AAS-1

Audit Manual

Conducting a Class D Determination Engagement — v0.1

Published by	Kadikoy Limited, Bermuda (Reg. 202302362)
Date	9 May 2026
Status	Working draft — for the AAS-1 reference engagement
Version	0.1 — accompanies AAS-1 Specification v0.1
Companion to	AAS-1 Specification v0.1 (aas-1.org)
Reference engagement	PayAgent (Bond No. 1 ALA, did:ais1:base:payagent-001)
Contact	info@aiagentsservices.net
Repository	github.com/Kadikoy1/aas-1
License	Creative Commons CC0 — no rights reserved

WHAT THIS MANUAL COVERS	
ENGAGEMENT	How to scope, plan and document an AAS-1 audit engagement (Class E)
EVIDENCE	How to receive, validate and sample Class A records and their evidence
PROCEDURES	Auditor procedures for each of the twelve standard assertions
FINDINGS	Common exceptions and how each maps to a finding type
OUTPUT	Issuing the Class D determination — fields, signature, publication
EXAMPLE	Worked walkthrough on the PayAgent USDC transfer reference engagement

ABOUT THIS MANUAL

This manual is a practical engagement guide for an auditor conducting an AAS-1 Class D determination. It is the operational companion to the AAS-1 Specification v0.1: where the specification defines *what* AAS-1 records are, this manual sets out *how* an auditor receives them, evaluates them, and issues an opinion.

The manual is written against the PayAgent reference engagement — Bond No. 1, an Autonomous Legal Agent under AIS-1 v0.2, sponsored by Kadikoy Limited (Bermuda Reg. 202302362). PayAgent's Class A records are emitted in production, anchored to Ethereum, and signed using its AIS-1 verification method. The reference engagement is intended to be the first AAS-1 Class D determination ever issued. The procedures generalise to any AAS-1 engagement.

This manual does not replace professional judgement, the auditor's own engagement methodology, or applicable ethical standards. It standardises the *technical procedures* over AAS-1 records so that the auditor's professional judgement can be applied to subject matter where the underlying data is structurally trustworthy.

CONTENTS

1. The audit object — what the auditor is looking at

The auditor is presented with one or more **Class A Action Records** emitted by an AI agent. Each Class A record is a self-contained, signed, attestable document capturing a single action the agent took, the principal it acted for, the policies it operated under, and the evidence supporting the action.

Class A records may be presented individually or as part of a **Class B Batch** (period aggregation, with a Merkle root over the canonicalised members) or a **Class C Continuous** stream (single entries within a continuously attested feed). Whichever container is used, the atomic unit of audit is the Class A record.

The auditor's deliverable is a **Class D Determination** — a signed, structured opinion over the subject records, issued under a **Class E Engagement** (the engagement metadata: scope, period, framework, materiality, agent population). All five record classes are defined in §3 and §4 of the AAS-1 Specification.

> **The shortest version.** The agent emits Class A. The auditor evaluates Class A. The auditor issues Class D. Class B and C are aggregations of Class A. Class E is the wrapper that scopes the engagement.

2. Pre-engagement — defining the Class E engagement

Before any records are evaluated, the auditor and the engaging party agree the **Class E Engagement record**. This is the equivalent of an engagement letter: it defines the boundaries of the audit, signed by both parties.

Class E required attributes

Field	Description
aas	Standard version. "0.1"
eventId	Unique engagement identifier.
class	"E"
auditorRef	Auditor's AIS-1 identity DID.
principalRef	AIS-1 identity of the engaging party (typically the agent's sponsor).
scope	Free-text or structured description of the audit scope.
periodStart, periodEnd	RFC 3339 dates bracketing the engagement period.
framework	Audit framework applied (e.g. ISAE 3000, SOC 2, ISA 315).
materiality	Materiality threshold and basis (monetary, transaction-count, risk-weighted).
agentPopulation	Array of AIS-1 DIDs in scope. Singular for single-agent engagements (PayAgent).
timestamp	RFC 3339 timestamp of engagement creation.
signature	Auditor signature over canonicalised engagement record.

Practical points

- The Class E should be agreed and signed *before* any Class A records are evaluated. Records subsequently emitted are matched against the engagement by their engagementRef field.
- For the PayAgent reference engagement: periodStart = 2026-04-01, periodEnd = 2026-06-30, framework = "ISAE 3000 (Revised)", materiality = USD 1,000 transaction value, agentPopulation = ["did:ais1:base:payagent-001"].

- Materiality should be expressed in the natural unit of the agent's activity. For a payments agent, transaction value. For a decision agent, action count or risk-weighted score. The choice is the auditor's professional judgement.
- Where the engagement is over a single agent (single-agent engagement, as PayAgent), the Class E is a one-time document. Where the engagement is over a population, the Class E lists each agent in agentPopulation and a separate Class D may be issued per agent or one combined Class D over the population.

3. Receiving and validating the population

Once the engagement is in flight, the auditor receives the population of Class A records. The mode of receipt depends on the agent:

- **Pull from registry** — auditor fetches records from a published endpoint (e.g. https://logs.payagent.ai/2026/05/...) using engagementRef as a filter.
- **Push by operator** — operator delivers a Class B batch covering the period, with a Merkle root over the records.
- **Continuous stream** — for Class C-emitting agents, auditor subscribes to the stream and accumulates records during the engagement period.

Initial validation procedures

3.1 Confirm the count of records received against any pre-declared count from the operator.

3.2 Where a Class B is provided, recompute the Merkle root from the canonicalised members and confirm it matches the published root.

3.3 Walk the prevHash chain end-to-end and confirm no breaks. A break indicates either omission, reordering, or substitution.

3.4 Confirm every record's engagementRef matches the Class E identifier.

3.5 Confirm every record's timestamp falls within periodStart <= ts <= periodEnd.

3.6 Spot-check schema conformance against the published Class A schema (aas-1-class-a.schema.json). Records failing schema validation are exceptions.

If the prevHash chain breaks. This is a serious finding. It means the population is incomplete or has been tampered with. The auditor's response: request the missing records, document the gap, and if not resolved, issue Class D with finding *modified* or *adverse* depending on materiality.

4. The verification flow per record

For each Class A record selected for evaluation (whether all records, or a sample — see §6), the auditor runs the following four-phase flow:

```
// Phase 1 — Identity binding
const identity = await ais1.resolve(record.agentRef);
assert(verifySignature(record, identity.verificationMethod));
assert(ais1.verifyBond(identity.bondId).valid);

// Phase 2 — Independent timestamp
assert(verifyTimestamp(record.timestampServiceRef, record.timestamp));

// Phase 3 — Hash recomputation (where source data is available)
assert(sha256(canonicalize(actualInputs))  === record.action.inputsHash);
assert(sha256(canonicalize(actualOutputs)) === record.action.outputsHash);

// Phase 4 — Per-assertion evaluation
for (const a of AAS1.ALL_ASSERTIONS) {
  findings[a] = evaluate(a, record, identity, sourceData, policies);
}
```

Phases 1–3 are *structural* — they confirm the record is well-formed, signed by the right party, timestamped independently, and consistent with the underlying data. Phase 4 is *evaluative* — the application of the auditor's judgement against the twelve assertions, which is the substance of §5.

5. Procedures for the twelve assertions

For each assertion, this section sets out the definition, the fields in a Class A record that support evaluation, the specific procedures the auditor performs, and the common exceptions encountered.

5.1 Existence

Definition. The recorded action actually took place.

Fields. evidence array — at least one entry of types: signature, attestation, witness, log, hash_anchor, human.

Procedures

5.1.1 Confirm the evidence array contains at least one entry.

5.1.2 For each entry, validate per type: signatures verify cryptographically; hash anchors resolve and match; logs are reachable; attestations have a valid execution-environment signature.

5.1.3 Where the action has external observable effects (e.g. an on-chain transaction), independently confirm the effect. For a USDC transfer, fetch the transaction from the destination chain and confirm value, sender, recipient.

Common exceptions. Empty evidence array; hash anchor not found on the cited chain; log endpoint unreachable; on-chain action not visible at the cited block.

5.2 Completeness

Definition. All relevant actions in scope are recorded.

Fields. prevHash chain across the population; Class B Merkle root; engagement-level reconciliation.

Procedures

5.2.1 Walk the per-issuer prevHash chain end-to-end. No break.

5.2.2 For payments agents, reconcile recorded transactions against bank/wallet statements over the period. Investigate any transaction in the statement without a corresponding Class A record.

5.2.3 For decision agents, reconcile recorded decisions against principal-side action logs (e.g. tickets resolved, emails sent, contracts signed).

5.2.4 For high-frequency Class C streams, confirm the stream-anchor record covers the engagement period without gap.

Common exceptions. prevHash break; transaction in source data without corresponding record; gap in Class C stream-anchor coverage.

5.3 Accuracy

Definition. Inputs and outputs are faithfully captured.

Fields. action.inputsHash, action.outputsHash, plus the underlying source data the auditor obtains separately.

Procedures

5.3.1 Where the auditor has access to the underlying inputs (action specification: amount, destination, timing, instruction body), canonicalise via JCS and hash with SHA-256. Confirm equality with action.inputsHash.

5.3.2 Where the auditor has access to the underlying outputs (transaction hash, confirmation block, response body), canonicalise and hash. Confirm equality with action.outputsHash.

5.3.3 Where the auditor does *not* have direct access (e.g. PII inputs the principal cannot disclose), accept the principal's signed attestation that the hashes were computed against the canonical underlying data, and document the limitation.

Common exceptions. Hash mismatch (most serious — indicates tampering or computation error); missing hash; principal unable to attest.

5.4 Authorisation

Definition. The agent acted within delegated authority.

Fields. delegationRef, principalRef, AIS-1 bond status, materiality.

Procedures

5.4.1 Resolve delegationRef to obtain the delegation document (board resolution, treasury policy, automated mandate). Confirm it was effective at the action's timestamp.

5.4.2 Confirm the action falls within any limits expressed in the delegation (monetary, geographic, counterparty, time-of-day).

5.4.3 Confirm the AIS-1 bond was active and not suspended at the action's timestamp.

5.4.4 For Subordinate Operating Agents (SOA), confirm the parent ALA's bond was also active at the timestamp.

Common exceptions. Action above delegation limit; delegation expired; AIS-1 bond suspended; SOA acting after parent revocation.

5.5 Cutoff

Definition. The action is recorded in the correct period.

Fields. timestamp, timestampServiceRef.

Procedures

5.5.1 Verify the timestamp via the secondary timestampServiceRef. RFC 3161 — fetch the timestamp token and verify the TSA signature. OpenTimestamps — verify the Bitcoin anchor proof. HCS — verify the Hedera consensus timestamp.

5.5.2 Confirm the action's timestamp is within the engagement period (periodStart <= ts <= periodEnd).

5.5.3 Where the agent's action has an external cutoff implication (e.g. a contract execution at end-of-quarter), confirm consistency between the agent's recorded time and the external time of effect.

Common exceptions. Independent timestamp does not verify; large discrepancy between agent timestamp and TSA timestamp; record dated outside engagement period.

5.6 Classification

Definition. The action is correctly categorised by type.

Fields. action.type, action.tools, action.summary.

Procedures

5.6.1 Confirm action.type is one of the standard types (tool_call | decision | communication | transaction | policy_check | human_handoff | other).

5.6.2 Confirm the type is consistent with the tool used and the summary. A transaction-typed action invoking a research-search tool is a misclassification.

5.6.3 For other-typed actions, the operator should provide a free-text classification. The auditor reviews these for consistency and may propose a standard type.

Common exceptions. Action type inconsistent with tool; over-use of other; misuse of policy_check for substantive transactions.

5.7 Presentation

Definition. Records are presented and described accurately.

Fields. Whole record, schema conformance, JCS canonicalisation.

Procedures

5.7.1 Validate against the AAS-1 Class A JSON Schema. Reject records with schema violations.

5.7.2 Confirm the canonicalisation method declared in the signature object is JCS (RFC 8785). Re-canonicalise and confirm the hash is reproducible.

5.7.3 Confirm summary fields (where present) are consistent with the structured fields. A summary describing a USDC transfer should not be paired with an action.type of communication.

Common exceptions. Schema validation failure; non-JCS canonicalisation; misleading summary fields.

5.8 Identity

Definition. The recorded actor is the agent of record.

Fields. agentRef, signature, AIS-1 DID Document.

Procedures

5.8.1 Resolve agentRef via the AIS-1 §7.1 resolution algorithm to obtain the DID Document.

5.8.2 Confirm the signature's keyRef is a verification method declared in the DID Document.

5.8.3 Verify the signature: canonicalise the record minus its signature, hash with the declared algorithm, verify the signature value against the public key.

5.8.4 Confirm the AIS-1 bond was active at timestamp: call verifyBond(bondId) on the AIS-1 contract; check status was active; for Verified or Sovereign tier, check amlStatus was cleared.

5.8.5 For SOA, resolve parentDid and confirm the parent ALA bond was active at the timestamp.

Common exceptions. Signature verification fails; key not in DID Document; bond suspended; bond revoked; AML status not cleared.

5.9 Provenance

Definition. Model, tools, prompt context and data sources are captured.

Fields. action.model, action.tools, action.inputsHash.

Procedures

5.9.1 Confirm action.model is populated with both id and version. A bare model name without a version is insufficient.

5.9.2 Confirm action.tools lists every tool, MCP server or external service the agent invoked in the course of the action. Cross-reference against the operator's tool inventory.

5.9.3 For tools, confirm name, version and serverRef are all present. The serverRef is needed so a downstream auditor can resolve the tool's own provenance.

5.9.4 Where the action involves retrieved context (RAG, prompt context), confirm the inputsHash covers the full retrieved context, not just the user's input.

Common exceptions. Missing model version; tool listed without serverRef; retrieved context not in inputsHash; model declared but a different model used.

5.10 Reproducibility

Definition. Sufficient state to permit re-derivation under stated determinism.

Fields. action.inputsHash, action.outputsHash, action.model, action.tools, plus model-determinism declaration.

Procedures

5.10.1 Confirm all four required fields are populated.

5.10.2 Where the principal declares the model was run with deterministic settings (temperature 0, fixed seed), the auditor may attempt re-derivation by re-running the model with the recorded inputs and confirming output match.

5.10.3 Where determinism is not declared, the auditor evaluates reproducibility weakly: the inputs, model and tools are *captured*, but identical re-derivation is not asserted. This is acceptable for non-deterministic models so long as

it is documented.

5.10.4 For tool calls, confirm the tool's behaviour at the recorded version was deterministic with respect to the recorded inputs (e.g. the stablecoin-transfer tool's effect is fully determined by amount, destination, signing key).

Common exceptions. Missing reproducibility-supporting field; declared determinism that fails on re-derivation.

5.11 Policy Compliance

Definition. Applicable policies and the action's compliance result are recorded.

Fields. policyRefs, policyResult.

Procedures

5.11.1 Confirm policyRefs lists every policy applicable to the action type. Cross-reference the operator's policy inventory at the timestamp.

5.11.2 Confirm each policy referenced is reachable, versioned (a permanent URL with a version qualifier), and was effective at the action's timestamp.

5.11.3 Confirm policyResult.outcome is one of compliant, non_compliant, compliant_with_exception. Where non-compliant or exception, confirm the action was not executed (or was executed under a documented override). An action executing despite a non-compliant policy result is a serious finding.

5.11.4 For high-materiality actions, sample the policy evaluation logic and re-run it against the recorded inputs to confirm the recorded outcome.

Common exceptions. Missing policy references; policy URL unversioned or unreachable; non-compliant outcome with action executed; policy result not recorded.

5.12 Independence

Definition. Agent action is recorded separately from any operator override.

Fields. signature (must be agent's, not operator's); evidence array (additional human attestation if override invoked); notes.

Procedures

5.12.1 Confirm the record's primary signature is the agent's AIS-1 verification method, not the operator's.

5.12.2 Where the operator intervened (manual approval, manual override, manual cancellation), confirm a human-type evidence entry is present capturing the operator's identity and rationale.

5.12.3 Where notes indicates "no human override invoked," confirm no human evidence entry is present.

5.12.4 Inconsistencies between recorded autonomy and recorded human attestation are exceptions.

Common exceptions. Operator's signature on a record claimed to be agent-autonomous; missing human evidence on a record where override clearly occurred; ambiguous notes.

6. Sampling methodology

Where the population is large (thousands of Class A records), the auditor cannot evaluate every record in detail. AAS-1 records are designed to support efficient sampling: most assertions can be evaluated automatically across the full population (signature verification, schema validation, prevHash chain), and the auditor's judgement-intensive procedures are applied to a sample.

Recommended sampling layers

- **Full-population checks** — schema validation, signature verification, prevHash chain integrity, timestamp range. Performed across 100% of records by automated tooling (see aas1-verify.js in the AAS-1 repository).
- **Materiality-based sampling** — every record with materiality.amount at or above a defined threshold (e.g. USD 1,000) is evaluated in detail. For PayAgent in the reference engagement: USD 1,000 transaction value.
- **Risk-based sampling** — every record where policyResult.outcome is anything other than compliant is evaluated regardless of materiality.

- **Statistical sampling** — for the residual population, the auditor applies their normal sampling methodology (e.g. ISA 530), drawing from Class B Merkle members.
- **Override sampling** — every record with a human-type evidence entry (operator override invoked) is evaluated.

7. Findings catalogue — common exceptions

The auditor encounters issues during evaluation. Each issue maps to one or more assertions and to a finding type. The catalogue below is non-exhaustive but covers the typical cases.

Issue	Assertion(s)	Severity	Likely finding
Schema validation fails on a record	Presentation	Per-record	Exception
Signature does not verify	Identity	Per-record	Exception
Bond suspended at timestamp	Identity, Authorisation	Per-record	Exception
prevHash chain breaks across the population	Completeness	Population	Modified or Adverse
Recomputed inputsHash does not match	Accuracy	Per-record	Exception
Action above delegation limit	Authorisation	Per-record	Exception
Independent timestamp does not verify	Cutoff	Per-record	Exception
Action type inconsistent with tool used	Classification	Per-record	Exception
Missing model version in action	Provenance	Per-record	Exception
Non-compliant policy result with action executed	Policy Compliance, Authorisation	Per-record	Exception (escalate)
Operator signature on autonomous-claimed action	Independence	Per-record	Exception
Pattern of exceptions across population (>5%)	Multiple	Population	Modified
Pervasive exceptions (>20%)	Multiple	Population	Adverse
Auditor unable to obtain sufficient evidence	n/a	Engagement	Disclaimer

Per-record vs population. A single Class A record with an exception does not necessarily condemn the engagement. The auditor's overall finding (in the Class D) reflects the population-level pattern: isolated exceptions are listed but support an *unmodified* opinion; pervasive exceptions support *modified* or *adverse*; complete inability to evaluate supports *disclaimer*.

8. Issuing the Class D determination

Once all evaluation procedures are complete, the auditor issues the Class D Determination. The Class D is itself an AAS-1 record — signed, attestable, and bound to the auditor's AIS-1 identity.

Class D required attributes

Field	Description
aas	"0.1"
eventId	Unique determination identifier.
class	"D"
auditorRef	Auditor's AIS-1 identity DID.
engagementRef	Class E engagement record reference.
subjectRefs	Array of Class A (and/or B/C) records under examination, or a Merkle root over the population.
finding	unmodified | modified | adverse | disclaimer | exception
assertionResults	Array, one entry per assertion: { assertion, result, notes }.
timestamp	RFC 3339 timestamp of issuance.
timestampServiceRef	Independent timestamp service reference.
signature	Auditor's signature over the canonicalised determination.

Finding types

Finding	Meaning
unmodified	Records satisfy all twelve assertions across the population. Equivalent to a clean opinion.
modified	Records satisfy assertions in most material respects, with isolated or non-pervasive exceptions documented.
adverse	Records do not satisfy one or more assertions in pervasive, material respects.
disclaimer	Auditor was unable to obtain sufficient evidence to form an opinion. Scope limitation.
exception	Reserved for engagement-level findings unrelated to the assertions (e.g. independence violation by the auditor).

Publication

- The Class D is signed using the auditor's AIS-1 verification method.
- It is published at a stable URL (e.g. https://audits.example.com/determinations/{eventId}.json).
- The hash of the canonical Class D may optionally be anchored to a public ledger for tamper-evidence (recommended for the reference engagement).
- Other agents and counterparties resolve the Class D by its eventId when forming trust decisions about the audited agent.

9. Worked example — PayAgent USDC transfer

This section walks through the evaluation of the reference Class A record (Appendix A of the AAS-1 Specification): PayAgent's USD 2,500 stablecoin transfer to a vendor wallet on 9 May 2026.

9.1 The record at a glance

Field	Value
agentRef	did:ais1:base:payagent-001 (PayAgent, ALA)
principalRef	did:ais1:sponsor:kadikoy-bm-202302362 (Kadikoy Limited)
delegationRef	https://kadikoy.bm/delegations/2026-q2-payments
timestamp	2026-05-09T14:32:11Z
timestampServiceRef	rfc3161:tsa.example.com
action.type	transaction
action.summary	Outbound USDC transfer 2,500.00 to vendor wallet
action.model	claude-opus-4-7 (version 2026-04)
action.tools	stablecoin-transfer v1.4.0 (mcp.payagent.ai/transfer)
materiality	USD 2,500 (transaction-value basis)
policyRefs	Kadikoy payments v3; Kadikoy AML screening v2
policyResult	compliant — counterparty cleared screening; within USD 5,000 limit
evidence	signature + TEE attestation + Ethereum hash anchor + log reference

9.2 Evaluation against the twelve assertions

#	Assertion	Procedure outcome	Result
1	Existence	4 evidence entries; on-chain transfer confirmed at the cited block	Satisfied
2	Completeness	prevHash chains to predecessor; population reconciled to wallet statement	Satisfied
3	Accuracy	Recomputed inputsHash and outputsHash match the principal's source data	Satisfied
4	Authorisation	Q2 2026 payments delegation effective; USD 2,500 within USD 5,000 limit	Satisfied
5	Cutoff	RFC 3161 token verifies; timestamp within engagement period (Q2 2026)	Satisfied
6	Classification	action.type = transaction; consistent with stablecoin-transfer tool	Satisfied
7	Presentation	Schema valid; JCS canonicalisation reproduces signature-input hash	Satisfied

#	Assertion	Procedure outcome	Result
8	Identity	DID resolves; key in DID Document; signature verifies; bond active	Satisfied
9	Provenance	Model id and version present; tools captured with serverRef	Satisfied
10	Reproducibility	Inputs, model, tools captured; non-deterministic re-derivation noted	Satisfied (with caveat)
11	Policy Compliance	Two policies referenced; both versioned; outcome compliant	Satisfied
12	Independence	Agent signature only; notes confirm no operator override	Satisfied

9.3 The auditor's Class D — illustrative output

After evaluating this record (and the surrounding population for the engagement period), an auditor satisfied with all twelve assertions issues the Class D as follows:

```
{
  "aas": "0.1",
  "eventId": "01HZB7K5N9PQX3YR4WMVT8CDAS",
  "class": "D",
  "auditorRef": "did:ais1:sponsor:[auditor-firm-bermuda]",
  "engagementRef": "https://audits.example.com/engagements/kadikoy-2026-h1",
  "subjectRefs": [
    "did:ais1:base:payagent-001/records/2026-04",
    "did:ais1:base:payagent-001/records/2026-05",
    "did:ais1:base:payagent-001/records/2026-06"
  ],
  "finding": "unmodified",
  "assertionResults": [
    { "assertion": "existence",        "result": "satisfied" },
    { "assertion": "completeness",     "result": "satisfied" },
    { "assertion": "accuracy",         "result": "satisfied" },
    { "assertion": "authorisation",    "result": "satisfied" },
    { "assertion": "cutoff",           "result": "satisfied" },
    { "assertion": "classification",   "result": "satisfied" },
    { "assertion": "presentation",     "result": "satisfied" },
    { "assertion": "identity",         "result": "satisfied" },
    { "assertion": "provenance",       "result": "satisfied" },
    { "assertion": "reproducibility",  "result": "satisfied",
      "notes": "Non-deterministic model; reproducibility weakly asserted." },
    { "assertion": "policy_compliance","result": "satisfied" },
    { "assertion": "independence",     "result": "satisfied" }
  ],
  "timestamp": "2026-07-15T10:00:00Z",
  "timestampServiceRef": "rfc3161:tsa.example.com",
  "signature": {
    "alg": "EdDSA", "hashAlg": "SHA-256", "canonicalisation": "JCS",
    "keyRef": "did:ais1:sponsor:[auditor-firm-bermuda]#key-1",
    "value": "z7HwQ2..."
  }
}
```

10. Engagement deliverables and retention

- **Class E Engagement record** — signed by both parties at engagement start.
- **Working papers** — auditor's evaluation evidence (samples drawn, hashes recomputed, exceptions raised, professional judgement notes). Retained per the auditor's normal records-retention policy.

- **Class D Determination** — the headline deliverable. Signed by the auditor, published at a stable URL, optionally anchored on-chain.
- **Engagement archive** — the auditor retains a snapshot of the Class A records evaluated, the Class B/C aggregations, the Class E engagement record, and the Class D. This snapshot is the equivalent of the audit working file.

For the AAS-1 reference engagement, the auditor is encouraged to publish the Class D openly (CC0) so it can serve as a reference output for the standard. The agent's own records remain the operator's property; the auditor publishes only the determination.

Appendix A: Class D determination template

A skeleton the auditor populates and signs:

```
{
  "aas": "0.1",
  "eventId": "&lt;ULID&gt;",
  "class": "D",
  "auditorRef": "&lt;auditor AIS-1 DID&gt;",
  "engagementRef": "&lt;Class E engagement reference&gt;",
  "subjectRefs": [
    "&lt;Class A or B or C record reference&gt;"
  ],
  "finding": "&lt;unmodified | modified | adverse | disclaimer | exception&gt;",
  "assertionResults": [
    { "assertion": "existence",        "result": "satisfied | exception", "notes": "" },
    { "assertion": "completeness",     "result": "satisfied | exception", "notes": "" },
    { "assertion": "accuracy",         "result": "satisfied | exception", "notes": "" },
    { "assertion": "authorisation",    "result": "satisfied | exception", "notes": "" },
    { "assertion": "cutoff",           "result": "satisfied | exception", "notes": "" },
    { "assertion": "classification",   "result": "satisfied | exception", "notes": "" },
    { "assertion": "presentation",     "result": "satisfied | exception", "notes": "" },
    { "assertion": "identity",         "result": "satisfied | exception", "notes": "" },
    { "assertion": "provenance",       "result": "satisfied | exception", "notes": "" },
    { "assertion": "reproducibility",  "result": "satisfied | exception", "notes": "" },
    { "assertion": "policy_compliance","result": "satisfied | exception", "notes": "" },
    { "assertion": "independence",     "result": "satisfied | exception", "notes": "" }
  ],
  "exceptions": [
    { "recordRef": "&lt;Class A reference&gt;", "assertion": "&lt;assertion&gt;",
      "description": "&lt;what went wrong&gt;", "materiality": "&lt;how material&gt;" }
  ],
  "timestamp": "&lt;RFC 3339&gt;",
  "timestampServiceRef": "&lt;TSA reference&gt;",
  "signature": {
    "alg": "EdDSA", "hashAlg": "SHA-256", "canonicalisation": "JCS",
    "keyRef": "&lt;auditor DID&gt;#key-1", "value": "&lt;signature value&gt;"
  }
}
```

Appendix B: Engagement letter template

The Class E engagement is the on-chain (or off-chain but signed) version of an engagement letter. The conventional engagement letter sits alongside it, in the auditor's normal form, and references the Class E by engagementRef:

```
[Auditor Firm Letterhead]

[Date]
[Engaging Party — typically the agent's sponsor]

Dear [Sponsor],

We have been engaged to perform an examination of the AAS-1 Class A
Action Records emitted by [Agent Name] (AIS-1 DID: [agentRef]) over
the period [periodStart] to [periodEnd].

The engagement will be conducted in accordance with [framework — e.g.
ISAE 3000 (Revised)] and the AAS-1 Audit Manual v0.1. We will issue a
Class D Determination expressing our opinion on whether the records
satisfy the twelve standard assertions defined by AAS-1 v0.1.

Our materiality threshold for the engagement is [materiality].

The engagement is captured on-record as Class E engagement
```

```
[engagementRef], signed by both parties.

Our Class D Determination will be issued by approximately [target
issuance date] and published at [Class D URL] under CC0.

Yours faithfully,
[Auditor], [Title]
[Auditor's AIS-1 DID]
```

Appendix C: Working-paper checklist

A short checklist the auditor works through during the engagement. Tick when complete.

Pre-engagement

- Class E engagement record drafted, agreed and signed
- Engagement letter signed; references Class E by engagementRef
- Auditor's AIS-1 identity confirmed and verification method available
- Population delivery method agreed (pull / push / continuous)
- Materiality threshold and basis documented

Population validation

- Record count agreed with operator
- Class B Merkle root recomputed and matched (if applicable)
- prevHash chain walked end-to-end without break
- All records' engagementRef matches Class E
- All records' timestamps within engagement period
- Schema validation pass across full population

Per-record evaluation

- Identity binding verified (signature, DID, bond status)
- Independent timestamp verified
- Hashes recomputed against source data (where accessible)
- All twelve assertions evaluated and findings recorded
- Exceptions documented with recordRef + materiality

Determination

- Population-level finding determined (unmodified / modified / adverse / disclaimer)
- Class D record drafted and signed using auditor's AIS-1 verification method
- Class D published at stable URL
- (Optional) Class D hash anchored on-chain
- Engagement archive retained per firm retention policy