ACAS-1

Agent Compliance Accountability Standard

Working Paper v0.1 — Draft for Comment

Published by	Kadikoy Limited, Bermuda (Reg. 202302362)
Date	31 July 2026
Status	Draft — open for public comment
Version	0.1 — initial release
Companion to	AIS-1 Agent Identity Standard (ais-1.org); AAS-1 Agent Auditability Standard (aas-1.org); AIPS-1 Agent Interaction Protocol Standard (aips-1.org); ARS-1 Agentic Remittance Standard (ars-1.org); AES-1 Agent Execution Standard (aes-1.org)
Contact	info@aiagentsservices.net
Repository	github.com/Kadikoy1/acas-1
Website	acas-1.org
License	Creative Commons CC0 — no rights reserved

v0.1 KEY FEATURES

INTRODUCES	Continuous assurance as the organising idea — customer due diligence performed at machine cadence, with detection latency measured in hours rather than months, and proved rather than asserted
DEFINES	The Compliance Step — the evidentiary output of one due-diligence act, with a common shape across every act, so a counterparty reads them all the same way
CLASSIFIES	Four carriage classes — Portable, Referenced, Freshness Signal, Subscription — because different due-diligence results travel in fundamentally different ways, and a flat catalogue misrepresents all of them
MEASURES	Detection latency as the assurance metric, with an evidenced performance record over a stated window, carried as a property of the programme rather than of any person
CATALOGUES	Seven step types anchored to the FATF Recommendations — R.10 supplies four of them, with R.6/7 and R.12 supplying the rest
SEPARATES	Continuous machine detection from human determination — the standard automates the finding of facts, never the making of decisions reserved to a responsible person
PRESENTS	A scoped, audience-bound, time-limited Presentation constructed under a revocable disclosure mandate — never a published file of personal information
COMPOSES	Built on AIS-1 for identity and AAS-1 for evidence; a Step is a specialised AAS-1 evidentiary record carrying a compliance vocabulary and a determination model

Contents

ABSTRACT

ACAS-1 is an open standard for **continuous, portable, provable customer due diligence** in agent-to-agent commerce. It addresses three problems at once.

The first is old. **Due-diligence work performed by one institution does not travel.** There is no portable, verifiable form in which completed diligence can be carried and checked, so every counterparty either repeats the work or accepts it on trust. The FATF Recommendations contemplate third-party reliance, but reliance is papered bilaterally between named institutions and does not scale to an open network.

The second is new and arriving quickly. **Agent-to-agent commerce** will generate counterparty relationships and transactions at volumes that no human review function can meaningfully process. The risk is not that a human is removed from the loop; it is that the human remains nominally in a loop they cannot read. Review that degrades into rubber-stamping is a control failure that presents as a control.

The third is an opportunity, and it is the organising idea of the standard. **An agent does not review periodically. It reviews continuously.** Where a conventional programme rescreens a relationship on a calendar — annually, or quarterly for higher risk — an agent rescreens on every list update, and can prove it did. **Detection latency**, the interval between a fact becoming true in the world and the obliged entity acting on it, falls from months to hours. And because every screening emits a signed, timestamped, hash-chained evidentiary record, the cadence is not asserted in a policy document but demonstrated to an auditor in seconds. An institution can evidence its own cadence internally; what it cannot do is hand a counterparty evidence that counterparty can verify without trusting it. Conventional assurance stops at the institution's boundary. These records cross it.

ACAS-1 specifies the **Compliance Step** — the evidentiary output of a single due-diligence act, with a uniform anatomy across every act — together with four **carriage classes** describing how different results can and cannot travel, a **step-type catalogue** anchored to the FATF Recommendations, a **continuous assurance** model built on detection latency and evidenced performance, a **determination model** recording where human judgment sits, and a **disclosure model** under which a scoped Presentation is constructed for one counterparty under a revocable mandate.

ACAS-1 creates no reliance right and discharges no obligation. It makes a counterparty's own diligence fast, evidenced, and current. The standard is published as a working paper for public comment, released CC0, with reference schemas and worked examples at the public repository.

IN ESSENCE

One. Continuous beats periodic, and provable beats claimed. A conventional programme rescreens a customer on a calendar. An agent rescreens on every list update and emits a signed record each time. The metric is detection latency — hours against months — and the evidence chain makes it auditable rather than asserted. A bank can show you a policy that says it screens daily. An agent can show you eight hundred and forty-seven signed executions and their maximum observed latency. That is the difference the standard exists to make legible.

Two. The unit is the Compliance Step. A due-diligence act is performed; a Step falls out of it. Every Step, of every type, has the same anatomy — the type, what was checked, what was obtained, who performed it, who determined it, and the evidence that makes it verifiable rather than merely asserted. Define that shape once and the whole of customer due diligence becomes a set of uniform records that any party can read.

Three. Different results travel in different ways. A verified identity is worth carrying. A sanctions screen is not — the recipient will re-run it in seconds and should. A source-of-funds enquiry cannot travel at all without disclosing what confidentiality and data-protection law require be withheld. Monitoring is not a past result but a live commitment. ACAS-1 therefore assigns each step type a **carriage class**: Portable, Referenced, Freshness Signal, or Subscription. A flat catalogue that treats them alike overstates the weak cases and undersells the strong ones.

Four. Detection is automated; determination is not. The standard automates the finding of facts and never the making of decisions reserved to a responsible person. Continuous screening surfaces more, faster, with the evidence pre-assembled. What it surfaces still goes to the human whose determination the rules require. The gain is not a shorter queue of decisions but a shorter interval before the right decision is possible.

Five. Nothing is published. A Compliance Record is held, not broadcast. What a counterparty receives is a **Presentation**: a signed subset, constructed for that counterparty, valid for a stated window, containing only what their profile requires. It is issued under a scoped and revocable disclosure mandate, and every Presentation emits an evidentiary record, so the subject can see precisely what was disclosed to whom.

Six. It is built on the stack, not beside it. A Compliance Step is a specialised AAS-1 evidentiary record with a compliance vocabulary and a determination model. Every subject, performer and determiner is an AIS-1 identity. The disclosure mandate is defined here, as a minimum object with five required properties that any existing authority format may satisfy. ACAS-1 adds the compliance layer and duplicates none of the others.

---

1. Motivation

1.1 Diligence that cannot travel

Customer due diligence is performed, at cost, inside an institution and stays there. When an agent presents itself to a counterparty it can present its identity — AIS-1 addresses that — but it cannot present its diligence. There is no portable, verifiable form in which work already completed can be carried and independently checked.

The consequence is that a counterparty cannot distinguish a diligenced agent from an undiligenced one. The searches an operator has already run, the beneficial-ownership determination it has already made and evidenced, the identity it has already verified to a stated standard — all are invisible to the party that would most benefit from seeing them. Every counterparty repeats the work, or does not, and neither answer is satisfactory.

The FATF Recommendations do contemplate this. Recommendation 17 permits a financial institution to rely on a third party for certain elements of customer due diligence. But reliance under R.17 is a bilateral arrangement: the relying institution must satisfy itself that the third party is regulated and supervised, must be able to obtain the underlying information immediately, and retains ultimate responsibility regardless. In practice it is negotiated, papered, and maintained between named counterparties. It works between two banks with a contract. It does not scale to an open network of agents meeting for the first time, and no amount of goodwill makes it scale, because the cost is in the bilateral negotiation rather than in the information transfer.

The information problem, however, is solvable. This is what this standard aims to address.

1.2 Review at a volume no human can read

Agent-to-agent commerce changes the arithmetic. Agents onboard counterparties, initiate and receive payments, and enter relationships at a rate set by machines rather than by business development. Every one of those relationships sits inside a customer-due-diligence obligation borne by a regulated person.

The risk this creates is widely misdescribed. It is not that agents will remove humans from compliance decisions. It is that the human will remain formally responsible for a volume of decisions they cannot meaningfully consider. A compliance function clearing a queue faster than it can read it has not automated anything; it has degraded into a rubber stamp, and a rubber stamp is a control failure that presents to an examiner as a control.

This standard is therefore not concerned with reducing the number of points at which a human determination is required. It is concerned with keeping those determinations meaningful when the surrounding volume multiplies — by ensuring that what reaches the responsible person is complete, evidenced, verified, and small enough to consider properly.

1.3 The opportunity: continuous assurance

The first two problems are defensive. The third is not.

A conventional due-diligence programme is periodic. Customer information is refreshed on a cycle — commonly annual for standard risk, more frequently for higher risk. Sanctions screening is better, and good practice rescreens the book on list update, but relationship review, source-of-funds enquiry, and adverse-media checking remain calendar-driven. A person added to a designated list in February may not be identified in a customer book until the following review cycle. The interval is real, it is measured in months, and it is invisible because nobody reports it.

An agent has no cycle. It screens on every list publication, monitors continuously, and evaluates against its rule set as often as its operator specifies. **Detection latency** — the interval between a fact becoming true in the world and the obliged entity acting on it — falls from months to hours.

More importantly, the agent can prove it. Every screening emits an evidentiary record under AAS-1: signed by the performing identity, independently timestamped, hash-chained to its predecessor. An auditor asking whether the cadence was actually maintained does not receive a policy document and a sample. It receives the complete execution history and verifies it cryptographically.

This is the categorical claim of ACAS-1 and it is worth stating precisely. Conventional compliance assurance is **assertion-based**: an institution states its programme and an examiner tests a sample against it. Agent compliance can be **evidence-based**: the programme's actual execution is the record, in full, verifiable by anyone holding it. Continuous monitoring is better than periodic monitoring. Provable continuous monitoring is a different thing altogether.

1.4 Agent assessing agent

Consider the case the standard is built for: one agent assessing another before transacting.

Knowing that the counterparty has a named responsible person establishes that accountability exists, which matters. But it does not advance the assessment. That person's determination is authoritative and not machine-resolvable: an assessing agent cannot query a name, read a judgment, or test whether it was well founded.

What the assessing agent can use is the work and its currency. The counterparty's identity verification, drawn from AIS-1 and evidenced to a stated assurance level. Its beneficial-ownership determination, made and evidenced, with the underlying data available on authorised request. Its screening programme — which list sets, what matching methodology, what maximum latency, and an evidenced execution history demonstrating that the stated cadence was in fact maintained. Its monitoring subscription, which will notify the assessing party if status changes after the assessment.

Given those, the assessing agent does one of two things. Where its own policy permits, it clears the counterparty directly. Where its policy or the applicable rules require a human determination, it verifies the carried Steps, runs whatever it must run itself, assembles the evidence, and places a complete package before the responsible person.

Either way the counterparty's completed work has travelled, been independently verified, and not been pointlessly repeated — and the human's attention has been spent on the determination rather than on the assembly.

1.5 What this standard does not do

Stated plainly, because the boundaries matter more than the capabilities.

ACAS-1 creates no reliance right. A Presentation is not a substitute for the recipient's own obligation and does not engage Recommendation 17. The recipient remains fully responsible for its own customer due diligence. What ACAS-1 offers is that the recipient's own diligence becomes fast, cheap, evidenced and current — not that it becomes unnecessary.

ACAS-1 does not automate determinations reserved to a person. Where the applicable rules require a responsible person to approve, assess or decide, that requirement is untouched. The standard records where the determination sat and what it covered; it does not relocate it.

ACAS-1 imposes no obligation of its own. Its authority is borrowed entirely from the frameworks it serves. It gives portable, verifiable form to obligations that national law already imposes on the regulated person.

ACAS-1 carries no suspicion. Nothing in the standard records, implies, or permits inference that a suspicious transaction or activity report (STR, or SAR in US and UK usage) has been made or contemplated. This is a schema constraint, not a policy preference, and it is addressed at §13.3.

2. Definitions

Term	Definition
AI Agent	A software system that pursues goals by perceiving its environment, selecting among available courses of action, and acting on that selection without a human determining each step. Autonomy is a matter of degree: an agent may act within a bounded mandate, under periodic supervision, or subject to specified human determinations, and remains an agent throughout. As defined in AIS-1.
Subject	The party whose diligence is evidenced — typically the agent presenting the record, or the natural or legal person on whose behalf it acts.
Compliance Step	The evidentiary output of one due-diligence act, carrying its type, inputs, result, performer, determiner, carriage class and evidence. The atomic unit of ACAS-1.
Compliance Record	The set of Compliance Steps held for a subject. Held, not published.
Presentation	A signed, scoped, audience-bound and time-limited subset of a Compliance Record, constructed for one counterparty under a disclosure mandate.
Carriage Class	How a given step type's result can travel: Portable, Referenced, Freshness Signal, or Subscription (§5).
Step Type	One of the standard categories of due-diligence act, anchored to the FATF Recommendations (§6).
Performer	The party that carried out the act — an agent or a human. Identified by AIS-1 identity.
Determiner	The party whose judgment stands behind the result at a given determination level (§8). Identified by AIS-1 identity. A natural person holds one as an AIS-1 Sponsor Card with `entity_type: individual` at `did:ais1:sponsor:{address}`, so a responsible person and a legal person are addressed identically.
Determination Level	Where the judgment supporting a Step sits: agent-determined, prepared-for-determination, person-determined, or independently-determined.
Prepared Package	A Step whose searches, evidence and form are complete and assembled, awaiting only the determination of the responsible person.
Detection Latency	The interval between a fact becoming true in an external source and the obliged entity's programme acting on it. The assurance metric of §7.
Monitoring Programme	A declared, evidenced continuous-assurance commitment: cadence, list sets, matching methodology, maximum latency, and disposition rule. Carried as a property of the programme, not of any person.
Disclosure Mandate	The scoped, revocable authority under which an agent may construct and issue Presentations (§9.1).
Evidence	The cryptographic or attestational material making a Step verifiable rather than asserted. Reuses the AAS-1 evidence vocabulary.
Canonicalisation	Deterministic serialisation prior to hashing or signing. ACAS-1 specifies JCS (RFC 8785), matching the rest of the stack.
RFC 3339	The internet date-and-time format (e.g. `2026-07-31T14:32:11Z`) used for all timestamps.

3. The ACAS-1 Standard

3.1 The Compliance Step

ACAS-1 defines the Compliance Step as the fundamental unit of agent compliance. A Step is **the evidentiary output of a due-diligence act**, in precisely the sense that an AAS-1 Class A record is the evidentiary output of an agent action.

The distinction matters and was insufficiently clear in v0.1. Nobody performs a Step. A party runs a screen, verifies an identity, makes a beneficial-ownership determination — and a Step falls out of that act as its record. The `inputs` and `result` fields describe the act; the Step itself is the output. The emission model is identical to AAS-1's, and this is what makes ACAS-1 a layer on that standard rather than a parallel one.

Every Step, of every type, shares one anatomy, specified in full at §4:

- a **type** — which due-diligence obligation the act addresses
- the **inputs** — what was searched or checked
- the **result** — what was obtained
- the **performer** — who carried it out, by AIS-1 identity
- the **determiner and determination level** — whose judgment stands behind it (§8)
- the **carriage class** — how this result may travel (§5)
- the **evidence** — what makes it verifiable rather than asserted

A Step is portable in the narrow sense that any party holding it and the referenced AIS-1 identities can validate its signature, read its result, check its evidence and assess its currency. Whether the *result* is useful to that party is a separate question, and is what the carriage classes answer.

3.2 The Compliance Record

A Compliance Record is the set of Compliance Steps held for a subject. It is not a new container type and it is not a file assembled about a person: it is simply the Steps that resolve for that subject, held by the subject or its operator.

A Compliance Record composes. Steps are added as diligence is performed, superseded as determinations are upgraded, and refreshed as monitoring executes. It is never published, never broadcast, and never handed over whole. What leaves is a Presentation.

3.3 The Presentation

A Presentation is what a counterparty actually receives: a signed object containing a subset of the subject's Steps, constructed for that counterparty, for a stated purpose, valid for a stated window.

A Presentation carries its own scope and expiry independent of the Steps inside it. A Step may remain current while the Presentation containing it has lapsed; a Presentation issued to one counterparty is not valid if replayed by another. This is the same relationship as between a credential and a presentation of it, and implementers familiar with that model will find nothing surprising here.

Presentations are constructed under a disclosure mandate and emit an evidentiary record on issue. The full model is at §9.

3.4 Completeness

A Compliance Record is **complete for a given profile** (§16) when it contains every step type that profile requires, each current and each determined to at least the level the profile demands.

Completeness is well-defined precisely because the catalogue is standard: an assessing party knows which types to expect and can identify what is missing. An incomplete record is not invalid — it is incomplete, and the assessing party sees exactly which Steps are absent, which have lapsed, and which are determined below the level its policy requires.

4. The Compliance Step Primitive

4.1 Anatomy

Attribute	Description	Required
`acas`	Standard version. `"0.1"`.	Yes
`stepId`	ULID or UUID, unique within the issuer.	Yes
`subjectRef`	AIS-1 identity of the party this Step evidences.	Yes
`type`	The step type from the catalogue (§6).	Yes
`carriage`	The carriage class of this Step (§5). Declared, not inferred.	Yes
`inputs`	What was searched or checked (§4.2).	Yes
`result`	What was obtained (§4.2).	Yes
`performedBy`	AIS-1 identity of the performer, agent or human.	Yes
`performedAt`	RFC 3339 timestamp of performance.	Yes
`determination`	Determination object: level and determiner (§8).	Yes
`programme`	Monitoring-programme object (§7.3). Required for Subscription-class Steps.	Conditional
`performance`	Evidenced execution history (§7.3). Required for Subscription-class Steps.	Conditional
`disclosure`	Authorised-request endpoint and material hash. Required for Referenced-class Steps (§9.3).	Conditional
`evidence`	Array of evidence entries (§4.3). Minimum one.	Yes
`validUntil`	RFC 3339. When this Step ceases to be current (§4.4).	Yes
`supersedes`	`stepId` of a prior Step this one replaces.	Optional
`aas1RecordRef`	URI of the AAS-1 evidentiary record emitted for this Step.	Yes
`signature`	Signature object over the canonicalised Step.	Yes

Two attributes are load-bearing and easily overlooked. `carriage` is declared explicitly rather than inferred from `type`, so that a verifier's handling is driven by the Step itself and profiles may constrain carriage independently. `validUntil` is required rather than optional: a Step without an expiry makes an implicit claim of permanence that no due-diligence result supports.

4.2 Inputs and results

The `inputs` and `result` objects are what make a Step evidenced work rather than a bare assertion. Their internal fields are type-specific (§6.3) but both follow a common pattern.

Inputs record what was checked: the query or subject data, the data source or list set consulted by reference, and — where the subject data is drawn from AIS-1 — the identity reference rather than a restated copy. Sensitive underlying values are carried by hash wherever the result can be verified without exposing them.

Result records the outcome: a normalised outcome code, the material obtained, and any determination reached. The result is what a counterparty reads; the evidence is what allows them to trust it; the carriage class is what tells them how far they may rely on it.

4.3 Evidence

Evidence is technology-neutral and reuses the AAS-1 evidence vocabulary, so a Step's evidence verifies with the same tooling as any AAS-1 record. Recognised types: `signature`; `attestation` (an execution-environment or provider attestation); `witness` (an independent co-signer); `log` (an append-only reference to the act performed); `hash_anchor` (a content hash anchored to a ledger or notary); and `human` (an attestation by a responsible person, Commissioner for Oaths, or other authorised individual).

A Step may carry several entries. A screening result typically carries a `log` of the execution and an `attestation` from the screening provider; a Subscription-class Step additionally carries a `hash_anchor` over its performance chain.

4.4 Currency and supersession

Every Step expires, and different types expire at very different rates. `validUntil` is required and its appropriate interval follows from the carriage class:

Carriage class	Typical currency	Rationale
Portable	12–36 months	Verified identity and ownership determinations are durable but not permanent
Referenced	12 months	The enquiry ages; the referenced material may be re-requested
Freshness Signal	24 hours – 90 days	The entire value of the Step is its recency
Subscription	Continuous while the subscription is live; lapses immediately on termination	The commitment, not the result, is what is current

A verifier **MUST** treat a Step past its `validUntil` as requiring refresh, not as clear. Profiles may set shorter intervals; none may set longer than the standard's maximum for the class.

A Step is never edited. Where a result changes, a determination is upgraded, or a monitoring window closes, a new Step is issued with `supersedes` pointing at its predecessor. The chain is the history and is itself evidence.

---

5. Carriage Classes

5.1 Why a flat catalogue fails

It is tempting to enumerate the step types as though each travelled the same way. That assumption does not survive contact with practice, and it fails in both directions.

A verified identity is genuinely worth carrying: the verification was slow and expensive, the result is durable, and a recipient gains real value from not repeating it. A sanctions screen is not worth carrying in the same sense: the recipient can and will re-run it in seconds, and a carried result of "clear" — necessarily stripped of the name that would let the recipient validate it — is not something any competent compliance function would rely on. A source-of-funds enquiry cannot travel at all in its substance, because what makes it meaningful is exactly the material that confidentiality and data-protection law require be withheld. And ongoing monitoring is not a result at all: a past search says nothing about a live relationship.

Treating these alike overstates the weak cases, which invites well-founded criticism, and undersells the strong ones, which wastes the standard's best material. ACAS-1 therefore declares the carriage class on every Step.

5.2 The four classes

Portable. The result itself travels and has standalone value to the recipient. The underlying work is costly, the result is durable, and the evidence permits independent verification without disclosing anything the subject has not consented to

disclose. The recipient may take the result into its own assessment on its own policy.

Referenced. The *fact* of the act travels — that it was performed, by whom, when, against what scope, to what outcome, with a cryptographic hash of the underlying material. The material itself does not travel. A recipient with authorisation requests it through the declared disclosure endpoint and verifies that what it receives hashes to the carried value. This is how a substantive enquiry can be proved to have occurred, and its integrity guaranteed, without disclosure.

Freshness Signal. The result carries little independent weight and the recipient is expected to re-perform the act. What travels is the existence, scope and recency of the subject's own programme: which list sets, what matching methodology, when last executed. This is a risk signal about the counterparty's compliance posture — a counterparty screening hourly against a comprehensive list set with documented matching is a different proposition from one that has never screened — and it is not a substitute for the recipient's own screening.

Subscription. Nothing meaningful travels as a past result. What travels is a live commitment — a declared monitoring programme with evidenced execution history — and an endpoint the recipient may subscribe to for notification of status change. The value is prospective rather than retrospective: not *this subject was clear in May* but *this subject is under continuous monitoring, here is the proof of cadence, and you will be told within the stated latency if that changes.*

5.3 Class assignment

Step type	Carriage class	What actually travels
`identity_verification`	Portable	The verification result, its assurance level, and the standard applied
`beneficial_ownership`	Portable + Referenced	The determination travels; the underlying ownership data is referenced and requestable
`purpose_and_nature`	Portable	The stated purpose and any risk classification. Low sensitivity, declared by the subject
`source_of_funds`	Referenced	Scope, date, outcome, and a hash of the material examined. The material is requestable under authorisation
`sanctions_screening`	Freshness Signal	List set, matching methodology, last execution, latency. The recipient re-screens
`pep_screening`	Freshness Signal	Source, methodology, last execution. The recipient re-screens
`ongoing_monitoring`	Subscription	Declared programme, evidenced performance, change-notification endpoint

A profile **MAY** require a stricter carriage class than the default — requiring, for instance, that beneficial ownership be Referenced rather than Portable in a jurisdiction whose ownership register is not public. A profile **MUST NOT** relax one.

5.4 Reserved: Proved carriage

A fifth class, **Proved**, is reserved and not specified in v0.1. It is recorded here because the four classes above leave a gap that is worth naming.

The gap is this. A Freshness Signal exists because a screening result stripped of the identity it was run against cannot be validated by the recipient, who must therefore re-perform the act. A Referenced Step exists because substantive material cannot be disclosed. In both cases the recipient is asked either to redo work or to accept an assertion. A zero-knowledge proof would close both: it can establish that a stated computation was performed over a stated input — *this subject was screened against list version L at time T with no match above threshold θ* — while disclosing neither the subject nor the underlying data. What the recipient verifies is the proof rather than the work.

Four constraints determine whether this is useful, and all four are open:

- **A proof establishes computation, not truth.** It can show a screen was executed correctly. It cannot show that the identity data supplied to it was genuine. Trust moves to whoever attested the inputs; it does not disappear, and a proved Step

would still depend on the identity Steps beneath it.

- **Fuzzy matching is the hard case.** Sanctions screening is not set membership. It is fuzzy matching across aliases, transliterations and date ranges, and expressing that faithfully inside a proving system is both expensive and disclosive — the matching function becomes a public parameter. Clean predicates (jurisdiction, licence held, age threshold, non-membership of a committed set) are tractable today; name matching is a research problem.
- **A supervisor must always be able to look.** Record-keeping obligations require underlying information to be available to competent authorities, and financial intelligence units must receive actual data. A scheme in which the obliged entity genuinely cannot produce the underlying material is not compliant. Proved carriage is therefore necessarily **opaque to the counterparty and open to the supervisor**, via viewing keys or selective opening. That asymmetry is the design, not a concession to it.
- **Silence remains a signal.** A proof that stops being produced discloses something. The inference channels at §13.3 apply with equal force.

The near-term path is more likely to be selective-disclosure signatures over already-signed credentials than general-purpose proving systems, which is also the direction the digital-identity wallet standards have taken. v0.1 therefore reserves the class name and the enum value, and specifies neither the predicate catalogue nor a proving system. Implementations **MUST NOT** claim Proved carriage against this version.

---

6. The Step-Type Catalogue

6.1 The FATF anchor

The catalogue is anchored to the FATF Recommendations as given effect in national law. FATF issues Recommendations and assesses implementation through mutual evaluation; the obligations that bind a regulated person are those enacted in its own jurisdiction. References throughout this document are to the Recommendations as the common source of those national obligations, not as a directly binding instrument.

Recommendation 10 is the spine. It supplies four of the seven types. The remainder come from distinct obligations that customer due diligence sits alongside rather than within — which is itself worth stating, because sanctions screening in particular is routinely and incorrectly described as a CDD obligation.

Recommendation	Obligation	Position in ACAS-1
R.10	Customer due diligence: (a) identify and verify the customer; (b) identify and verify the beneficial owner; (c) understand the purpose and intended nature of the relationship; (d) conduct ongoing due diligence	**Four step types**
R.11	Record-keeping, five years minimum	Served structurally — Steps are signed, timestamped, retained and independently re-verifiable
R.12	Politically exposed persons: identification, senior management approval, source of wealth and funds, enhanced ongoing monitoring	`pep_screening` and `source_of_funds`
R.6 / R.7	Targeted financial sanctions — terrorism and proliferation financing	`sanctions_screening`. Not an R.10 obligation
R.15	New technologies; virtual asset service providers	Context for the applicable profile, not a step type
R.16	Originator and beneficiary information for transfers	ARS-1, not ACAS-1
R.17	Reliance on third parties for R.10(a)–(c)	Addressed at §13.2. ACAS-1 creates no reliance right
R.20 / R.21	Suspicious transaction reporting; prohibition on tipping off	**Deliberately out of scope.** See §13.3
R.22 / R.23	Application of R.10 and related measures to DNFBPs	The same step set under a different profile
R.24 / R.25	Beneficial ownership transparency of legal persons and arrangements	The source feeding `beneficial_ownership`

6.2 The seven types

Type	Anchor	Carriage	What the Step evidences
`identity_verification`	R.10(a)	Portable	The subject's identity has been verified to a stated standard. Draws identity data from AIS-1 rather than restating it
`beneficial_ownership`	R.10(b); sourced from R.24/25	Portable + Referenced	The beneficial owners of the subject's sponsor entity — the legal person behind the agent — have been identified and verified
`purpose_and_nature`	R.10(c)	Portable	The purpose and intended nature of the business relationship has been established and recorded
`ongoing_monitoring`	R.10(d)	Subscription	A declared, evidenced continuous monitoring programme is live over the relationship
`sanctions_screening`	R.6 / R.7	Freshness Signal	The subject is screened against a named list set under a declared methodology, with stated latency
`pep_screening`	R.12	Freshness Signal	The subject is screened for PEP status against a named source under a declared methodology
`source_of_funds`	R.10 (enhanced); R.12	Referenced	The source of the subject's funds, and where required wealth, has been established and evidenced

6.3 Per-type requirements

Each type constrains its `inputs` and `result` so a Step of that type is meaningful and comparable across issuers. The normative field lists are in the schema; in summary:

- **`identity_verification`** — `inputs` reference the AIS-1 identity and the verification method and standard applied; `result` carries `verified` or `insufficient` and the assurance level attained.
- **`beneficial_ownership`** — the subject of this Step is the agent's **sponsor entity**, not the agent: an agent has no beneficial owners of its own, and the ownership that matters is that of the legal person accountable for it under its AIS-1 bond. `inputs` reference the sponsor entity and the ownership data source; `result` carries the verification outcome and the identified owners by reference or hash, never in clear. `disclosure` supplies the authorised-request endpoint. Where the sponsor is a natural person, the Step records that fact and no further ownership enquiry arises.
- **`purpose_and_nature`** — `inputs` carry the stated purpose; `result` records it with any risk classification.
- **`ongoing_monitoring`** — `programme` and `performance` are required (§7.3); `result` carries the current status and the subscription endpoint. `inputs` and `result` carry no per-execution detail; the evidence chain does.
- **`sanctions_screening`** — `inputs` carry the `listSetRef`, the matching methodology and threshold, and the execution time; `result` carries `clear`, `match` or `review`. A `match` or `review` outcome halts reliance on that limb pending determination.
- **`pep_screening`** — `inputs` carry the source and methodology; `result` carries `clear`, `match` or `review` and, on a hit, the classification by reference.
- **`source_of_funds`** — `inputs` carry the scope of the enquiry and the categories of material examined; `result` carries the established source at category level and an outcome; `disclosure` supplies the endpoint and the hash of the material.

6.4 Extension types

Implementations **MAY** define additional types under a reverse-DNS namespace (for example `com.example.adverse-media`) for sector- or jurisdiction-specific acts not in the core catalogue. An extension type **MUST** declare a carriage class. Assessing parties **MAY** reject unknown types.

The core catalogue is deliberately small and anchored. Extensions carry the long tail without diluting the comparability of the core.

---

7. Continuous Assurance

This section is the organising claim of the standard.

7.1 Detection latency

Conventional due-diligence programmes are periodic. Customer information is refreshed on a cycle. Screening is better — good practice rescreens the book on list update — but relationship review, source-of-funds enquiry and adverse-media checking remain calendar-driven, and the cycle is measured in months.

The consequence is an interval that is real, material, and almost never measured: the time between a fact becoming true in the world and the obliged entity's programme acting on it. ACAS-1 names this **detection latency** and makes it the assurance metric.

Latency is the right metric for three reasons. It is **measurable** — an interval in hours, not a maturity rating. It is **comparable** — the same number means the same thing across institutions, sectors and jurisdictions. And it is **the number that actually determines outcomes** — the harm from a sanctions exposure is a function of how long the exposure persisted undetected, not of how thorough the eventual review was.

An agent-operated programme executing on every list publication achieves a latency measured in hours. A quarterly review cycle achieves one measured in months. The difference is not marginal and it is not rhetorical.

7.2 Provability

Frequency is the smaller half of the claim.

A conventional institution can evidence its own cadence, and it is worth being precise that it can. Scheduler logs, batch records, system reports and internal audit testing are real evidence, and a supervisor or auditor with access to the institution's systems can examine them properly. The limitation is not that the evidence is absent.

The limitation is that the evidence is **not portable**. It sits inside the institution's perimeter; it is interpretable only with access and context; and it is produced and retained by the same party whose programme is in question. A counterparty cannot obtain it, and could not independently verify it if they could. What reaches a counterparty is therefore an assertion — however well founded that assertion is internally.

An agent emitting an AAS-1 record on every execution produces evidence that is portable by construction. Each record is signed by the performing AIS-1 identity, independently timestamped, and hash-chained to its predecessor. A counterparty — not only a supervisor exercising access rights — receives the complete execution history, with omission, reordering and substitution all cryptographically detectable, and verifies it in seconds without trusting the party that produced it.

The distinction is therefore not that one party has evidence and the other does not. It is that **conventional assurance produces evidence for itself, and this produces evidence for anyone.** Compliance assurance today terminates at the institution's boundary. These records cross it.

An institution can tell a counterparty what its programme is. An agent can show them what its programme did.

7.3 The monitoring programme object

The material consequence of §7.1 and §7.2 is that continuous assurance is expressible as a **property of the programme rather than of any person**. This resolves what would otherwise be the hardest carriage problem in the standard: what travels contains no personal data at all.

A Subscription-class Step carries:

```
"programme": {
  "cadence": "on_list_update",
  "maxLatency": "PT4H",
  "listSetRefs": ["https://compliance.example.com/lists/un-ofac-eu-hmt"],
  "matching": {
    "method": "fuzzy",
    "threshold": 0.85,
    "providerRef": "did:ais1:sponsor:screening-provider-example"
  },
  "disposition": "human_required_on_hit",
  "policyRef": "https://operator.example.com/policies/monitoring/v4"
},
"performance": {
  "window": "P90D",
  "executions": 847,
  "expectedExecutions": 841,
  "maxObservedLatency": "PT3H12M",
  "meanObservedLatency": "PT41M",
  "missedWindows": 0,
  "evidenceChainRef": "aas1:chain/01K1ACAS...",
  "chainHead": "sha256-4f3edf..."
}
```

No name. No identifier of any natural person. No subject data of any kind. The entire object describes what the programme is and what it demonstrably did, and it is fully verifiable by a recipient who fetches the referenced evidence chain and

recomputes it.

`expectedExecutions` against `executions`, and `missedWindows`, are required precisely because they are the fields a hostile reviewer would ask for. A programme claiming continuous coverage should be able to show that it did not silently stop.

7.4 Detection and determination

Continuous assurance automates the **finding of facts**. It does not automate the **making of decisions**.

The separation is load-bearing and is the reason the model is compliance-positive rather than compliance-reducing. Screening is inexpensive; dispositioning what screening surfaces is the expensive part, and it is the part that the applicable rules reserve to a responsible person. Increasing screening frequency by two orders of magnitude increases what is surfaced. If an agent then auto-cleared those results, the programme would have relocated a reserved determination to a machine, which this standard does not do and does not permit implementations to do while claiming conformance.

The `disposition` field in the programme object is therefore normative, not descriptive. A conformant Subscription-class Step **MUST** declare its disposition rule, and a rule of `auto_clear_on_hit` is non-conformant for any step type whose determination the applicable profile reserves to a person.

What the model actually delivers is this: the responsible person's determination is unchanged in nature and unchanged in authority, but it arrives at a genuine hit within hours rather than months, with the evidence already assembled and the false positives already reduced by declared matching. The determination is not removed. It is made earlier, on better material, and less often on noise.

7.5 Match quality

Frequency without match quality is theatre, and a standard that carried cadence alone would deserve the criticism it received. Screening daily against a stale list set with naive exact-match logic is a worse control than screening quarterly with well-tuned fuzzy matching and disciplined disposition.

The `matching` object is therefore required in every declared programme: method, threshold, and provider. A recipient assessing a counterparty's programme reads cadence and matching together, and a programme declaring hourly execution with unstated matching should be assessed as unevidenced, not as strong.

Profiles **MAY** set minimum matching requirements. Where a profile does so, a programme below that minimum is non-conformant for that profile regardless of its latency.

7.6 The cost of continuous screening

Continuous execution has a cost that periodic execution does not, and an operator declaring a four-hour latency is committing to pay it. The standard takes no position on the commercial model, but three points bear on whether the commitment is credible.

Cost per execution is falling and the shape of the bill is changing. Conventional screening is priced per customer per period under enterprise contracts negotiated for a book of known size. Continuous execution inverts the assumption: many small, machine-initiated queries rather than few large batch runs. Where a provider prices per query, high cadence is expensive; where it prices per list delta evaluated, it is not, because a list update touching no monitored subject is nearly free to evaluate. Operators declaring aggressive cadence should expect to negotiate on that basis rather than on volume.

An agent that pays for its own searches needs the means to pay. Where screening is metered, the performing agent requires either a funded account held by its operator or, in the machine-to-machine case, its own settlement capability — which is a settlement and delegated-authority concern rather than an ACAS-1 one. The spending authority is its own mandate: bounded by amount, counterparty and purpose, revocable, and emitting an evidentiary record on every disbursement. ACAS-1 requires only that the resulting execution be evidenced; how it was paid for is out of scope.

Provider integration is the practical constraint. An agent can only screen at machine cadence against providers exposing a machine interface — an API, a command-line tool, or a Model Context Protocol server. Coverage of the major list-set providers is uneven and changing, and an operator should verify it before committing to a `maxLatency` it cannot meet. A declared programme the operator cannot execute is worse than a modest one it can: `missedWindows` is a required field precisely so that the gap is visible rather than silent.

7.7 What continuous assurance does not claim

Three limits, stated because they will otherwise be found and stated for us.

No regulatory credit is claimed. No supervisory framework presently rewards a four-hour detection latency over a ninety-day one, and none provides a mechanism to recognise it. The immediate value of continuous assurance is commercial and evidentiary: a counterparty can price it, an auditor can verify it, and a supervisor can examine it. Whether it becomes an expected standard is a matter for supervisors and is not asserted here.

Continuous processing is still processing. Screening a natural person continuously is more intrusive than screening them annually, and requires a lawful basis for each processing operation. An obliged entity screening its own customer under a legal obligation is on firm ground. An assessing party screening a counterparty's beneficial owners may not be. See §13.4.

Latency is not the only dimension. A programme with excellent latency, poor list coverage and untuned matching is a poor programme. Latency is proposed as the missing metric, not the only one.

---

8. The Determination Model

8.1 The four levels

Every Step carries a `determination` object recording a level and a determiner. These levels are not a ladder of decreasing human involvement, and should not be read as one. They do not measure how little human judgment was applied. They record **where the judgment sits and what it covered**, which is what a recipient needs in order to apply its own policy.

Level	Meaning	Determiner
`agent_determined`	An agent performed the act and its result stands on the evidence carried, in a case where no person's determination is reserved	The performing agent
`prepared_for_determination`	An agent performed the act and assembled a complete package; the reserved determination has not yet been made	The performing agent; the responsible person identified, not yet signed
`person_determined`	A responsible person has made the determination, typically by considering a prepared package	The determining person
`independently_determined`	An independent third party — an auditor, a regulated verifier — has determined the result	The independent determiner

8.2 Where the determination sits

A recipient reading a Step needs to answer one question: *whose judgment stands behind this, and is that sufficient for my purposes?* The level answers it directly.

An `agent_determined` sanctions screen tells the recipient that a machine executed a search against a declared list set with declared matching, and that no reserved determination was engaged because none was required — the result is a fact, not a judgment. A `person_determined` beneficial-ownership Step tells the recipient that a named responsible person considered the evidence and reached a conclusion. An `independently_determined` identity verification tells the recipient that a third party with its own regulatory standing has vouched, which may allow the recipient's own policy to require less of its own function.

None of these transfers the recipient's obligation. All of them inform how the recipient discharges it.

8.3 The prepared package

`prepared_for_determination` is where most of the operational value of the standard sits, so its requirements are normative. Such a Step **MUST** carry, in addition to the standard anatomy:

- the completed `inputs` and `result` — the acts performed and their outcomes;
- the assembled `evidence` — everything the determiner requires to reach a conclusion;
- the identified responsible person, by AIS-1 identity, whose determination is awaited;
- a populated form reference where the applicable profile specifies a form.

The test of conformance is simple and strict: **if the responsible person must go and perform an act the agent could have performed, the package was not conformant.** Their attention is for the determination, not the assembly.

On determination, a superseding Step is issued at `person_determined` with a `human` evidence entry carrying the determiner's signature and `supersedes` pointing at the prepared Step. The prepared Step is not deleted; the pair is the record of what was put before the person and what they decided.

---

9. Disclosure and Consent

9.1 The disclosure mandate

An agent does not decide for itself what to disclose about its subject. It acts under a **disclosure mandate**: a scoped, revocable grant from the subject or its sponsor specifying which step types may be presented, to which classes of counterparty, for what purpose, and for how long.

Within the mandate the agent constructs and issues Presentations without seeking case-by-case authorisation. This is necessary: a model requiring per-request human consent does not survive machine-speed commerce, and would reintroduce precisely the bottleneck this standard exists to remove.

The obvious hazard is that a standing grant is an unlock. The controls are that the mandate is **narrow** — enumerated step types, enumerated counterparties, a stated purpose, a stated expiry; that it is **revocable** with immediate effect; and that it is **observed** — every Presentation emits an evidentiary record, so the subject can see exactly what was disclosed, to whom, and when. The subject's protection is not a consent prompt they will stop reading. It is a narrow grant, a working revocation, and a complete log.

Attribute	Description	Required
`mandateId`	ULID or UUID.	Yes
`grantorRef`	AIS-1 identity of the subject or its sponsor — the party whose diligence may be disclosed.	Yes
`granteeRef`	AIS-1 identity of the agent authorised to construct Presentations under this mandate.	Yes
`stepTypes`	Enumerated step types that may be presented. No wildcard.	Yes
`audiences`	Enumerated counterparties or counterparty classes to which Presentations may be issued.	Yes
`purposes`	Enumerated purposes for which disclosure is permitted.	Yes
`notAfter`	RFC 3339. The mandate's own expiry.	Yes
`statusEndpoint`	Resolvable endpoint returning current mandate status.	Yes
`signature`	Signature object over the canonicalised mandate, by the grantor.	Yes

Five properties are required of any disclosure mandate, whatever object expresses it:

1. the scope is **enumerated** rather than open — no wildcard step types, audiences or purposes;
2. the **grantor and grantee are named identities**, resolvable and verifiable;
3. the **purpose is stated**, and constrains the recipient's onward use;
4. there is an **expiry**; and
5. **revocation status is independently resolvable** by a verifier, without the grantee's cooperation.

A grant lacking any of these is not a conformant disclosure mandate, and a Presentation issued under it **MUST** be rejected.

ACAS-1 specifies the minimum object above so that the standard is implementable on its own. Where an operator already runs a general delegated-authority framework — a capability or authorisation token scheme, a verifiable credential with a resolvable status list, or a dedicated agent authority standard — the disclosure mandate **MAY** be expressed within it and referenced by `mandateRef`, provided the five properties hold and status resolves. **The standard constrains the properties, not the format.**

Implementers profiling an existing scheme should attend to properties 3 and 5 in particular. Most capability and authorisation formats carry scope but not purpose, and several have revocation mechanisms that are not reliably queryable by a third party. Both usually require a profile rather than being satisfied as they stand.

9.2 Constructing a Presentation

On request, the agent constructs a Presentation containing only the Steps that the requesting counterparty's stated profile requires and the mandate permits.

Attribute	Description
`acas`	Standard version
`presentationId`	ULID or UUID
`subjectRef`	AIS-1 identity of the subject
`audienceRef`	AIS-1 identity of the counterparty this Presentation is constructed for
`purpose`	The stated purpose for which disclosure is made
`profile`	The profile being tested against
`mandateRef`	The disclosure mandate under which this Presentation is issued (§9.1)
`steps`	The included Steps, by reference, with type, carriage class and determination level
`completeFor`	The profile for which this Presentation asserts completeness, or null
`assurance`	What this Presentation does and does not establish (§9.2.1). Required
`issuedAt` / `expiresAt`	RFC 3339. The Presentation's own validity window
`aas1RecordRef`	The evidentiary record emitted on issue
`signature`	Over the canonicalised Presentation

A Presentation is **audience-bound**: a verifier **MUST** reject one whose `audienceRef` is not itself. It is **time-bound** independently of the Steps within it. And it is **purpose-bound**: the stated purpose constrains the recipient's onward use and is the record of the basis on which disclosure was made.

9.2.1 The assurance object

§13.2 states in prose that ACAS-1 creates no reliance right. Because a Presentation is a machine-read artefact, the point is also carried in the object itself:

```
"assurance": {
  "relianceBasis": "none",
  "recipientObligation": "undischarged",
  "statementRef": "https://acas-1.org/no-reliance/v1"
}
```

`relianceBasis` is normative and single-valued in v0.1. This is deliberately stronger than a disclaimer: a conforming Presentation **cannot** assert that it establishes a third-party reliance arrangement, because the format provides no way to say so. Any future support for a genuine reliance arrangement widens the enum under a named profile, explicitly, never by silence. A verifier **MUST NOT** treat a Presentation as discharging its own obligation, whatever the issuer intended.

Two things this object is not. It is **not a liability disclaimer**: the issuer's responsibility for the accuracy of the Steps it signs is a matter for its terms of business and is deliberately outside this standard — a Step nobody stands behind has no value, and the standard does not invite issuers to disclaim their own work. And it is **not boilerplate to be skipped**: it is the field that forecloses a recipient later asserting it was told it was covered.

9.3 Referenced substance and authorised request

For Referenced-class Steps the substance does not travel. The Step carries a `disclosure` object:

```
"disclosure": {
  "endpoint": "https://disclosure.operator.example.com/acas/steps/01K1...",
  "materialHash": "sha256-a3f81c...",
  "hashAlg": "SHA-256",
  "requiresAuthorisation": true,
  "authorisationScheme": "acas1-disclosure-mandate"
}
```

A recipient requiring the underlying material requests it at the endpoint, presenting its own identity and the authorisation its request requires. If disclosure is granted, the recipient verifies that what it receives hashes to `materialHash` — which establishes that the material is exactly what was examined at `performedAt`, and has not been assembled or amended since.

This is what allows a substantive enquiry to be **proved to have occurred, and proved to be intact**, without being disclosed. It is the answer for source of funds, and it generalises to any material that cannot travel in clear.

9.4 Revocation

Revocation of a disclosure mandate takes effect immediately and prospectively. It prevents further Presentations. It cannot recall Presentations already issued, which is why `expiresAt` matters: a Presentation's window is the outer bound of the exposure a revocation cannot reach, and profiles should set it as short as the use case tolerates.

Implementations **MUST** publish mandate status at a resolvable endpoint and **SHOULD** support a status-check at verification time. A verifier presented with a Presentation whose mandate has been revoked **MUST** reject it even if the Presentation is within its own validity window.

---

10. Schema Specification

10.1 JSON Schemas

The Compliance Step schema is published as JSON Schema 2020-12 in the repository under `schemas/`, with per-type constraints on `inputs` and `result` and conditional requirements driven by `carriage`. The Presentation schema is published alongside it. Both are normative for v0.1.

10.2 Canonicalisation and hashing

Steps and Presentations **MUST** be canonicalised before hashing or signing. v0.1 specifies JCS (RFC 8785) as the default canonicalisation — the deterministic JSON serialisation used across AIS-1, AAS-1, AIPS-1, ARS-1 and AES-1 — so that independent parties compute identical bytes. The hash algorithm is declared per-record in the signature object; SHA-256 is the default. Implementations **MAY** use other algorithms via `hashAlg`; verifiers **SHOULD** reject unknown algorithms unless present in a published registry.

10.3 Signature object

Field	Description
`alg`	Signature algorithm identifier (EdDSA, ES256K, etc.)
`hashAlg`	Hash algorithm. Default SHA-256
`canonicalisation`	Canonicalisation method. Default JCS
`keyRef`	Verification method identifier within the signer's AIS-1 identity document
`value`	Signature value, base64url-encoded

Structurally identical to the AIS-1, AAS-1, AIPS-1, ARS-1 and AES-1 signature objects — shared verification tooling across the stack.

---

11. AIS-1 and AAS-1 Binding

ACAS-1 is built on identity and evidence, and duplicates neither.

Identity (AIS-1). Every `subjectRef`, `performedBy`, determiner and `audienceRef` is an AIS-1 identity. An `identity_verification` Step draws the subject's identity data from AIS-1 rather than restating it: the licence, sponsor and status a sponsor already holds in its AIS-1 bond are referenced, not copied, and ACAS-1 maintains no parallel licence record. A verifier resolves any identity via the AIS-1 §7.1 resolution algorithm and **MAY** confirm a bond is active via `verifyBond(bondId)`.

Evidence (AAS-1). A Compliance Step is a specialised AAS-1 evidentiary record. Every Step emits an AAS-1 Class A record at issuance (`aas1RecordRef`), every Presentation emits one on issue, and the evidence array uses the AAS-1 vocabulary throughout. The evidence chain underpinning §7.2 is an AAS-1 chain: it is AAS-1's `prevHash` construction that makes omission, reordering and substitution detectable, and therefore AAS-1 that makes provable cadence possible at all.

Authority. ACAS-1 defines the disclosure mandate it requires (§9.1) as a minimum object with five required properties, so that the standard is implementable standing on identity and evidence alone. Where an operator runs a general delegated-authority framework, the mandate may be expressed within it provided those properties hold.

The relationship is precise: **AAS-1 records what an agent did. ACAS-1 is the subset of that activity which is due-diligence work, given a compliance vocabulary, a carriage model, a determination model and a disclosure model.**

---

12. Presenting and Verifying

A subject's agent presents to a counterparty over AIPS-1, alongside an ARS-1 message, or directly. The counterparty verifies as follows.

1. **Resolve** the subject's AIS-1 identity and confirm the bond is active.

2. **Check the Presentation** — that `audienceRef` is the verifier, that it is within `issuedAt` / `expiresAt`, and that its `mandateRef` has not been revoked.
3. **Verify each Step** — validate the signature against the performer's or determiner's AIS-1 verification method, check the evidence, and confirm the Step is within `validUntil`.
4. **Read carriage before result.** For Portable Steps, take the result into the assessment. For Referenced Steps, decide whether the underlying material is required and request it if so. For Freshness Signal Steps, read the programme as a risk signal and re-perform the act. For Subscription Steps, verify the performance chain and subscribe.
5. **Assess completeness** against the profile being tested — which required types are present, current and sufficiently determined.
6. **Assess determination levels** against the verifier's own policy.
7. **Decide.** Where policy is satisfied, clear the subject. Where a reserved determination is required, assemble a prepared package from the verified Steps and place it before the responsible person.

Step 4 is the one implementers most often get wrong. A verifier that reads results without reading carriage will over-rely on screening results and under-use monitoring subscriptions — exactly inverting the value on offer.

---

13. The Regulatory Substrate

ACAS-1 asserts no obligation of its own. Its authority is borrowed entirely from the frameworks it serves.

13.1 Frameworks served

Regime	What it requires	What ACAS-1 carries
FATF Recommendations, as enacted nationally	Customer due diligence, PEP measures, targeted financial sanctions, record-keeping	The completed acts as evidenced, current, carriage-classified Steps
US Bank Secrecy Act / FinCEN CDD Rule	Customer identification; beneficial ownership	The identity and beneficial-ownership Steps, evidenced and determined
EU AMLD / AMLR; MiCA	CASP and obliged-entity due diligence	The full step set under a CASP profile
Bermuda POCR / DABA	CDD obligations on the licensed person	The step set under a DABA profile; licence read from the AIS-1 bond
UK MLR 2017	CDD, EDD, ongoing monitoring	The step set with monitoring as a Subscription-class commitment

ACAS-1 does not determine whether a given record satisfies a supervisor. That remains the judgment of the regulated person and its supervisor.

13.2 On third-party reliance (R.17)

This section exists to forestall a misreading.

Recommendation 17 permits an institution to rely on a third party for elements (a) to (c) of Recommendation 10, subject to conditions: the relying institution must immediately obtain the necessary information, must satisfy itself that copies of underlying documentation will be made available on request without delay, must be satisfied that the third party is regulated, supervised and has CDD measures in place — and retains ultimate responsibility in all cases.

In practice, reliance is a bilateral arrangement. It is negotiated, contracted and maintained between named institutions, and the cost sits in the negotiation rather than in the information transfer. That is why it works between two banks and does not scale to an open network of agents meeting for the first time.

ACAS-1 does not create a reliance right and does not purport to satisfy R.17. A Presentation is not a reliance arrangement. A recipient's obligation is undiminished by anything carried in one.

What ACAS-1 does is narrower and, we suggest, more useful: it makes the recipient's *own* diligence fast, evidenced and current. Where a recipient chooses to enter a reliance arrangement, the standard happens to supply the technical substrate that the R.17 conditions describe — immediate availability of information, and underlying documentation obtainable without delay through the disclosure endpoint. Whether that is sufficient in any jurisdiction is a question for that jurisdiction, and nothing here should be read as an answer to it.

13.3 Out of scope: suspicious transaction reporting

Recommendations 20 and 21 require the reporting of suspicious transactions and prohibit disclosure of the fact that a report has been or is being made. FATF calls the instrument a **suspicious transaction report (STR)**; the United States under the Bank Secrecy Act and the United Kingdom under the Proceeds of Crime Act both call it a **suspicious activity report (SAR)**. The terms are used interchangeably here and the constraint is identical under either. Tipping off is a criminal offence in most implementing jurisdictions.

ACAS-1 is designed so that no Step, Presentation or evidence chain can carry or imply that a report has been made or contemplated. This is a schema constraint and a conformance requirement, not a stylistic preference. Implementations must attend to three inference channels in particular:

- **Persistent outcome states.** A `review` outcome that persists indefinitely, or an escalation flag that is never resolved, is an inference channel. Outcome states must resolve or the Step must lapse under `validUntil`.
- **Silent absence.** A Step that disappears from a Presentation it previously appeared in is an inference channel. Withdrawal must be indistinguishable from expiry or scope change.
- **Cadence anomalies.** An abrupt change in a published monitoring programme is an inference channel. Programme changes should be published on a schedule rather than on an event.

Implementations **MUST NOT** define extension types for suspicion, escalation to a financial intelligence unit, or internal report status.

13.4 Data protection

Continuous screening of a natural person is continuous processing of personal data and requires a lawful basis for each operation.

An obliged entity screening its own customer generally processes under a legal obligation. An assessing party screening a counterparty's beneficial owners, where it has no relationship with those individuals, may not have that basis available and should not assume it. The carriage model is designed with this in mind: Freshness Signal and Subscription Steps carry no personal data at all, and Referenced Steps carry none until an authorised request is made and granted.

Implementations should treat the Presentation record required by §9.1 as their record of processing, and the disclosure mandate as their record of the basis on which disclosure was made.

14. Comparison with Existing Approaches

Approach	Scope	Gap ACAS-1 addresses
AIS-1	Agent identity (companion)	Carries identity, not the diligence performed on it
AAS-1	Agent auditability (companion)	Records what an agent did, without a compliance vocabulary, carriage model or determination model
FATF R.17 reliance	Third-party reliance on CDD	Bilateral, negotiated, contract-bound; does not scale to an open network
Periodic review programmes	Ongoing due diligence under R.10(d)	Calendar-driven; detection latency in months; cadence asserted rather than proved
KYC utilities and shared registries	Pooled due diligence	Centralising custodian; membership-bound; no agent-resolvable presentation; no continuous assurance
A named compliance officer	Establishes a responsible person exists	Authoritative but not machine-resolvable; an assessing agent cannot query a name
Institutional compliance stacks	Perform the diligence	Produce no portable, verifiable artefact; the work stays in the institution and is repeated by every counterparty
Verifiable Credentials (KYC VCs)	A claim that a check was passed	A pass/fail claim without the standard catalogue, the carriage model, the latency evidence, or the determination gradient
ACAS-1 (this standard)	Continuous, portable, provable due diligence	A standard set of evidenced acts, classified by how they can travel, with cadence proved rather than claimed, presented under a revocable mandate

15. Security and Privacy Considerations

15.1 Step integrity. Every Step is signed by its performer or determiner; tampering is detectable by hash recomputation. A Step whose signature does not verify against the claimed AIS-1 identity is not conformant.

15.2 Chain integrity. The performance claims of §7.3 rest entirely on the AAS-1 evidence chain. A verifier relying on a latency claim **MUST** verify the chain rather than the summary — `executions` and `maxObservedLatency` are assertions until the chain is recomputed. Implementations **SHOULD** anchor the chain head periodically to an independent notary or ledger so that wholesale reconstruction is detectable.

15.3 Data minimisation. Steps carry sensitive underlying values by hash or reference wherever the result can be verified without exposing them. The carriage model does most of this work structurally: two of the four classes carry no personal data by construction.

15.4 Presentation replay. A Presentation is bound to its `audienceRef` and `expiresAt`. Replay by another party is detectable and **MUST** be rejected. Verifiers **MUST NOT** forward a Presentation issued to them.

15.5 Determiner key custody. A `person_determined` or `independently_determined` Step is only as strong as the determiner's key custody. Determiner identities are AIS-1 identities; HSM-bound custody limits compromise. A recipient relying on a determination relies transitively on the determiner and **MAY** apply its own policy on which determiners it accepts.

15.6 Staleness. `validUntil` is required and enforced. A clear screening result is clear only as at its `performedAt` against the named list set. Verifiers **MUST** treat lapsed Steps as requiring refresh, never as clear.

15.7 Programme theatre. A declared programme with high cadence and unstated matching should be assessed as unevidenced. §7.5 makes `matching` required for this reason, and verifiers **SHOULD** reject programme objects lacking it.

15.8 Over-reliance. A recipient remains responsible for its own compliance decision. ACAS-1 makes verified, current work available rather than requiring its repetition; it transfers nothing.

16. Regulatory Profiles

A profile defines which step types a complete record must contain, the minimum determination level for each, the minimum carriage class, and any minimum programme requirements. Profiles in scope for subsequent revisions:

- **FATF baseline CDD** — identity, beneficial ownership, purpose and nature, sanctions, PEP; monitoring as a live subscription.
- **Enhanced due diligence** — the baseline plus source of funds and wealth, with higher determination minimums and shorter currency intervals.
- **Bermuda DABA / POCR** — the DABA step set; sponsor licence read from the AIS-1 bond.
- **EU CASP (MiCA / AMLR)** — the CASP step set with EU data-protection constraints on carriage.
- **US BSA / FinCEN CDD Rule** — including beneficial ownership under the CDD Rule.
- **Agent-to-agent payment** — the minimal step set two agents need to clear each other under ARS-1, composing with ARS-1 Travel Rule data.

A profile is what makes "complete" concrete. The same record may be complete for one profile and incomplete for another; the assessing party names the profile it is testing against.

17. Implementation Roadmap

Phase	Deliverable	Target
0.1 — this document	The Compliance Step primitive; carriage classes; step-type catalogue and FATF anchor; continuous assurance and detection latency; determination model; Record and Presentation split; disclosure mandate; Step, Presentation and disclosure-mandate schemas; both operator manuals	July 2026
0.2	Per-type normative schemas. FATF baseline and Bermuda DABA profiles. Prepared-package conformance criteria. Latency measurement methodology, including computation where a list publisher does not timestamp additions	Q4 2026
0.3	Reference deployment — PayAgent operates a declared monitoring programme over 90 days and publishes the verified performance record; a counterparty agent clears against it	Q4 2026
0.4	Independent determination operationalised with a reference verifier programme; MiCA CASP and US BSA profiles	Q1 2027
0.5	Proved carriage (§5.4): predicate catalogue, proving-system profile, and supervisory viewing-key requirement	Q1 2027
0.6	Conformance suite: test vectors, harness, reference verifier. Composition with ARS-1 for agent-to-agent payment	Q2 2027
1.0	Submission to FATF private-sector consultation and ISO TC 68. Stable schemas. Convening with supervisory authorities on latency as a reportable metric	Q3 2027

18. Request for Comment

ACAS-1 v0.1 is published as a draft for public comment.

Feedback is invited from compliance officers and MLROs; AML/CFT supervisors and competent authorities; FATF, FIUs and standard-setting bodies; VASPs, EMIs, banks and digital-asset businesses running agent-mediated payments; screening and monitoring providers; data-protection practitioners; AI agent developers; and standards organisations including ISO TC 68 and the BIS Innovation Hub.

We are particularly interested in comment on:

- whether **detection latency** is the right assurance metric, and how it should be measured and reported;
- whether the **four carriage classes** correctly describe how due-diligence results can and cannot travel;
- whether the **detection / determination separation** at §7.4 is drawn in the right place, and whether the `disposition` conformance rule is strict enough;
- whether the **step-type catalogue** is the right decomposition of the obligations at §6.1;
- whether the **tipping-off inference channels** at §13.3 are completely enumerated;
- the **lawful basis** analysis at §13.4, particularly for an assessing party screening a counterparty's beneficial owners;
- real-world agent-to-agent deployments to pilot the standard.

Feedback may be submitted via the form at acas-1.org, by email to info@aiagentsservices.net, or at github.com/Kadikoy1/acas-1/issues.

The comment period for v0.1 closes **31 October 2026**. A revised draft will be published as v0.2.

---

19. Authors

Field	Value
Author	Kadikoy Limited, Bermuda
Affiliation	BDA Law; BDA AI Agent Services
Companions	AIS-1 (ais-1.org); AAS-1 (aas-1.org); AIPS-1 (aips-1.org); ARS-1 (ars-1.org); AES-1 (aes-1.org)
Contact	info@aiagentsservices.net
Website	acas-1.org
Repository	github.com/Kadikoy1/acas-1
License	Creative Commons CC0. No rights reserved. Open for free implementation.

Appendix A — A Freshness Signal Step

A `sanctions_screening` Step. Note that the carried result is not offered as a substitute for the recipient's own screening: what has value here is the declared programme and its recency.

```
{
  "acas": "0.1",
  "stepId": "01K1ACAS3M7YPB4N9XJ2VQ5RTFW",
  "subjectRef": "did:ais1:base:counterparty-agent-047",
  "type": "sanctions_screening",
  "carriage": "freshness_signal",
  "inputs": {
    "listSetRefs": ["https://compliance.example.com/lists/un-ofac-eu-hmt-2026-07-31"],
    "matching": { "method": "fuzzy", "threshold": 0.85,
                  "providerRef": "did:ais1:sponsor:screening-provider-example" },
    "screenedSubject": "did:ais1:base:counterparty-agent-047",
    "screenedAt": "2026-07-31T14:32:11Z"
  },
  "result": { "outcome": "clear", "matchCount": 0 },
  "performedBy": "did:ais1:base:payagent-001",
  "performedAt": "2026-07-31T14:32:11Z",
  "determination": {
    "level": "agent_determined",
    "determinerRef": "did:ais1:base:payagent-001"
  },
  "evidence": [
    { "type": "log", "value": "https://logs.payagent.ai/2026/07/31/screen-01K1..." },
    { "type": "attestation", "value": "screen-provider-attestation-base64...",
      "issuerRef": "https://screening.example.com/attest/0xabc" }
  ],
  "validUntil": "2026-08-30T00:00:00Z",
  "aas1RecordRef": "aas1:01K1ACAS4K5M6N7P8Q9R0S1T2V",
  "signature": {
    "alg": "EdDSA", "hashAlg": "SHA-256", "canonicalisation": "JCS",
    "keyRef": "did:ais1:base:payagent-001#key-1",
    "value": "z58dYMy3..."
  }
}
```


Appendix B — A Subscription Step

An `ongoing_monitoring` Step. This is the Step that carries the continuous-assurance claim, and it contains no personal data of any kind.

```
{
  "acas": "0.1",
  "stepId": "01K1ACAS5N6P7Q8R9S0T1V2W3X",
  "subjectRef": "did:ais1:base:counterparty-agent-047",
  "type": "ongoing_monitoring",
  "carriage": "subscription",
  "inputs": { "relationshipStart": "2026-04-02T00:00:00Z" },
  "result": {
    "status": "live",
    "subscriptionEndpoint": "https://monitor.operator.example.com/acas/subscribe/01K1...",
    "notifiesOn": ["status_change", "programme_change", "termination"]
  },
  "programme": {
    "cadence": "on_list_update",
    "maxLatency": "PT4H",
    "listSetRefs": ["https://compliance.example.com/lists/un-ofac-eu-hmt"],
    "matching": { "method": "fuzzy", "threshold": 0.85,
                  "providerRef": "did:ais1:sponsor:screening-provider-example" },
    "disposition": "human_required_on_hit",
    "policyRef": "https://operator.example.com/policies/monitoring/v4"
  },
  "performance": {
    "window": "P90D",
    "executions": 847,
    "expectedExecutions": 841,
    "maxObservedLatency": "PT3H12M",
    "meanObservedLatency": "PT41M",
    "missedWindows": 0,
    "evidenceChainRef": "aas1:chain/01K1ACAS6P7Q8R9S0T1V2W3X4Y",
    "chainHead": "sha256-4f3edf..."
  },
  "performedBy": "did:ais1:base:payagent-001",
  "performedAt": "2026-07-31T00:00:00Z",
  "determination": {
    "level": "agent_determined",
    "determinerRef": "did:ais1:base:payagent-001"
  },
  "evidence": [
    { "type": "log", "value": "aas1:chain/01K1ACAS6P7Q8R9S0T1V2W3X4Y" },
    { "type": "hash_anchor", "value": "ethereum:0x4f3edf...",
      "issuerRef": "https://etherscan.io" }
  ],
  "validUntil": "2026-10-29T00:00:00Z",
  "aas1RecordRef": "aas1:01K1ACAS7Q8R9S0T1V2W3X4Y5Z",
  "signature": {
    "alg": "EdDSA", "hashAlg": "SHA-256", "canonicalisation": "JCS",
    "keyRef": "did:ais1:base:payagent-001#key-1",
    "value": "z7kQpNm9..."
  }
}
```


`executions` against `expectedExecutions`, and `missedWindows`, are the fields a hostile reviewer asks for first. A programme claiming continuous coverage must be able to show it did not silently stop.

Appendix C — A Referenced Step and its Prepared Determination

A `source_of_funds` Step. The substance does not travel; the fact, scope, outcome and integrity hash do.

```
{
  "acas": "0.1",
  "stepId": "01K1ACAS8R9S0T1V2W3X4Y5Z6A",
  "subjectRef": "did:ais1:sponsor:counterparty-047-principal",
  "type": "source_of_funds",
  "carriage": "referenced",
  "inputs": {
    "scope": "source_of_funds",
    "categoriesExamined": ["employment_income", "corporate_distribution"],
    "periodCovered": { "from": "2024-01-01", "to": "2026-06-30" }
  },
  "result": {
    "outcome": "established",
    "sourceCategory": "corporate_distribution",
    "consistencyWithProfile": "consistent"
  },
  "disclosure": {
    "endpoint": "https://disclosure.operator.example.com/acas/steps/01K1ACAS8R9S...",
    "materialHash": "sha256-a3f81c...",
    "hashAlg": "SHA-256",
    "requiresAuthorisation": true,
    "authorisationScheme": "acas1-disclosure-mandate"
  },
  "performedBy": "did:ais1:base:payagent-001",
  "performedAt": "2026-07-28T09:14:02Z",
  "determination": {
    "level": "prepared_for_determination",
    "determinerRef": "did:ais1:base:payagent-001",
    "awaitingRef": "did:ais1:sponsor:officer-mlro-example",
    "formRef": "https://acas.operator.example.com/forms/edd/subject-047"
  },
  "evidence": [
    { "type": "log", "value": "https://logs.payagent.ai/2026/07/28/sof-01K1..." },
    { "type": "hash_anchor", "value": "ethereum:0x9c2b1a...",
      "issuerRef": "https://etherscan.io" }
  ],
  "validUntil": "2027-07-28T00:00:00Z",
  "aas1RecordRef": "aas1:01K1ACAS9S0T1V2W3X4Y5Z6A7B",
  "signature": {
    "alg": "EdDSA", "hashAlg": "SHA-256", "canonicalisation": "JCS",
    "keyRef": "did:ais1:base:payagent-001#key-1",
    "value": "z4mRtQx2..."
  }
}
```

On determination, a superseding Step is issued carrying the officer's judgment. The prepared Step is retained: the pair records what was put before the responsible person and what they decided.

```
"determination": {
  "level": "person_determined",
  "determinerRef": "did:ais1:sponsor:officer-mlro-example",
  "determinedAt": "2026-07-29T11:20:44Z"
},
"supersedes": "01K1ACAS8R9S0T1V2W3X4Y5Z6A",
"evidence": [
  { "type": "human", "value": "z9pLcVk4...",
    "issuerRef": "did:ais1:sponsor:officer-mlro-example#key-1" }
]
```

Appendix D — A Presentation

Constructed for one counterparty, under a mandate, against a named profile.

```
{
  "acas": "0.1",
  "presentationId": "01K1ACASB1C2D3E4F5G6H7J8K9",
  "subjectRef": "did:ais1:base:counterparty-agent-047",
  "audienceRef": "did:ais1:base:assessing-agent-012",
  "purpose": "counterparty_assessment_for_payment",
  "profile": "a2a-payment",
  "mandateRef": "acas1:mandate/01K1MNDT4C5D6E7F8G9H0J1K2L",
  "steps": [
    { "type": "identity_verification", "stepRef": "acas:step/id-047",
      "carriage": "portable", "level": "independently_determined" },
    { "type": "beneficial_ownership", "stepRef": "acas:step/bo-047",
      "carriage": "portable_referenced", "level": "person_determined" },
    { "type": "purpose_and_nature", "stepRef": "acas:step/purpose-047",
      "carriage": "portable", "level": "agent_determined" },
    { "type": "sanctions_screening", "stepRef": "acas:step/sanc-047",
      "carriage": "freshness_signal", "level": "agent_determined" },
    { "type": "pep_screening", "stepRef": "acas:step/pep-047",
      "carriage": "freshness_signal", "level": "agent_determined" },
    { "type": "ongoing_monitoring", "stepRef": "acas:step/mon-047",
      "carriage": "subscription", "level": "agent_determined" }
  ],
  "completeFor": "a2a-payment",
  "issuedAt": "2026-07-31T14:35:00Z",
  "expiresAt": "2026-08-07T14:35:00Z",
  "aas1RecordRef": "aas1:01K1ACASC2D3E4F5G6H7J8K9L0",
  "signature": {
    "alg": "EdDSA", "hashAlg": "SHA-256", "canonicalisation": "JCS",
    "keyRef": "did:ais1:base:counterparty-agent-047#key-1",
    "value": "z6nWpTr8..."
  }
}
```

Appendix E — A Disclosure Mandate

The grant under which the Presentation at Appendix D was issued. Note that `source_of_funds` is deliberately absent from `stepTypes`: the grantor has authorised disclosure of the rest of the record to this counterparty for this purpose, and nothing more.


```
{
  "acas": "0.1",
  "mandateId": "01K1MNDT4C5D6E7F8G9H0J1K2L",
  "grantorRef": "did:ais1:sponsor:counterparty-047-principal",
  "granteeRef": "did:ais1:base:counterparty-agent-047",
  "stepTypes": [
    "identity_verification",
    "beneficial_ownership",
    "purpose_and_nature",
    "sanctions_screening",
    "pep_screening",
    "ongoing_monitoring"
  ],
  "audiences": [
    "did:ais1:base:assessing-agent-012",
    "class:licensed-payment-institution"
  ],
  "purposes": [
    "counterparty_assessment_for_payment"
  ],
  "notBefore": "2026-07-01T00:00:00Z",
  "notAfter": "2026-12-31T23:59:59Z",
  "statusEndpoint": "https://mandates.operator.example.com/acas/status/01K1MNDT4C5D6E7F8G9H0J1K2L",
  "signature": {
    "alg": "EdDSA",
    "hashAlg": "SHA-256",
    "canonicalisation": "JCS",
    "keyRef": "did:ais1:sponsor:counterparty-047-principal#key-1",
    "value": "z2kFbXr7..."
  },
  "notes": "source_of_funds deliberately excluded from stepTypes; disclosed only on separate authorisation."
}
```

Appendix F — Counterparty Verification Flow

```
// Agent A assesses Agent B before transacting.

// 1. Presentation-level checks — audience, window, mandate
assert(presentation.audienceRef === myDid);
assert(now() < presentation.expiresAt);
assert(!(await mandate.isRevoked(presentation.mandateRef)));

// 2. Subject identity
const subject = await ais1.resolve(presentation.subjectRef);
assert((await ais1.verifyBond(subject.bondId)).valid);

// 3. Per-Step verification — signature, evidence, currency
for (const entry of presentation.steps) {
  const step   = await acas1.fetch(entry.stepRef);
  const signer = await ais1.resolve(step.determination.determinerRef);
  assert(verifySignature(step, signer.verificationMethod));
  assert(checkEvidence(step.evidence));
  assert(now() < step.validUntil);
}

// 4. Act on carriage class — the substantive step
for (const step of steps) {
  switch (step.carriage) {

    case 'portable':
      accept(step.result);                    // take into the assessment
      break;

    case 'referenced':
      if (policy.requiresMaterial(step.type)) { // request under authorisation
        const material = await acas1.request(step.disclosure, myMandate);
        assert(sha256(material) === step.disclosure.materialHash);
      }
      break;

    case 'freshness_signal':
      riskSignal(step.programme ?? step.inputs); // read posture, then re-run
      await self.screen(subject, policy.listSets);
      break;

    case 'subscription':
      assert(await aas1.verifyChain(step.performance.evidenceChainRef,
                                    step.performance.chainHead));
      assert(step.performance.missedWindows === 0);
      assert(duration(step.performance.maxObservedLatency)
               <= duration(policy.maxAcceptableLatency));
      await acas1.subscribe(step.result.subscriptionEndpoint);
      break;
  }
}
```

```
// 5. Completeness and determination levels against A's own profile
const required = profiles['a2a-payment'].requiredTypes;
assert(required.every(t => presentation.steps.some(s => s.type === t)));
const meetsPolicy = presentation.steps.every(s =>
  levelRank(s.level) >= policy.minLevelFor(s.type));

// 6. Decide — clear, or prepare a package for the responsible person
if (meetsPolicy) {
  return clear(subject);
} else {
  const pkg = buildPreparedPackage(presentation, policy.reservedDeterminations);
  return routeToOfficer(pkg);
}
```

Note step 4's `subscription` branch: the verifier recomputes the evidence chain rather than trusting the summary. Under §15.2 the performance figures are assertions until the chain is verified.

End of ACAS-1 v0.1 specification. Published 31 July 2026 by Kadikoy Limited, Bermuda. Released under CC0 1.0 Universal — no rights reserved. Comment closes 31 October 2026.