domain 7 supplies reconstructable actual controls and uncertainty; domain 8 supplies explicit authority and protected required audiences; domain 9 supplies all four hard sensing/purpose principles in S02-05.

S04’s explicit consent/separate governance/necessity test is not weakened by this draft’s distinction between processing bases. S05’s consent-based expansion requirement is not quietly replaced with an employer’s asserted legitimate interest. If valid consent cannot be established, withhold the expansion and refer the conflict. Q04 concerns consequences of optional refusal, not permission to disregard S04/S05. S06 requires the board to decide the welfare hierarchy; DEC-051 approves how that becomes enforceable rather than deciding that all welfare overrides consent.

Net transparency is assessed against the preceding service’s explanations and ability to challenge. Redaction that conceals assurance weakness fails this assessment even if the resulting prose looks tidy. A required audience duty cannot be silently defeated by privacy settings; determine a lawful, appropriately scoped projection or escalate the conflict.

8.3 GT disposition - contribution, not claimed organisational pass

Table row 1
GT: M1.1 Strategic Coherence
AOS-03 contribution / assessment owner: Purpose-bound flows support GI coherence; strategy adequacy remains GI/board

Table row 2
GT: M1.2 Sensing Architecture
AOS-03 contribution / assessment owner: Explicit purpose/inference barriers and visible excluded sensing

Table row 3
GT: M1.3 Risk Intelligence
AOS-03 contribution / assessment owner: Misuse, stale permits and cross-domain inference monitored; risk synthesis AOS-23

Table row 4
GT: M1.4 Composition and Capability
AOS-03 contribution / assessment owner: Appropriate empowered human reviewers required; board capability AOS-12/30

Table row 5
GT: M1.5 Performance Legibility
AOS-03 contribution / assessment owner: Blocking/disclosure/rights outcomes visible without unapproved individual surveillance

Table row 6
GT: M1.6 Compliance Assurance
AOS-03 contribution / assessment owner: Verified legal mapping and enforcement evidence required; not established by this draft

Table row 7
GT: M1.7 Governance Documentation
AOS-03 contribution / assessment owner: Current approved bases/notices/policies and exact revisions

Table row 8
GT: M1.8 Accountability Architecture
AOS-03 contribution / assessment owner: Human ownership and decision powers distinct from delivery

Table row 9
GT: M1.9 Value for Money
AOS-03 contribution / assessment owner: Assess control burden and less intrusive alternatives; financial value judgement outside AOS-03

Table row 10
GT: M1.10 Human-AI Interaction Norms
AOS-03 contribution / assessment owner: Accessible consent/challenge, private boundary, no deliberation capture

Table row 11
GT: M1.11 Learning Metabolism
AOS-03 contribution / assessment owner: Learn from permitted outcome evidence; learning cannot enlarge purpose

Table row 12
GT: M1.12 Continuous Self-Assessment
AOS-03 contribution / assessment owner: Monitor permissions/exception drift; independent adequacy assessment remains necessary

Table row 13
GT: M1.13 Emergent System Behaviour
AOS-03 contribution / assessment owner: Joined data, derived artefacts, retries and multi-agent boundaries tested

Table row 14
GT: M1.14 Golden Thread Integrity
AOS-03 contribution / assessment owner: Permitted evidence/review access without suppressible material findings; safety evidence owners elsewhere

Table row 15
GT: M2.1 Values Architecture
AOS-03 contribution / assessment owner: Structural choice, inference and disclosure limits

Table row 16
GT: M2.2 Coherence Under Pressure
AOS-03 contribution / assessment owner: Welfare/outage tests prevent convenience-based override

Table row 17
GT: M2.3 Trade-off Capacity
AOS-03 contribution / assessment owner: Human welfare/privacy conflict decisions; no algorithmic balancing substitutes

Table row 18
GT: M2.4 Epistemic Brake
AOS-03 contribution / assessment owner: Uncertain basis or identity stops dependent use and permits authorised referral

Table row 19
GT: M2.5 Directorial Independence
AOS-03 contribution / assessment owner: Unobserved deliberation, approved evidence access; board culture assessed elsewhere

Table row 20
GT: M2.6 Social Legitimacy
AOS-03 contribution / assessment owner: Meaningful resident control/challenge; lived legitimacy requires human assessment

Table row 21
GT: M2.7 No-Exit Obligation
AOS-03 contribution / assessment owner: Consent not inferred from passivity; proposed refusal protection

Table row 22
GT: M2.8 Radical Transparency
AOS-03 contribution / assessment owner: Assurance-chain legibility and reviewable disclosure restrictions

Table row 23
GT: M2.9 Moral Drift Detection
AOS-03 contribution / assessment owner: Longitudinal expansion/exception/provider-use review

Table row 24
GT: M2.10 Purpose Stability
AOS-03 contribution / assessment owner: Current purpose register and protected amendments; constitutional owner AOS-01/board

Table row 25
GT: M2.11 Murmuration Capacity
AOS-03 contribution / assessment owner: Deliberative privacy enables distributed judgement; collective cognition not verified here

Table row 26
GT: M2.12 Constitutional Authority
AOS-03 contribution / assessment owner: Board-defined hierarchy with bounded operational powers

Table row 27
GT: M2.13 AI Constitutional Framework Governance
AOS-03 contribution / assessment owner: Provider processing/embedded-value implications assessed with AOS-04/05/25; board determination outstanding

Table row 28
GT: M2.14 Purpose-Led Design
AOS-03 contribution / assessment owner: Principles precede legal conformance mapping and process tests

Table row 29
GT: M2.15 Telos/Function Distinction
AOS-03 contribution / assessment owner: Permission rationale tied to approved purpose, never model optimisation alone

The Source Traceability Matrix still needs exact component-level entries and source fingerprints. This applicability assessment does not declare every individual RP principle fully allocated or every GT test satisfied.

9. Data, privacy and disclosure

Collect only information needed by approved identity, use, consent or review purposes. Minimise identity documents and sensitive verification evidence; storing a complete document is not automatically necessary to record a verification result. Authentication secrets and protected tokens must not appear in explanation or general audit payloads. Exact security classification and permitted evidence projection are commissioned under CON-001/005.

An actor may be a resident, worker, director, representative, service or deployed agent. A human principal, authenticated actor, model/deployment provenance and accountable human role remain distinct. Source-entity matching under AOS-02 DEC-045

does not by itself authenticate a person or establish their legal representation.

Consent records distinguish agreement to a communication channel, participation in an optional service, specific inference scope and representation. A communication preference does not become an Article 6 finding. Legal categories and extra safeguards are assessed explicitly, including sensitive inferences and criminal-offence information; not all sensitive-in-context information is automatically a statutory special category, and absence of that category is not blanket permission.

Derived summaries, embeddings, caches, exports, logs and model/provider processing remain in the data-flow assessment. Aggregation or pseudonymisation does not automatically remove restrictions or establish anonymity. Claimed anonymisation needs approved re-identification risk assessment before relying on that claim.

Assurance transparency retains a governed account of source origin, supporting validation/evidence, responsible assurance role, relevant method/version/time and limitations. Affected people need enough permitted information to interrogate a significant decision. They do not automatically gain unrestricted access to another resident's, employee's or confidential source's details. DEC-053 approves reviewable, least-restrictive meaningful disclosure. Technical source references never confer access by themselves.

Approved record-class policies govern lifecycle across operational data, assurance records, consent and audit. Legal hold/retention conflict is assessed by empowered owners; no universal immutable personal-data archive or automatic deletion entitlement is assumed. Minimal deletion evidence needs its own permitted retention basis and cannot reproduce the disposed content.

10. Behaviour and workflows

10.1 Ordinary permitted operation

Trigger → scoped actor/capacity evidence → declared data/operation/purpose/basis → independent permitted-use assessment → organisational authority where action requires it → last-enforceable currentness check → bounded processing/disclosure → actual effect and limitations recorded → permitted feedback/review.

If a purpose, actor, payload, audience or location changes, bind a revised request. A permit for a harmless retrieval does not cover an external disclosure or newly proposed inference. A denied/unresolved use withholds only dependent processing; separately permitted work is assessed on its own scope.

10.2 Resident choice and withdrawal

Accessible notice and actual expression → scoped consent/notice revision → permitted processing → later refusal/withdrawal/expiry → identify dependent pending operations and derived artefacts → invalidate at commissioned checkpoints → authorised restriction/deletion/retention assessment → downstream result/limitation → person receives permitted explanation and human review route through agreed channels.

Unreachable downstream copy and already delivered information remain visible limitations. A withdrawal recorded during control outage does not vanish on restart; queued use waits for reconciliation. Do not replace the withdrawn consent with a newly asserted basis merely to continue the same unwanted optional feature.

10.3 Welfare concern with contested permission

Permitted detection/evidence → classification with explicit uncertainty → separately authorised minimal internal referral → empowered human acknowledgement → applicable board hierarchy/threshold and legal basis checked → authorised bounded action or recorded withholding/fallback → permitted resident explanation → consequence/follow-up reviewed.

This pathway neither authorises generating prohibited behavioural inference nor permits automatic external contact. DEC-051 approves a tightly defined acute-risk protocol; exact thresholds/roles/purposes and channel exceptions remain decisions. Human responsibility persists during technical outage, using separately authorised arrangements.

10.4 Contrasting adequacy tests

Table row 1
Context: Asset environmental sensor
Boundary exposed: Damp/temperature observation can reveal occupancy habits
Expected general treatment: Separate asset purpose from explicit behavioural inference; no byproduct permission

Table row 2
Context: Staff development conversation
Boundary exposed: Learning support could become disciplinary evidence
Expected general treatment: Declared purpose, confidentiality and consent-based expansion checked; disputed new use withheld

Table row 3
Context: Resident private assistant
Boundary exposed: Drafting a complaint can reveal distress/confidential information
Expected general treatment: DEC-050 private-by-default direction; resident chooses scoped sharing; defined exceptions only

Table row 4
Context: Governance post-meeting record
Boundary exposed: Capture could slide into live boardroom observation
Expected general treatment: Authorised approved debrief record only; live observation prohibited even with claimed consent

Table row 5
Context: Cross-organisation service/provider
Boundary exposed: Authenticated counterparty could seek unrelated data/model training
Expected general treatment: Separate organisation, recipient, purpose, location and onward-use checks

Table row 6
Context: Repair resident notification
Boundary exposed: Valid task authority could be mistaken for permission to select any channel
Expected general treatment: Current resident agreement controls channel(s); unknown delivery not closure

Table row 7
Context: Allocation or employment analysis
Boundary exposed: Human presence could conceal automated adjudication
Expected general treatment: Use/basis/sensitive-category assessment and meaningful empowered review; Mode 2 remains human

The final scenario is a general test, not an assertion that any particular allocation/employment decision has been classified in the organisational Schedule. These contexts must be refined with domain owners before executed acceptance.

10.6 Combined control coordination

For effects, activation, material changes, concurrent reservations, withholding and resumption, apply the common protocol in Control Coordination v0.1 §§3-8. Denial or missing current controls/accounting withholds dependent work; actual application and responsibility are separately evidenced. Timeouts/cancellations do not establish no prior effect or release uncertain capacity. Numeric/profile/role selections remain commissioning dependencies.

10.7 Protected reporting and controlled recovery

Apply Protected Reporting and Recovery v0.1 §§3-4: withhold dependent effects, attempt only permitted reporting, retain original tracking owner until accepted handoff and preserve unresolved failure duties. Restore in isolation; prove required authoritative current state and complete material changes, apply current dispositions and reconcile effects/reservations. Only scoped accepted release can restore operation, followed by fresh current CHECK and capacity admission; no automatic queue replay. Unaffected release requires evidence of no material dependency, not mere absence of a known incident.

10.8 External-research workflow and exceptions

Approved profile/exact draft and governing baseline → permitted AOS-14 retrieval → source/admission/assurance/status evidence → specialist component relevance assessment → common run and finding/coverage record → permitted tracked review through 13/30 → empowered disposition → separately controlled change under 01 → required evaluation/compatible application and outcome follow-up. Shared retrieval retains each component's assessment, owner, deadlines and disposition. A stale baseline or corrected/restricted source prompts recorded reassessment; preserve the original historical assessment, and propagate material impact under existing CHG/lifecycle rules.

Blocked access, missing baseline, partial/failed coverage, unavailable reviewer or failed delivery produces an explicit owned exception. No silent substitution of sources, route, processing basis or reviewer is permitted. Ordinary quiet reporting cannot conceal missing coverage records; if the platform cannot retain a run record, expose that operational gap. Urgent operational/legal/safety concerns follow the separately authorised protected route without waiting for amendment; receipt is not human acceptance or completion.

11. Failure, escalation and recovery

Table row 1
Failure: Identity/representation unavailable
Required handling / separately authorised fallback: Protected access withheld; approved public or assisted route may continue within its independent scope

Table row 2
Failure: Basis/consent evidence missing or contradictory
Required handling / separately authorised fallback: Unresolved; do not treat source "consent obtained" as verified scope; human route with permitted metadata

Table row 3
Failure: Use control unavailable
Required handling / separately authorised fallback: Dependent processing withheld; no fail-open cache or inferred permit; authorised human arrangements need independent evidence

Table row 4
Failure: Withdrawal propagation delayed
Required handling / separately authorised fallback: Pending dependent uses invalidated/rechecked under race profile; timings/copies not reached recorded; incidents assessed

Table row 5
Failure: Unexpected sensitive inference
Required handling / separately authorised fallback: Stop affected unapproved inference/disclosure; minimise authorised containment and refer design/policy gap

Table row 6
Failure: Required disclosure conflicts with privacy
Required handling / separately authorised fallback: Preserve finding/duty; seek approved meaningful projection or empowered resolution,

not administrator suppression

Table row 7
Failure: External effect partial/unknown
Required handling / separately authorised fallback: Keep indeterminate; authorised status/reconciliation before consequential repeat

Table row 8
Failure: Deletion incomplete / backup restored
Required handling / separately authorised fallback: Track outstanding copies; prevent reactivation/reuse, apply approved backup-expiry/restoration rules; do not claim full deletion

Table row 9
Failure: Private transcript shared accidentally
Required handling / separately authorised fallback: Contain affected access, preserve permitted incident evidence, authorised remedial notification/review; do not erase event history

Table row 10
Failure: Prompt injection or administrator scope expansion
Required handling / separately authorised fallback: Untrusted instruction supplies no permission; reject unauthorised rule change and record attempted bypass

Table row 11
Failure: Human route unacknowledged
Required handling / separately authorised fallback: Visible pending state, commissioned cover/escalation windows; no assumption that sending discharged responsibility

Recovery checks current instruments/roles/consent and invalidation evidence before resuming affected work. A fallback is a governed operating arrangement, not a general administrator override. Its data use, action power and audit evidence must all be established.

12. Evidence, provenance and audit

Record trigger and request revision → actor/acting capacity and assurance → proposed data/operation/purpose → exact instruments/basis/consent states → evaluator/rules and recorded evidence → determination/conditions/explanation → actual enforcement boundary and timing → processing/disclosure consequence → intervention/challenge → outcome and permitted feedback.

The resulting chain links AOS-02 fact-assurance provenance: source origin is separate from the evidence or validation providing assurance for a fact. An authorised reviewer can inspect the permitted supporting record; an affected-person projection preserves material assurance scope/limitations even when protected source details are withheld under policy.

“Reasoning” records applied rules, cited evidence, material model output and approved human rationale. Private chain-of-thought is not required; a later generated explanation is not proof of the original check. Evidence of a configuration is not evidence that the actual request followed it. Lost control evidence blocks a conformance claim and, where required for consequential processing, the dependent operation.

Operational metrics include permitted/denied/unresolved uses, actual invalidation delays, inaccessible choice/rights routes, disputed representation, new inferences, repeated exception use and unresolved required-audience conflicts. Classification changes and near-misses are reviewed longitudinally under approved, themselves purpose-limited oversight.

13. Security and operational requirements

Authentication, secrets handling, isolation, enforcement, cache control and restored-copy barriers need AOS-05 mechanisms and threat evidence. The requesting model cannot be the sole enforcer of its own access. A prompt prohibition is insufficient for data already exposed to an unauthorised model/provider.

Policy evaluation uses approved interpretable rules and explicit outcome semantics. Probabilistic identity/fraud/anonymisation/sensitivity assessment is advisory within commissioned conditions; it does not establish legal basis or settle Mode 2. Each such use needs dataset provenance, representative evaluation conditions, false-accept/false-reject and exclusion risk measures, approved thresholds, limitations, human challenge and model-change review. Thresholds/availability/latency/expiry are deliberately unresolved; no numerical default is authorised.

Accessible service routes cover assistive technologies, human support, representation and alternatives to digital-only identity proof. Assisted service must preserve assurance proportional to the operation. DEC-049 approves this direction; detailed methods require resident/workforce testing.

No deployment claim rests on source/schema checks alone. Threat assessment covers credential theft, cross-tenant access, confused-deputy service calls, forged consent, coercive choice, purpose laundering, data reconstruction through joins, malicious content, provider retention, backup resurrection, covert suppression and control outage.

14. Invariants

Table row 1
INV: 001
Invariant / binding REQ under the approved direction: Authentication and organisational authority cannot substitute for an exact permitted-use result. 004/006/007
Planned VER: 003/004

Table row 2
INV: 002
Invariant / binding REQ under the approved direction: Source admission or transformation cannot create a new purpose permission. 009/010/013
Planned VER: 006/007/009

Table row 3
INV: 003
Invariant / binding REQ under the approved direction: Asset observation cannot silently become behavioural monitoring. 011/012
Planned VER: 007/008

Table row 4
INV: 004
Invariant / binding REQ under the approved direction: Silence and continued tenancy cannot create consent. 014/015
Planned VER: 010

Table row 5
INV: 005
Invariant / binding REQ under the approved direction: A withdrawn/expired consent cannot support dependent pending use beyond the approved boundary. 008/017
Planned VER: 005/012

Table row 6
INV: 006
Invariant / binding REQ under the approved direction: A model-classified welfare concern cannot create exception powers. 019/020
Planned VER: 014

Table row 7
INV: 007

Invariant / binding REQ under the approved direction: A transparency restriction cannot rewrite evidence meaning or quietly disable protected audiences. 025-029
Planned VER: 019/020

Table row 8
INV: 008
Invariant / binding REQ under the approved direction: Deletion/recovery cannot leave an unapproved reusable shadow copy. 030/031
Planned VER: 013/021

Table row 9
INV: 009
Invariant / binding REQ under the approved direction: Instance isolation and boardroom exclusion cannot be waived by local access settings. 033/042
Planned VER: 022/025

These are proposed invariants linked to explicit proposed REQs. There is no binding component-conformance claim until the relevant baseline is adopted and tested.

15. Conformance and acceptance

15.1 Conformance claims

Table row 1
CR: CR-001
Claim scope / required evidence: Actor/capacity assurance and accessible routes conform to the approved risk profile; VER-001/002/011/022

Table row 2
CR: CR-002
Claim scope / required evidence: Exact independent use controls operate at every relevant boundary; VER-003-009/025

Table row 3
CR: CR-003
Claim scope / required evidence: Consent/withdrawal and credible optional choice work end to end; VER-010-013/017, Q04 decision

Table row 4
CR: CR-004
Claim scope / required evidence: Welfare, private-space and disclosure conflicts remain governed and human reviewable; VER-014-016/019/020, Q02/03/05 decisions

Table row 5
CR: CR-005
Claim scope / required evidence: Locations/lifecycle/provider use and recovery respect policy; VER-013/018/021-024

Table row 6
CR: CR-006
Claim scope / required evidence: Longitudinal joined-data/exception drift and cross-component adequacy are assessed; combined VER-006-009/014/020/023 plus human review

Explicit conformance navigation - 29 October 2026

This index completes the documentary navigation from every retained kernel requirement to its proposed conformance criterion and its existing planned case(s). It neither adds a requirement nor claims that a case was executed or that its coverage is adequate. CR-EXCHANGE, CR-COORDINATION, CR-CONTINUITY and CR-RESEARCH below are derived grouping labels local to this component, not new system obligations. Original numbered CR claims remain applicable with their stated scope and limitations. Exact requirement text in §4.3 and case definitions in §15 remain authoritative.

Table row 1
Derived criterion: CR-EXCHANGE
Existing obligation family / derivation: Common definition/revision, compatibility, assurance and staged evidence adoption; existing §19.2 allocation.

Table row 2
Derived criterion: CR-COORDINATION
Existing obligation family / derivation: Current checkpoint, compatible activation, change propagation, cumulative accounting and owned withholding/resumption; existing §19.3 allocation.

Table row 3
Derived criterion: CR-CONTINUITY
Existing obligation family / derivation: Protected reporting, accepted human duty and current-state recovery/release; existing §19.4 allocation.

Table row 4
Derived criterion: CR-RESEARCH
Existing obligation family / derivation: Controlled research, evidence/coverage, human review and separate amendment authority; existing research requirements and their allocation.

CR-BOOTSTRAP: the checking service’s own minimum metadata permission is independently established, bounded and current under DEC-100; evidence is assessed through REQ-069 and its planned case.

Table row 1
Requirement: AOS-03-REQ-001
Proposed criterion (AOS-03 prefix): CR-001
Existing planned case(s): AOS-03-VER-001
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 2
Requirement: AOS-03-REQ-002
Proposed criterion (AOS-03 prefix): CR-001
Existing planned case(s): AOS-03-VER-002
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 3
Requirement: AOS-03-REQ-003
Proposed criterion (AOS-03 prefix): CR-001
Existing planned case(s): AOS-03-VER-002
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 4
Requirement: AOS-03-REQ-004
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-003
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 5
Requirement: AOS-03-REQ-005
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-003
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 6
Requirement: AOS-03-REQ-006
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-004
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 7
Requirement: AOS-03-REQ-007
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-004, AOS-03-VER-005
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 8
Requirement: AOS-03-REQ-008
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-005
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 9
Requirement: AOS-03-REQ-009
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-006
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 10
Requirement: AOS-03-REQ-010
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-006, AOS-03-VER-007
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 11
Requirement: AOS-03-REQ-011
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-007
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 12
Requirement: AOS-03-REQ-012
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-008
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 13
Requirement: AOS-03-REQ-013

Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-009
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 14
Requirement: AOS-03-REQ-014
Proposed criterion (AOS-03 prefix): CR-003
Existing planned case(s): AOS-03-VER-010
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 15
Requirement: AOS-03-REQ-015
Proposed criterion (AOS-03 prefix): CR-003
Existing planned case(s): AOS-03-VER-010
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 16
Requirement: AOS-03-REQ-016
Proposed criterion (AOS-03 prefix): CR-001
Existing planned case(s): AOS-03-VER-011
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 17
Requirement: AOS-03-REQ-017
Proposed criterion (AOS-03 prefix): CR-003
Existing planned case(s): AOS-03-VER-012
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 18
Requirement: AOS-03-REQ-018
Proposed criterion (AOS-03 prefix): CR-003
Existing planned case(s): AOS-03-VER-012, AOS-03-VER-013
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 19
Requirement: AOS-03-REQ-019
Proposed criterion (AOS-03 prefix): CR-004
Existing planned case(s): AOS-03-VER-014
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 20
Requirement: AOS-03-REQ-020
Proposed criterion (AOS-03 prefix): CR-004
Existing planned case(s): AOS-03-VER-014
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 21
Requirement: AOS-03-REQ-021
Proposed criterion (AOS-03 prefix): CR-004
Existing planned case(s): AOS-03-VER-015

Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 22
Requirement: AOS-03-REQ-022
Proposed criterion (AOS-03 prefix): CR-004
Existing planned case(s): AOS-03-VER-016
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 23
Requirement: AOS-03-REQ-023
Proposed criterion (AOS-03 prefix): CR-003
Existing planned case(s): AOS-03-VER-017
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 24
Requirement: AOS-03-REQ-024
Proposed criterion (AOS-03 prefix): CR-005
Existing planned case(s): AOS-03-VER-018
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 25
Requirement: AOS-03-REQ-025
Proposed criterion (AOS-03 prefix): CR-004
Existing planned case(s): AOS-03-VER-019
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 26
Requirement: AOS-03-REQ-026
Proposed criterion (AOS-03 prefix): CR-004
Existing planned case(s): AOS-03-VER-019
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 27
Requirement: AOS-03-REQ-027
Proposed criterion (AOS-03 prefix): CR-004
Existing planned case(s): AOS-03-VER-019, AOS-03-VER-020
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 28
Requirement: AOS-03-REQ-028
Proposed criterion (AOS-03 prefix): CR-004
Existing planned case(s): AOS-03-VER-020
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 29
Requirement: AOS-03-REQ-029
Proposed criterion (AOS-03 prefix): CR-004
Existing planned case(s): AOS-03-VER-020
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 30
Requirement: AOS-03-REQ-030
Proposed criterion (AOS-03 prefix): CR-005
Existing planned case(s): AOS-03-VER-013
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 31
Requirement: AOS-03-REQ-031
Proposed criterion (AOS-03 prefix): CR-005
Existing planned case(s): AOS-03-VER-013, AOS-03-VER-021
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 32
Requirement: AOS-03-REQ-032
Proposed criterion (AOS-03 prefix): CR-005
Existing planned case(s): AOS-03-VER-018, AOS-03-VER-021
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 33
Requirement: AOS-03-REQ-033
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-022
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 34
Requirement: AOS-03-REQ-034
Proposed criterion (AOS-03 prefix): CR-001
Existing planned case(s): AOS-03-VER-011
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 35
Requirement: AOS-03-REQ-035
Proposed criterion (AOS-03 prefix): CR-005
Existing planned case(s): AOS-03-VER-023
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 36
Requirement: AOS-03-REQ-036
Proposed criterion (AOS-03 prefix): CR-005
Existing planned case(s): AOS-03-VER-023
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 37
Requirement: AOS-03-REQ-037
Proposed criterion (AOS-03 prefix): CR-005
Existing planned case(s): AOS-03-VER-024
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 38

Requirement: AOS-03-REQ-038
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-025
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 39
Requirement: AOS-03-REQ-039
Proposed criterion (AOS-03 prefix): CR-005
Existing planned case(s): AOS-03-VER-009, AOS-03-VER-018
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 40
Requirement: AOS-03-REQ-040
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-003, AOS-03-VER-005
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 41
Requirement: AOS-03-REQ-041
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-008, AOS-03-VER-009
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 42
Requirement: AOS-03-REQ-042
Proposed criterion (AOS-03 prefix): CR-002
Existing planned case(s): AOS-03-VER-025
Derivation / applicability: Explicit allocation to the existing numbered claim in §15.1; assess the unchanged requirement through its linked case(s).

Table row 43
Requirement: AOS-03-REQ-043
Proposed criterion (AOS-03 prefix): CR-EXCHANGE
Existing planned case(s): AOS-03-VER-026, AOS-03-VER-030
Derivation / applicability: Existing common exchange and assurance/evidence obligation.

Table row 44
Requirement: AOS-03-REQ-044
Proposed criterion (AOS-03 prefix): CR-EXCHANGE
Existing planned case(s): AOS-03-VER-026
Derivation / applicability: Existing common exchange and assurance/evidence obligation.

Table row 45
Requirement: AOS-03-REQ-045
Proposed criterion (AOS-03 prefix): CR-EXCHANGE
Existing planned case(s): AOS-03-VER-027, AOS-03-VER-031
Derivation / applicability: Existing common exchange and assurance/evidence obligation.

Table row 46
Requirement: AOS-03-REQ-046
Proposed criterion (AOS-03 prefix): CR-EXCHANGE
Existing planned case(s): AOS-03-VER-029
Derivation / applicability: Existing common exchange and assurance/evidence obligation.

Table row 47
Requirement: AOS-03-REQ-047
Proposed criterion (AOS-03 prefix): CR-EXCHANGE
Existing planned case(s): AOS-03-VER-028
Derivation / applicability: Existing common exchange and assurance/evidence obligation.

Table row 48
Requirement: AOS-03-REQ-048
Proposed criterion (AOS-03 prefix): CR-COORDINATION
Existing planned case(s): AOS-03-VER-032, AOS-03-VER-033
Derivation / applicability: Existing coordinated current-control/effect/duty obligation.

Table row 49
Requirement: AOS-03-REQ-049
Proposed criterion (AOS-03 prefix): CR-COORDINATION
Existing planned case(s): AOS-03-VER-033
Derivation / applicability: Existing coordinated current-control/effect/duty obligation.

Table row 50
Requirement: AOS-03-REQ-050
Proposed criterion (AOS-03 prefix): CR-COORDINATION
Existing planned case(s): AOS-03-VER-034, AOS-03-VER-035
Derivation / applicability: Existing coordinated current-control/effect/duty obligation.

Table row 51
Requirement: AOS-03-REQ-051
Proposed criterion (AOS-03 prefix): CR-COORDINATION
Existing planned case(s): AOS-03-VER-036, AOS-03-VER-037
Derivation / applicability: Existing coordinated current-control/effect/duty obligation.

Table row 52
Requirement: AOS-03-REQ-052
Proposed criterion (AOS-03 prefix): CR-COORDINATION
Existing planned case(s): AOS-03-VER-036
Derivation / applicability: Existing coordinated current-control/effect/duty obligation.

Table row 53
Requirement: AOS-03-REQ-053
Proposed criterion (AOS-03 prefix): CR-COORDINATION
Existing planned case(s): AOS-03-VER-037
Derivation / applicability: Existing coordinated current-control/effect/duty obligation.

Table row 54
Requirement: AOS-03-REQ-054
Proposed criterion (AOS-03 prefix): CR-COORDINATION
Existing planned case(s): AOS-03-VER-038, AOS-03-VER-039
Derivation / applicability: Existing coordinated current-control/effect/duty obligation.

Table row 55
Requirement: AOS-03-REQ-055
Proposed criterion (AOS-03 prefix): CR-COORDINATION
Existing planned case(s): AOS-03-VER-035, AOS-03-VER-039
Derivation / applicability: Existing coordinated current-control/effect/duty obligation.

Table row 56
Requirement: AOS-03-REQ-056
Proposed criterion (AOS-03 prefix): CR-CONTINUITY
Existing planned case(s): AOS-03-VER-040

Derivation / applicability: Existing protected-reporting, handoff or recovery obligation.

Table row 57
Requirement: AOS-03-REQ-057
Proposed criterion (AOS-03 prefix): CR-CONTINUITY
Existing planned case(s): AOS-03-VER-041
Derivation / applicability: Existing protected-reporting, handoff or recovery obligation.

Table row 58
Requirement: AOS-03-REQ-058
Proposed criterion (AOS-03 prefix): CR-CONTINUITY
Existing planned case(s): AOS-03-VER-042
Derivation / applicability: Existing protected-reporting, handoff or recovery obligation.

Table row 59
Requirement: AOS-03-REQ-059
Proposed criterion (AOS-03 prefix): CR-CONTINUITY
Existing planned case(s): AOS-03-VER-043
Derivation / applicability: Existing protected-reporting, handoff or recovery obligation.

Table row 60
Requirement: AOS-03-REQ-060
Proposed criterion (AOS-03 prefix): CR-CONTINUITY
Existing planned case(s): AOS-03-VER-044
Derivation / applicability: Existing protected-reporting, handoff or recovery obligation.

Table row 61
Requirement: AOS-03-REQ-061
Proposed criterion (AOS-03 prefix): CR-CONTINUITY
Existing planned case(s): AOS-03-VER-045
Derivation / applicability: Existing protected-reporting, handoff or recovery obligation.

Table row 62
Requirement: AOS-03-REQ-062
Proposed criterion (AOS-03 prefix): CR-RESEARCH
Existing planned case(s): AOS-03-VER-046
Derivation / applicability: Existing research obligation; assessment remains distinct from amendment/activation.

Table row 63
Requirement: AOS-03-REQ-063
Proposed criterion (AOS-03 prefix): CR-RESEARCH
Existing planned case(s): AOS-03-VER-047
Derivation / applicability: Existing research obligation; assessment remains distinct from amendment/activation.

Table row 64
Requirement: AOS-03-REQ-064
Proposed criterion (AOS-03 prefix): CR-RESEARCH
Existing planned case(s): AOS-03-VER-048
Derivation / applicability: Existing research obligation; assessment remains distinct from amendment/activation.

Table row 65
Requirement: AOS-03-REQ-065
Proposed criterion (AOS-03 prefix): CR-RESEARCH
Existing planned case(s): AOS-03-VER-049
Derivation / applicability: Existing research obligation; assessment remains distinct from amendment/activation.

Table row 66
Requirement: AOS-03-REQ-066

Proposed criterion (AOS-03 prefix): CR-RESEARCH
Existing planned case(s): AOS-03-VER-050
Derivation / applicability: Existing research obligation; assessment remains distinct from amendment/activation.

Table row 67
Requirement: AOS-03-REQ-067
Proposed criterion (AOS-03 prefix): CR-RESEARCH
Existing planned case(s): AOS-03-VER-051
Derivation / applicability: Existing research obligation; assessment remains distinct from amendment/activation.

Table row 68
Requirement: AOS-03-REQ-068
Proposed criterion (AOS-03 prefix): CR-RESEARCH
Existing planned case(s): AOS-03-VER-046
Derivation / applicability: Existing research obligation; assessment remains distinct from amendment/activation.

Table row 69
Requirement: AOS-03-REQ-069
Proposed criterion (AOS-03 prefix): CR-BOOTSTRAP
Existing planned case(s): AOS-03-VER-052
Derivation / applicability: DEC-100 approved direction; independently verifiable advance permission for the checking service itself.

All verification cases below are planned, unexecuted. Each inherits method test plus document/human review as appropriate; required configuration is an approved test-only profile fixing the open parameters, with synthetic data and exact component/contract versions. A missing Q decision or profile blocks a dependent pass claim. Steps are inject the stated fixture, exercise the relevant boundary/recovery and compare actual trace to expected behaviour. Retain inputs, versions, observed timestamps/result/effect, explanation and reviewer findings; no production personal data is required.

Assessors: implementation/security testers for enforceability; empowered privacy/governance/domain reviewers for basis and semantic adequacy; resident/workforce accessibility participants for usable choice. Independent project-review appointment remains deferred. Executed results require a separate dated record naming assessors, versions, actual evidence and deviations.

Table row 1
VER: 001
REQ: 001
Fixture / precondition: Low-risk public query versus protected resident disclosure; stolen or insufficient credential
Expected result / acceptance: Apply distinct approved assurance requirements; protected data withheld without excluding independently permitted public/assisted service.

Table row 2
VER: 002
REQ: 002/003
Fixture / precondition: Same address, different resident; employee role expired; agent claims human principal; representative scope limited
Expected result / acceptance: No inferred household or role rights; require exact capacity/representation evidence; changed/expired capacity blocks dependent use.

Table row 3
VER: 003
REQ: 004/005/040
Fixture / precondition: Same data used for different operation/purpose; missing basis; narrowed request
Expected result / acceptance: Results bind exact evaluated revision and basis; narrow scope is separately checked; complete actual determination trace.

Table row 4
VER: 004
REQ: 006/007

Fixture / precondition: Authority allow with use deny, then use permit with authority deny; control outage
Expected result / acceptance: Neither favourable result substitutes; affected operation withheld; separately authorised route remains available.

Table row 5
VER: 005
REQ: 007/008/040
Fixture / precondition: Permit becomes stale immediately before processing; delayed invalidation; cached permit; restart
Expected result / acceptance: Approved checkpoint/race profile enforced; out-of-boundary effects visible, no instantaneous-cancellation claim.

Table row 6
VER: 006
REQ: 009/010
Fixture / precondition: Repair evidence received by People Intelligence for employee surveillance; summaries, aggregates, embeddings/search indexes, joined views and exports; vary source restrictions, intended purpose and lineage completeness.
Expected result / acceptance: Receiving purpose independently assessed against every applicable source restriction; incompatible purposes or insufficient lineage/use evidence withhold the affected use and create accountable review. Approved original use assessed separately; transformation supplies no permission. A different treatment requires evidence of existing governing authorisation. Planned, not executed.

Table row 7
VER: 007
REQ: 010/011
Fixture / precondition: Environmental sensor pipeline, cache, storage, restored index and joined sources can expose occupancy routines or other additional sensitive information; withdraw relevant permission and include an unreachable external copy.
Expected result / acceptance: Architectural separation demonstrated across collection/processing/storage/output; additional sensitive information from combination is assessed, unauthorised inference/use withheld, and controlled dependent copies respect current restrictions. Unreachable copies/completed disclosure remain explicit limitations with accountable handling. REQ-012 conditions remain unchanged; no new inference exception or recall guarantee. Planned, not executed.

Table row 8
VER: 008
REQ: 012/041
Fixture / precondition: Proposed energy-poverty or health inference without necessity, explicit consent, separate governance or current review
Expected result / acceptance: Each missing prerequisite blocks the inference; sensitive-category assessment/evidence applies; confidence does not cure missing permission.

Table row 9
VER: 009
REQ: 013/039/041
Fixture / precondition: Workforce learning data reused for assessment; resident service data proposed for provider training
Expected result / acceptance: No inherited or convenient new basis; consent-based expansion and separately approved training arrangements required; invalid consent blocks use.

Table row 10
VER: 010
REQ: 014/015
Fixture / precondition: Unanswered notice, low complaint volume, continued tenancy, generic source “consent obtained”
Expected result / acceptance: No consent manufactured; actual scoped expression/notice evidence required; refusal/unknown kept distinct.

Table row 11
VER: 011
REQ: 016/034
Fixture / precondition: Person cannot use digital route; voice/assisted withdrawal; representative rights challenge; no human acknowledgement

Expected result / acceptance: Usable verified alternatives and tracked human ownership/disposition; sending alone not completion; open accessibility findings retained.

Table row 12
VER: 012
REQ: 017/018
Fixture / precondition: Consent withdrawn/expired with queued inference, disclosure, derived cache and independently retained record
Expected result / acceptance: Dependent uses stop under profile; independent retention assessed separately; no silent basis switch or universal deletion.

Table row 13
VER: 013
REQ: 018/030/031
Fixture / precondition: Retention duty conflicts with deletion request; disposed content remains in export or explanatory log
Expected result / acceptance: Empowered conflict review; only approved custody/disposition; no hidden retained content or unapproved new use.

Table row 14
VER: 014
REQ: 019/020
Fixture / precondition: Potential acute welfare concern, uncertain threshold, no exception powers, control outage; then approved protocol fixture
Expected result / acceptance: No self-created override; authorised minimal referral and accountable human ownership; adopted protocol applies exact limits, basis and follow-up.

Table row 15
VER: 015
REQ: 021
Fixture / precondition: Resident has email/telephone agreement; system chooses unagreed SMS; agreement changed mid-queue
Expected result / acceptance: Only current agreed channel(s) for scoped communication used; failed contact follows authorised escalation without invented substitute.

Table row 16
VER: 016
REQ: 022
Fixture / precondition: Resident drafts complaint privately; staff seek whole transcript; resident selects one item to share
Expected result / acceptance: Under DEC-050, private content remains outside enterprise access; scoped sharing and explicitly governed exception only.

Table row 17
VER: 017
REQ: 023
Fixture / precondition: Optional analytics refused; employee declines learning-data expansion; service/job score changed because of refusal
Expected result / acceptance: Under DEC-052, no refusal-derived penalty; genuinely required core processing distinguished with approved explanation.

Table row 18
VER: 018
REQ: 024/032/039
Fixture / precondition: External provider changed; overseas support added; new recipient/onward use or provider training
Expected result / acceptance: Dependent new arrangement withheld pending exact assessment/approval; no UK-only or overseas-allowed assumption.

Table row 19
VER: 019
REQ: 025/026/027
Fixture / precondition: Significant decision rests on stale/limited assurance; source detail protected; generated explanation proposes

certainty
Expected result / acceptance: Permitted explanation preserves material basis, validation/assurance scope, uncertainty and human review; no misleading redaction.

Table row 20
VER: 020
REQ: 027/028/029
Fixture / precondition: Privacy setting hides protected finding; administrative change removes audience; legitimate protected source
Expected result / acceptance: Suppression attempt rejected; lawful meaningful projection or empowered conflict resolution; recorded exception and review cannot waive duty/control.

Table row 21
VER: 021
REQ: 031/032
Fixture / precondition: Deletion event followed by backup restore; orphan export/provider copy; expired support approval
Expected result / acceptance: No reactivation/reuse outside policy; outstanding copies/delay acknowledged; no unsupported full-deletion claim.

Table row 22
VER: 022
REQ: 033
Fixture / precondition: Same actor, organisation A versus B; copied token, record reference and matching person name
Expected result / acceptance: Independent organisation scope enforced; no cross-instance permission by identity similarity.

Table row 23
VER: 023
REQ: 035/036
Fixture / precondition: Material correction affects one pending analysis and one completed disclosure, plus unrelated task
Expected result / acceptance: Pending dependencies selectively reassessed; completed effect/history preserved with approved follow-up; unrelated task independently evaluated.

Table row 24
VER: 024
REQ: 037
Fixture / precondition: Disclosure timeout followed by duplicate attempt; partial recipient acknowledgement
Expected result / acceptance: Indeterminate state retained; separately authorised reconciliation precedes consequential repetition; no repeated exposure by timeout default.

Table row 25
VER: 025
REQ: 038/042
Fixture / precondition: Retrieved document instructs override; administrator widens policy; directors consent to live AI capture
Expected result / acceptance: No permission from model/content/admin convenience; prohibited deliberation capture rejected; attempted bypass and actual boundary evidence retained.

Table row 26
VER: 026
REQ: 043/044
Fixture / precondition: Definition/version compatibility; inspect/test exact approved synthetic fixture and definition revisions
Expected result / acceptance: KXV-01: supported, unsupported and accepted translated records; original and translation retained, restricted meaning preserved, declared loss suitable for use. Planned, not executed.

Table row 27
VER: 027
REQ: 045
Fixture / precondition: Assurance status and exact fact binding; inspect/test exact approved synthetic fixture and definition revisions
Expected result / acceptance: KXV-02: multiple incomplete/disputed/purpose-bounded assessments; preserve all chains and disagreements; no admission-to-truth or new-revision validation shortcut. Planned, not executed.

Table row 28
VER: 028
REQ: 047
Fixture / precondition: Original evaluation and later effects; inspect/test exact approved synthetic fixture and definition revisions
Expected result / acceptance: KXV-03: permit/deny before effect, later checkpoint/withheld/effect links; original decision reconstructable, absent evidence never proof of enforcement. Planned, not executed.

Table row 29
VER: 029
REQ: 046
Fixture / precondition: Acknowledgement stages; inspect/test exact approved synthetic fixture and definition revisions
Expected result / acceptance: KXV-04: delivery without application/responsibility; no false completion; pure information requires no invented human acknowledgement. Planned, not executed.

Table row 30
VER: 030
REQ: 043
Fixture / precondition: Reciprocal CON walkthrough; inspect/test exact approved synthetic fixture and definition revisions
Expected result / acceptance: KXV-05: inspect every component CON against the same producer/consumer definitions, field/status/units/ack manifest; retain mismatches and non-kernel dependencies. Planned, not executed.

Table row 31
VER: 031
REQ: 045
Fixture / precondition: Restricted assurance projection; inspect/test exact approved synthetic fixture and definition revisions
Expected result / acceptance: KXV-06: permitted projection preserves required assurance substance; unavailable material evidence leaves reliance unresolved; no privacy bypass. Planned, not executed.

Table row 32
VER: 032
REQ: 048
Fixture / precondition: KCV-01: Exact checkpoint and restriction race; inspect/test exact authorised synthetic fixture and versions
Expected result / acceptance: Substitute arguments/current evidence and restrict before/after last enforceable point; affected pre-boundary effect blocked, irreversible crossing and uncertainty/follow-up evidenced. Planned, not executed.

Table row 33
VER: 033
REQ: 048/049
Fixture / precondition: KCV-02: Partial compatible activation; inspect/test exact authorised synthetic fixture and versions
Expected result / acceptance: Wrong/old/missing required applied member and restriction during rollout; affected path withheld, compatible unaffected scope evidenced, no approval-to-activation shortcut. Planned, not executed.

Table row 34
VER: 034
REQ: 050
Fixture / precondition: KCV-03: Change receipt versus application; inspect/test exact authorised synthetic fixture and versions
Expected result / acceptance: Duplicate/conflicting/out-of-order notices and missing consumer; actual applied/no-material-dependency basis or owned unresolved cover/escalation; old permission not revived. Planned, not executed.

Table row 35
VER: 035
REQ: 050/055
Fixture / precondition: KCV-04: Selective impact and restart; inspect/test exact authorised synthetic fixture and versions
Expected result / acceptance: Correct pending input and significant completed consequence; reassess affected work, preserve history and owner review, no replay on restart. Planned, not executed.

Table row 36

VER: 036
REQ: 051/052
Fixture / precondition: KCV-05: Concurrent overlapping capacity; inspect/test exact authorised synthetic fixture and versions
Expected result / acceptance: Parallel workers request same remaining allowance across multiple scopes and provider switch; no partial grant, double spend or account reset evasion; exact authoritative evidence. Planned, not executed.

Table row 37
VER: 037
REQ: 051/053
Fixture / precondition: KCV-06: Partial/unknown reservation; inspect/test exact authorised synthetic fixture and versions
Expected result / acceptance: Expire/cancel/failover after possible effect and cross period boundary; confirmed quantity consumed, uncertain remainder held, release only evidenced unused quantity. Planned, not executed.

Table row 38
VER: 038
REQ: 054
Fixture / precondition: KCV-07: Withheld duty notification; inspect/test exact authorised synthetic fixture and versions
Expected result / acceptance: Accounting/control unavailable, missing acknowledgement, failed route and coalesced repeats; dependent work blocked, separate permitted notification and accountable delivery exception/cover; every operation traceable. Planned, not executed.

Table row 39
VER: 039
REQ: 054/055
Fixture / precondition: KCV-08: Resident update and controlled resume; inspect/test exact authorised synthetic fixture and versions
Expected result / acceptance: Service affected with acknowledgement but unresolved task, unagreed channel and sensitive content, then premature resume; only permitted agreed-channel update, contact duty visible, no replay without current reconciled evidence/approval. Planned, not executed.

Table row 40
VER: 040
REQ: 056
Fixture / precondition: KPV-01 / DEC-104: approved finding-class profile; primary controls/reporting failure plus implicated or suppressing normal recipient/release controller; false alternative sharing technical dependency or implicated sole gatekeeper; valid authorised independent alternative.
Expected result / acceptance: The component supplies its assigned authority/record/use/task/runtime evidence for both technical and organisational independence. No implicated sole release gate; no assumed independence from an alternate address alone. Use only pre-authorised verified minimal-content routes; inadequate arrangements remain owned, block protected-reporting assurance/affected dependent reliance and preserve tracking/service duties. Inspect actual alternate attempt, custody/control, recipient and acceptance evidence; no external-disclosure default. Planned, not executed.

Table row 41
VER: 041
REQ: 057
Fixture / precondition: KPV-02: Reporting permission and recipient invalid; authorised synthetic fixture, exact profile and source revisions
Expected result / acceptance: Expired/wrong-scope advance permission, unverified recipient or excessive content; refuse unauthorised payload, retain minimal permitted fallback if valid, otherwise owned unresolved duty; no emergency grant. Planned, not executed.

Table row 42
VER: 042
REQ: 058
Fixture / precondition: KPV-03: No human accepts and fallback also fails; authorised synthetic fixture, exact profile and source revisions
Expected result / acceptance: Receipt without responsibility acceptance, absent cover, escalation failure and repeated linked reports; original tracking owner persists, all affected work traceable, approved human fallback/owned exception and resident-channel duty remain visible. Planned, not executed.

Table row 43
VER: 043

REQ: 059
Fixture / precondition: KPV-04: Protected backup is stale or incomplete; authorised synthetic fixture, exact profile and source revisions
Expected result / acceptance: Valid integrity check but omitted withdrawal/consent/deletion/change or uncertain source coverage; dependent release blocked until scope-specific currentness and completeness are established from authoritative evidence. Planned, not executed.

Table row 44
VER: 044
REQ: 060
Fixture / precondition: KPV-05: Restore contains old permission and uncertain effects; authorised synthetic fixture, exact profile and source revisions
Expected result / acceptance: Isolated old snapshot with deleted/restricted payload, completed/partial/unknown effects, uncertain reservation and incompatible config; no normal effects, apply dispositions and reconcile exposure, no repeated known effect or hidden retained payload. Planned, not executed.

Table row 45
VER: 045
REQ: 061
Fixture / precondition: KPV-06: Premature selective release under compound failure; authorised synthetic fixture, exact profile and source revisions
Expected result / acceptance: Combine compromise, incomplete current-state evidence, outstanding handoff and provider failover; reject unsupported automatic/human release, accept only evidenced approved unaffected scope, preserve unresolved duties and require fresh CHECK/reservation for continuation. Planned, not executed.

Repeat cross-domain/exception cases over a controlled sequence of changes to reveal cumulative drift. Verify equity and usability of identity/consent controls across relevant groups through permitted evaluation; do not turn fairness assessment into unapproved profiling. A component pass does not establish systemwide safety, legal compliance or meaningful human judgement.

15.3 External-research planned acceptance

Approved synthetic fixtures, scope values and assessor roles must be supplied before execution. Component/privacy/platform reviewers and AOS-04/40 evaluators assess their respective meanings/controls; retain source, task, control, coverage, finding, handoff and human disposition evidence with limitations.

Table row 1
VER: 046
REQ coverage: 062/068
Controlled inputs / procedure: Profile/remit/source admission incomplete; wrong jurisdiction or future-effective proposal; relevant authoritative development; exact synthetic profile/dependency revisions, permitted assessor/tool scope
Expected result / retained evidence: Require scoped approved profile; correctly distinguish relevance/source status and exact baseline; unsupported reliance withheld; no invented values. Planned, not executed.

Table row 2
VER: 047
REQ coverage: 063
Controlled inputs / procedure: Denied retrieval, hostile page instructions and substituted tools/processing purpose; exact synthetic profile/dependency revisions, permitted assessor/tool scope
Expected result / retained evidence: Observe independent denial; source cannot change powers/profile; disclose coverage gap without broadening access. Planned, not executed.

Table row 3
VER: 048
REQ coverage: 064
Controlled inputs / procedure: Stale baseline, conflicting assurance or missing source/effective dates; partial/failed/unperformed run and

completed bounded no-finding; exact synthetic profile/dependency revisions, permitted assessor/tool scope
Expected result / retained evidence: Preserve evidence/inference/unknowns and exact history; correctly distinguish coverage states and record owned follow-up. Planned, not executed.

Table row 4
VER: 049
REQ coverage: 065
Controlled inputs / procedure: Shared source impacts two components; duplicate finding and later source correction; exact synthetic profile/dependency revisions, permitted assessor/tool scope
Expected result / retained evidence: Reuse source identity while retaining distinct findings/owners/deadlines; propagate/reassess material correction without dropping duties. Planned, not executed.

Table row 5
VER: 050
REQ coverage: 066
Controlled inputs / procedure: Unresponsive reviewer, failed delivery and urgent live implication; accepted-for-work candidate attempts direct activation; exact synthetic profile/dependency revisions, permitted assessor/tool scope
Expected result / retained evidence: Retain tracker/cover/approved escalation; no simulated delivery or self-amendment; human disposition does not equal release/application. Planned, not executed.

Table row 6
VER: 051
REQ coverage: 067
Controlled inputs / procedure: Human-approved rubric with relevant, irrelevant, missed and distorted evidence examples; deterministic bypass fixture; exact synthetic profile/dependency revisions, permitted assessor/tool scope
Expected result / retained evidence: Retain assessed evidence-fidelity/relevance/false-missed findings and limits separately from observed control tests; no self-certified sufficiency. Planned, not executed.

DEC-100 planned bootstrap/access case

Table row 1
VER: 052
REQ coverage: 069/007
Preconditions / procedure: Startup with a valid advance metadata-read instrument, then missing, expired, withdrawn, wrong-instance or excessive permission. Try to derive the checker’s permission from the pending business request or the other check’s favourable result; request underlying operational records. Interrupt permission/currentness lookup and restore stale metadata.
Expected result / retained evidence: Minimum scoped metadata reads are permitted only on independently verified advance authority/use evidence; no self-authorisation, circular favourable grant or wider operational access. Unverified/currentness failures withhold affected reliance and retain accountable referral; separately authorised fallback has no enlarged powers. Startup/recovery must re-establish valid current permission before reliance. Retain instrument/profile, checked identity/metadata scope, ordered access attempts, prevention/currentness/referral observations and competent assessor findings. Planned, not executed.

16. Dependencies

Table row 1
Stage: Drafting
Dependency / responsible owner: Q01-Q05 directions settled under DEC-049-053; AOS-01/02 reciprocal requirements; AOS-11/12 private-space/choice protocols; AOS-13/14/30 routing and disclosure; full source-matrix allocation

Table row 2
Stage: Build
Dependency / responsible owner: Exact REC-D/identity/consent/projection/lifecycle schemas; accepted revisions; control metadata bootstrapping; approved identity/role/inference/currentness threat profiles; risk-based scope classification; dependency lineage; test

configuration

Table row 3
Stage: Activation
Dependency / responsible owner: Verified lawful bases/additional conditions/rights/impact assessment; approved board welfare hierarchy and operational powers; actual providers/locations/onward use; usable human/accessible routes; retention/backup arrangements; resident agreements; appointments and readiness evidence

Table row 4
Stage: Operation
Dependency / responsible owner: Current roles/representation, consent/permission state, protected audience obligations, incident response, review cycles, configuration/model-change assessment and accountable outcome tracking

Generic specification drafting can continue while commissioning details remain open. A build depending on an unresolved material contract cannot invent a default; a harmless test fixture is labelled synthetic and carries no operational authority.

17. Issues and design questions

17.1 Design directions approved by Mark, 5 October

Table row 1
Question: Q01 / ISS-001
Decision requested / recommendation: Should identity assurance be proportionate to the operation, with verified accessible human-assisted alternatives? Approved yes: public information does not need the same assurance as sensitive disclosure or changing another person’s permissions; protected actions retain sufficient verification
Reason / consequence: Avoid both weak assurance and excluding people who cannot use standard digital proof. Exact methods/risk classes remain commissioned, not a blanket low-assurance exception

Table row 2
Question: Q02 / ISS-002
Decision requested / recommendation: Should the resident’s assistant have a private space, separate from organisational intelligence? Approved yes: no enterprise visibility, profiling or performance use of private content by default; resident explicitly selects what to share. Any exception needs its own narrowly defined lawful and governance basis
Reason / consequence: Build trust in assistance without covert observation. Define service/provider access transparently; private does not mean an unqualified promise of absolute secrecy

Table row 3
Question: Q03 / ISS-003
Decision requested / recommendation: How should welfare-versus-consent exceptions operate? Approved direction: a board-approved, tightly bounded acute-risk protocol: named empowered human decision makers, evidenced threshold, verified lawful basis, minimum necessary processing, time-limited scope and recorded explanation/review; agent’s role is permitted detection and authorised referral
Reason / consequence: Implements the RP board-hierarchy duty without a broad “safeguarding” override. Pre-approved human emergency operating routes can avoid waiting for board meetings; no prohibited behavioural inference is thereby authorised

Table row 4
Question: Q04 / ISS-004
Decision requested / recommendation: Should refusing or withdrawing optional data use carry no adverse service or employment consequence attributable to that refusal? Approved yes, for residents and workers, with genuinely required core processing identified and explained separately
Reason / consequence: Makes choice credible under no-exit/power imbalance. Service features intrinsically requiring the declined optional processing may be unavailable, but core service/job treatment cannot become a penalty; invalid consent never permits scope expansion

Table row 5

Question: Q05 / ISS-005
Decision requested / recommendation: When explanation conflicts with confidentiality, should the default be meaningful disclosure with the least restriction consistent with approved obligations, plus an accountable review route? Approved yes: preserve decision substance, uncertainty and assurance provenance; protect only what must be protected; record material withholding and offer human challenge
Reason / consequence: Radical Transparency remains interrogable without exposing another person’s data. No blanket redaction or automatic release; required audience conflicts need empowered resolution

17.2 Issue register

Every issue is open unless stated. Owner roles are required appointments, not assumed named post-holders. Confidence is high in materiality; evidence sufficiency/current legal mapping remains unassessed. Resolution requires a recorded decision/evidence reference; no research citation alone closes an issue.

Table row 1
ISS / type / status: 001 / dependency / open - general direction resolved
Source and affected elements: Q01; S01/S11; CAP-001, CON-001, REQ-001/016
Owner / evidence / gate / disposition: Approved Mark direction (5 October); organisational security/privacy and accessibility owners fix methods/risk classes; before dependent build/activation

Table row 2
ISS / type / status: 002 / dependency / open - general direction resolved
Source and affected elements: Q02; S01/S02; CAP-004, CON-004, REQ-022
Owner / evidence / gate / disposition: Approved Mark direction (5 October); AOS-11/03/05 owners define provider/private boundary and exceptions; before private-assistant build

Table row 3
ISS / type / status: 003 / dependency / open - general direction resolved
Source and affected elements: Q03; S04/S06/S08; CAP-003/005, CON-007, REQ-012/019/020
Owner / evidence / gate / disposition: Mark design direction; organisation board/privacy/safeguarding powers, threshold, basis, explanation/review; before exception activation

Table row 4
ISS / type / status: 004 / dependency / open - general direction resolved
Source and affected elements: Q04; S01/S05; CAP-003, REQ-013/016/023
Owner / evidence / gate / disposition: Approved Mark direction (5 October); resident/workforce/privacy review of optional/required classification and credible choice; before dependent activation

Table row 5
ISS / type / status: 005 / dependency / open - general direction resolved
Source and affected elements: Q05; S07/S10; CAP-005, CON-005, REQ-025-029
Owner / evidence / gate / disposition: Approved Mark direction (5 October); privacy/governance owners specify restrictions, protected audiences and appeal; before disclosure build

Table row 6
ISS / type / status: 006 / dependency / open
Source and affected elements: Identity/representation, notice and consent schemas, accessible rights/capacity routes; CON-001/003/007
Owner / evidence / gate / disposition: AOS-02/03/11/12/30 semantic owners; exact types/version/evidence/succession and usable testing; before dependent build

Table row 7
ISS / type / status: 007 / dependency or conflict / open
Source and affected elements: Legal basis, additional category conditions, purpose expansion and valid consent; EXT-P01-04/S04/05
Owner / evidence / gate / disposition: Empowered legal/privacy/governance owners; exact current provisions/commencement, scope, impact/risk assessment and AOS conflict resolution; before dependent activation

Table row 8
ISS / type / status: 008 / dependency / open
Source and affected elements: Invalidation/currentness, caches/races and selective pending-work reassessment; CON-002/004
Owner / evidence / gate / disposition: AOS-03/04/05/02 owners; enforceable profiles with checkpoints/delay/restart tests; before dependent build

Table row 9
ISS / type / status: 009 / design gap / open
Source and affected elements: Permitted inference register, asset/behaviour architecture and join/sensitive-class assessment
Owner / evidence / gate / disposition: AOS-10-14/03/05; concrete data-flow designs, prohibited outputs, evaluation and review; before sensing/inference build

Table row 10
ISS / type / status: 010 / dependency / open
Source and affected elements: Record-class lifecycle, legal hold, audit projections and all-copy deletion/restoration
Owner / evidence / gate / disposition: AOS-02/03/05 with professional owners; approved policies/copy inventory/disposition assurance; before lifecycle build/activation

Table row 11
ISS / type / status: 011 / dependency / open
Source and affected elements: Resident agreement granularity, alternate versus combined channels, failed agreed channel
Owner / evidence / gate / disposition: AOS-11/03/13/14/30; organisation profile with agreement revisions, no unilateral substitution and authorised cover; before communication build

Table row 12
ISS / type / status: 012 / dependency / open
Source and affected elements: Provider/support/backup locations, external recipients/onward use, training arrangements
Owner / evidence / gate / disposition: AOS-03/05/14 professional owners; actual flows, contracts, assessments and approvals; before dependent activation

Table row 13
ISS / type / status: 013 / dependency / open
Source and affected elements: Source-matrix adoption, REC-D definitive IF allocation and reciprocal component coverage
Owner / evidence / gate / disposition: AOS-02/03 and all consumers; one accepted schema/semantic owner, exact trace links and compatibility; before complete handover

Table row 14
ISS / type / status: 014 / dependency / open
Source and affected elements: Independent review/readiness and executed evidence
Owner / evidence / gate / disposition: Mark/project then organisational reviewers/AOS-40; reviewer appointment and dated evidence; no achieved gate or activation claim

Mark approved all five recommendations on 5 October (“Agree all 5”), recorded as DEC-049-053. No further general design question is currently submitted. Other items are detailed schema, organisational policy, legal, implementation or assurance work; additional design conflicts may emerge during those reviews.

AOS-03-ISS-015 - External-research setup and assurance

Common logical inheritance is incorporated; remaining exact sources/jurisdictions/cadence/triggers, agent assignment, recipients/response/cover, approved rubrics and wire schema/compatibility are owned dependencies per §3.1. Component owner coordinates 01/02/03/04/05/14/13/30/40 and specialist reviewers. Gate: dependent build/research activation/reliance; evidence: controlled profiles/schema mappings, accepted evaluations and actual coverage/handoff/disposition results. No new general architecture question is submitted. Existing unresolved issues retain their scope; research pilot item 5b is not closed.

18. Implementation guidance - NON-NORMATIVE

Architectural requirement: precise, independent, current and accountable permitted use. Possible patterns: purpose-labelled record envelopes; separate policy evaluation/enforcement points; scoped credentials and claims; dependency indexes for invalidation; segregated private-assistant stores; field-level explanation projections; provider-processing controls; immutable event identities with policy-governed content lifecycle.

No pattern requires a vendor, token protocol, central database, zero-trust product or universal consent service. Cryptographic evidence can bind a claim to an issuer; it cannot prove valid consent, adequate human judgement or truth. Risk-based identity profiles may use several methods, but biometrics are not a default accessibility solution.

An inference guard must control the actual data/model/tool path. Asking a model to ignore available private data is not equivalent to keeping that data outside the path. Physical/logical separation choices and threat adequacy belong to implementation assurance under AOS-05.

19. Traceability and change

Maintain source/decision → REQ → relevant FUN/CON/state/INV → planned VER → executed evidence. §2 keys resolve versions and locators; §§4/14/15 provide requirement/control/acceptance relationships. The exact central Source Traceability Matrix allocation and source manifest updates remain ISS-013, not assumed complete by this local register.

Changes identify impacted purposes, actors, private boundaries, inference capability, disclosure/lifecycle policies, recipients/locations, dependent permits and tests. Schema/policy/model/provider change cannot acquire approval merely because it passed transport validation. New consent scope needs new choice evidence; old notices cannot be relabelled. Record exact compatibility, professional/human decisions and effective times.

Research custodians observe → analyse → challenge → propose. They cannot amend, approve or activate specification rules. Q01-Q05 directions were approved by Mark on 5 October and recorded in DEC-049-053; exact normative text remains proposed and subject to review.

19.1 Common decision-baseline reconciliation, 6 October 2026

Author review against AOS-00 v0.15 (DEC-001-061) and Specification Map v0.15. Earlier dated source/approval references identify historical derivation, not a competing current baseline. Decisions DEC-001-044 remain applicable as scoped in §§2-8: logical ownership, human reserved powers, common contracts, separate organisation instances, controlled locations, technology neutrality and bounded repair profiles. Repair-specific choices do not become universal rules. DEC-018 remains deferred; independent review remains unassigned. No new decision, permission, numerical setting or requirement approval is inferred.

The table records later-decision applicability and existing document anchors. It is a decision/status reconciliation, not the completed source-to-field-to-producer/consumer traceability required by KR-09.

Table row 1
Decision set: DEC-045-053
Applicable direction / responsibility boundary: Common assurance/lifecycle and independent identity/use, private-space, welfare, refusal and disclosure directions retain their approved status.
Existing component anchors: §§2/3/6/8/17; AOS-02/03 v0.3 and their shared dependencies
Remaining work / status: Exact assurance fields, use/enforcement sequencing and reciprocal adoption remain KR-01/07/08; no completed assurance claim.

Table row 2
Decision set: DEC-054-057
Applicable direction / responsibility boundary: Each worker needs its own use checks; task-scoped memory default and approved persistence preserve private-space boundaries.

Existing component anchors: REQ-006-009/022/030-032; CON-002/003/006; §§10/13/17
Remaining work / status: Receiving-use/memory settings and common checkpoint definitions remain open; KR-01/02/06.

Table row 3
Decision set: DEC-058-061
Applicable direction / responsibility boundary: Operational containment, continuity and failover do not create a processing exemption or permit a new recipient/location.
Existing component anchors: REQ-024/027-032/036/037; CON-005/006/007; VER-018/020/021/024
Remaining work / status: Permitted protected route and recovery basis remain KR-04/05; evaluation versus later enforcement evidence remains KR-07.

Stable REQ/VER/CON/IF identifiers, requirement wording and planned-case status are preserved. The five current component revisions are v0.3; their historical v0.1/v0.2 records remain intact. KR-09 decision/status/interface-label work is complete; full reciprocal source/REQ/contract/field/VER allocation remains open with the shared-contract work. Author checks are document checks, not executed verification or independent readiness evidence.

19.2 Action-2 source/field/consumer/verification allocation

New REQ-043-047 originate in v0.4, 6 October 2026; status proposed, owner inherited from document control, logical scope only. VER-026-031 are planned cases. Earlier records retain their origins; AOS-03 REQ-040 is clarified under DEC-064, not retired. Totals at this historical adoption step: 47 proposed REQs and 31 planned VERs.

Table row 1
Source / decision: DEC-002/065; QS-12/21; GT M1.13
Register obligation / common field: KXR-01/02/07/08; definition_revision/profile_manifest; KX-10 field_map/losses
Component REQ → planned VER: REQ-043/044 → VER-026/030
Reciprocal adoption: Every local CON ↔ declared producer/consumer ends in register §6

Table row 2
Source / decision: FP4/6; RP7 audit/uncertainty; DEC-046/062/063
Register obligation / common field: KXR-03/04; REC-E assurance_refs/status, complete REC-Q and use suitability
Component REQ → planned VER: REQ-045 → VER-027/031
Reciprocal adoption: Evidence producer/AOS-02 ↔ this consumer under independently permitted use

Table row 3
Source / decision: RP7 auditability; DEC-064
Register obligation / common field: KXR-05; original REC-A/D evaluation, REC-X exact-result/checkpoint/effect links
Component REQ → planned VER: REQ-047 → VER-028
Reciprocal adoption: AOS-01/03 evaluator ↔ AOS-04 execution/AOS-05 runtime ↔ AOS-02 custody

Table row 4
Source / decision: RP1 accountability; GT M1.13; DEC-066
Register obligation / common field: KXR-06; KX-21 stage/result/evidence
Component REQ → planned VER: REQ-046 → VER-029
Reciprocal adoption: Actual receiver/applier/empowered human ↔ sender/tracker; no assumed non-kernel adoption

Shared fields and reciprocal logical definitions are now adopted at kernel document level. Old local source-matrix/schema issue descriptions remain residual commissioning/full-suite tasks, not a reason to duplicate definitions. Full-suite source allocation and non-kernel adoption remain open; no implemented conformance or independent readiness evidence.

19.3 Action-3 exact obligation/field/consumer/verification allocation

REQ-048-055 originate in v0.5, 6 October; proposed logical scope, custodian/approver inherited, no implementation approval. VER-032-039 are planned. Totals at this historical adoption step: 55 proposed REQs/39 planned VERs. Original record wording and IDs remain unchanged.

Table row 1
Source / approved decision: DEC-067; FP4/5/6/7/10; RP1/7 audit/8 contextual authority/9 purpose; GT M1.13
Common obligation / field / reciprocal ends: KCR-01; CHECK.request/current sources/version/outcome; 01/03 controls → 04/05 effect gate, 02 custody
Proposed REQ → planned VER: REQ-048 → VER-032/033

Table row 2
Source / approved decision: DEC-068; FP4/5/6/7/10; RP1/7 audit/8 contextual authority/9 purpose; GT M1.13
Common obligation / field / reciprocal ends: KCR-02; ACT.required members/applied vector/restriction fence; 01/03/04/05 application → coordinator/02
Proposed REQ → planned VER: REQ-049 → VER-033

Table row 3
Source / approved decision: DEC-069; FP4/5/6/7/10; RP1/7 audit/8 contextual authority/9 purpose; GT M1.13
Common obligation / field / reciprocal ends: KCR-03; CHG.consumer application/impact owner; semantic source/02 → all material consumers
Proposed REQ → planned VER: REQ-050 → VER-034/035

Table row 4
Source / approved decision: DEC-070; FP4/5/6/7/10; RP1/7 audit/8 contextual authority/9 purpose; GT M1.13
Common obligation / field / reciprocal ends: KCR-04; ACC.linked scope/period/units; 04 semantics → 05 accounting, 01/03 constraints, 02 custody
Proposed REQ → planned VER: REQ-051 → VER-036/037

Table row 5
Source / approved decision: DEC-071; FP4/5/6/7/10; RP1/7 audit/8 contextual authority/9 purpose; GT M1.13
Common obligation / field / reciprocal ends: KCR-05; RSV.complete demand/admission vector; 04 request → 05 authoritative admission → exact executor
Proposed REQ → planned VER: REQ-052 → VER-036

Table row 6
Source / approved decision: DEC-071; FP4/5/6/7/10; RP1/7 audit/8 contextual authority/9 purpose; GT M1.13
Common obligation / field / reciprocal ends: KCR-06; RSV.confirmed/residual/release evidence; observed effects → 05 account and 02/04 evidence
Proposed REQ → planned VER: REQ-053 → VER-037

Table row 7
Source / approved decision: DEC-071; FP4/5/6/7/10; RP1/7 audit/8 contextual authority/9 purpose; GT M1.13
Common obligation / field / reciprocal ends: KCR-07; WHD.owner/ack/cover/resident duty; service/05 blockers → permitted operational recipient, 13/30/resident workflow
Proposed REQ → planned VER: REQ-054 → VER-038/039

Table row 8
Source / approved decision: DEC-072; FP4/5/6/7/10; RP1/7 audit/8 contextual authority/9 purpose; GT M1.13
Common obligation / field / reciprocal ends: KCR-08; BRK.resume evidence/current check; authorised owner/controls/account → 04/05 executor
Proposed REQ → planned VER: REQ-055 → VER-035/039

Record types and source locators are the annex §§9-10, using unchanged FP/RP/GT versions. Non-kernel adoption and wire/profile/role implementation remain explicit gaps. This source/field/case allocation does not supply executed or independent assurance.

19.4 Action-4 sources and reciprocal verification

REQ-056-061 link DEC-073-078/KPR-01-06 to planned VER-040-045/KPV-01-06 one-to-one; all cases include cross-component failure/acceptance evidence. Source references and derivation boundaries are Protected Reporting and Recovery §7; exact fields, ownership and CON reciprocity are §§2/5. Current authoritative source mechanisms, human capacity, numerical profiles and commissioned independence need explicit owners/evidence before release. These cases have not been executed.

19.5 External-research traceability and current adoption

DEC-086 / AOS-00 REQ-050-054 and VER-023-025 → AOS-03-CAP-007/FUN-013/CON-008 → new REQ-062-068 → VER-046-051; exact row links in §§4.4/15.3. AOS-04 v0.7 §§3.1/5.1/6.6/10.8 (CON-009), AOS-02 v0.7 §6.6 (CON-007) and AOS-01 v0.7 §§6.6/10.8; Register v0.5 §13 and source matrix v0.7 §11 record reciprocal logical adoption. FP/RP/GT motivations retain their existing controlled versions; DEC-086 is Mark's approved architectural direction, not a new standards-derived mandate. No existing approvals, REQs, VERs, IFs or source histories are retired/promoted.

20. Build and handover

No implementation or activation is authorised by this draft. A selected handover fixes component/contract versions, scope and exclusions, resolved Q decisions, approved test/configuration profiles, authoritative instruments, human routes and acceptance evidence. It states which detailed controls the builder may choose and which choices require return to governance.

Builder stop conditions include unspecified identity risk class, missing legal/policy/consent basis, undefined welfare powers or threshold, unresolved private boundary, unsupported schema, unknown race/revocation behaviour, unexplained provider/location/training use, missing lifecycle copy controls and inadequate accessible/human routes. Do not invent consent expiry, retention duration, geographic permission, emergency powers, identity threshold or disclosure priority.

Independent project review is deferred. Author checks cannot substitute for the separate-reviewer G3 walkthrough. Organisational independent governance interpretation/precedent review under DEC-010-012 remains required separately.

21. Review and control

Table row 1
Quality assessment: Purpose/context/boundaries
Evidence / conclusion: §§1-3 explicitly separate authority, data use, common records, runtime and private/external boundaries

Table row 2
Quality assessment: Requirement records
Evidence / conclusion: §4.3 stable IDs, proposed status, owner/approver/versions/history/scope and sources/dependencies/VER links; profiles unresolved rather than defaulted

Table row 3
Quality assessment: Contract completeness
Evidence / conclusion: §6 identifies owners and timing/ordering/duplicates/retry/withdrawal semantics; executable schemas and accepted IF allocation still open

Table row 4
Quality assessment: Human boundaries / source applicability
Evidence / conclusion: §§7-8 distinguish permanent Mode 2, all FP/RP domains and 29 GT contributions; detailed central trace allocation incomplete

Table row 5

Quality assessment: Privacy/security/failure/evidence
Evidence / conclusion: §§9-13 cover joins, provider uses, currentness, accessible choices, protected audiences and actual enforcement; no proven resilience claim

Table row 6
Quality assessment: Verification
Evidence / conclusion: §15 has 39 planned cases covering normal/adversarial/degraded/cross-component and longitudinal scenarios; none executed

Table row 7
Quality assessment: Dependencies/issues/handover
Evidence / conclusion: §§16-20 isolate five settled directions and remaining material build/activation blockers; independent review explicitly deferred

Table row 8
Quality assessment: Author checks
Evidence / conclusion: Required sections, stable local IDs, references and table shapes checked; findings below. Checks establish document consistency, not design adequacy or legal validity

Table row 9
Quality assessment: Tailoring
Evidence / conclusion: No template section omitted; common metadata shared across REQ/VER rows explicitly. No quality-rule waiver asserted

Table row 10
Quality assessment: Specification quality conclusion
Evidence / conclusion: Structured review draft; complete schema/trace/commissioning and reviewer evidence outstanding

Table row 11
Quality assessment: Design adequacy conclusion
Evidence / conclusion: Plausible principle-derived design to test across contrasting contexts; five general directions settled; detailed commissioning and all executed adequacy evidence outstanding

Table row 12
Quality assessment: Approvals / gate
Evidence / conclusion: No component wording/whole-document approval recorded; no formal gate/build/activation approval

Residual findings: Q01-05 directions settled under DEC-049-053; legal/guidance currency and exact organisational mapping incomplete; detailed consumer obligations and common schemas not adopted; real enforcement/accessibility/deletion tests absent; independent reviewer unassigned. These findings stay visible when a general design direction is agreed.

Component summary

Purpose: accountable, purpose-bounded information use. Owns: identity/capacity assurance and use/consent/privacy semantics. Does not own: constitutional action powers, common record shapes, agent execution or runtime mechanisms. Receives: exact actor/data/purpose/basis requests and current approved instruments. Produces: scoped use determinations, consent/invalidation evidence, permitted explanations and human referrals. Key states: verified/unresolved identity; scoped active/refused/withdrawn consent; permit/deny/unresolved/unavailable; current/invalidated; pending/disposed. Depends upon: AOS-01/02/04/05, domain and human workflows, professional approvals and actual provider arrangements. Reserved human authority: values conflicts, hierarchy/exception policy, disputed rights and professional legal findings. Conformant when: adopted scope is evidenced through actual enforceable controls and meaningful human routes. Open now: detailed contract/commissioning/assurance dependencies; five general choices settled.

5 October v0.2 disposition: Mark agreed all five recommendations. DEC-049-053 settle proportionate accessible identity

assurance, private resident assistance, bounded human welfare protocols, protection for optional-use refusal and meaningful reviewable disclosure. REQ-001-042 remain proposed; VER-001-025 remain planned. No further general question currently awaits Mark. Next: AOS-04; reciprocal schema/consumer allocation and commissioning continue under Item 6.

Action-2 current disposition, 6 October: v0.4 uses AOS-00/Map v0.16 and approved DEC-062-066. §6.3/§19.2 record common logical adoption and traceability. Current totals 47 proposed REQs/31 planned VERs; earlier counts/versions in approval histories remain historical. No requirement-wording, executed-case or readiness promotion.

Action-3 current disposition, 6 October: DEC-067-072 approved, including revised recommendation 5 notification/acknowledged duty and appropriate resident update. AOS-03 v0.5 adopts Register v0.2, Core/Shared v0.3 and Control Coordination v0.1 against AOS-00/Map v0.17. Current totals 55/39 proposed REQs/planned VERs; no executed assurance or readiness promotion. KR-02/03/06 logically reconciled; actual commissioned implementation remains open.

Action-4 current disposition, 6 October: all six directions approved; DEC-073-078 and standards-reference instruction recorded. AOS-03 v0.6; 61 proposed REQs/45 planned VERs. KR-04/05 logically reconciled through the common annex and reciprocal adoption. No executed recovery/report delivery, clause-level ISO conformity, independent assurance or readiness promotion.

Current research amendment, 6 October 2026: AOS-03 v0.7; 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. 7 additional proposed REQs/6 planned VERs. Current totals 68 proposed REQs/51 planned VERs. Current component-control/traceability counts supersede earlier dated review counts; full-source and executed assurance remain open. Author document checks only; no live research, delivery, independent review or readiness evidence. Earlier dated counts and next-step notes remain historical; AOS-30 functional work is complete and current next work follows the to-do list.

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.