DEC-100 - minimum control-metadata access

Document: aos-dec-100-control-metadata-access-2026-10-29 · Source revision or record: DEC-100, 29 October 2026

AOS Specifications v1.0 · Edition dated 3 November 2026

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

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

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

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

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

29 October 2026 · Mark approved substantive question 2 in this chat (“yes”). Author: Codex. Approved direction; detailed normative wording remains subject to ordinary separate review/readiness gates.

Approved rule

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.

Allocation and retained limits

AOS-00/Map v0.50; AOS-01 v0.9 REQ-069 → planned VER-045; AOS-03 v0.10 REQ-069 → planned VER-052; Core v0.8; Shared v0.23; Exchange Register v0.22; Source Matrix v0.23. Existing IDs/wording preserved; two independently assessable new component obligations and two planned cases added. Current kernel catalogue now 364 requirement identities. DEC-099 and AOS-03 REQ-011/012 remain unchanged.

The approved principle does not establish an implemented non-circular bootstrap. Profiles, legitimate instruments, independent current-state verification, service identity, compatibility, accountability and actual adversarial/failure observations remain required before dependent reliance. No case execution, G3/G4, independent assurance, deployment or new inference/emergency permission follows. S-03-09 remain open.

Evidence

Originals, candidates, exact diff and hash/validation evidence are retained in the local AOS/deliverability-review-2026-10-29/decision-100 folder. Checks preserve existing normative rows/IDs, current inventory counts, planned case targets, new document links and saved contents. No running system was tested.