

ODA3 INSTITUTE

TECHNICAL REFERENCE

UAIF Validation Rules Catalogue

Conformance Rule Reference for the Canonical UAIF™ v1.0 Schema

TCR-UAIF-015 | Public

© ODA3 Pvt Ltd

Document Control

Item	Value
Document Identifier	TCR-UAIF-015 (legacy identifier retained for citation continuity)
Doc Type	Technical Reference - Validation Rules Catalogue
Framework Tag	UAIF™ v1.0
Canonical Schema	uaif-core-v1.0.json (JSON Schema Draft 2020-12)
Canonical SHA-256	55056e7cfa4fcf4b76cc4656833cb5b360a1b40fa90f23488d488409ccebeeca
Authoritative Schema Specification	ODA3-2026-06-TCR-STD-003 - UAIF™ v1.0 Schema Specification
Companion Data Dictionary	TCR-UAIF-014 - corrected 04 October 2026 against the same canonical schema
Publication History	Issued 14 July 2026; updated 04 October 2026
Review Cycle	On every schema correction; otherwise annual
Audience	Implementers building conformance tests, CI pipelines, validators and integration gates
Licence	GAISSF Ecosystem Licence (GEL) v1.0
Contact	contact@oda3.org
Classification	Public

VERIFICATION NOTICE

This corrected edition is aligned to the frozen canonical schema uaif-core-v1.0.json (SHA-256 55056e7cfa4fcf4b76cc4656833cb5b360a1b40fa90f23488d488409ccebeeca). The reviewed repository contains 6 valid fixtures and 14 invalid fixtures. All 6 valid fixtures pass; all 14 invalid fixtures fail for their intended rule markers; and the repository test suite passes 23/23 tests. The separate 15-case normative conformance corpus remains a distinct release-gate evidence set.

1. Purpose and Scope

This catalogue translates the canonical UAIF™ v1.0 validation model into implementer-facing rule statements and expected outcomes. It covers top-level structure, primitive constraints, controlled vocabularies, profile and extension gating, conditional rules, nested severity_rationale rules, and the separate semantic score-precision rule.

The canonical uaif-core-v1.0.json schema and ODA3-2026-06-TCR-STD-003 remain normative for machine validation. Where this catalogue differs from the canonical schema, the schema governs. TCR-UAIF-014 provides the companion field-level reference.

2. Class 1 - Structural Rules

ID	Rule	Expected result on violation
VAL-S01	All 12 top-level required fields must be present: incident_uuid, incident_title, incident_summary, reporting_timestamp, deduplication_hash, remediation_status, record_type, profile, root_cause_primary_domain, root_cause_specific_type, sector_code, jurisdiction_country_code.	Reject; report missing required field(s).
VAL-S02	The top-level record is closed (unevaluatedProperties: false); undeclared top-level properties are invalid except for fields explicitly declared by the schema.	Reject; report unexpected property.
VAL-S03	x_extensions is an open object; organisation/sector-specific nested keys may appear inside it.	Accept x_extensions content subject to JSON type/object validity and any external extension contract.
VAL-S04	severity_justification is not a declared property in UAIF™ v1.0.	Reject as unexpected property.
VAL-S05	record_type = Observation is not part of the normative v1.0 vocabulary.	Reject as invalid enum value.

3. Class 2 - Type, Format, Pattern and Range Rules

ID	Field(s)	Rule	Expected result
VAL-T01	incident_uuid	string; format uuid	Reject

ID	Field(s)	Rule	Expected result
VAL-T02	reporting_timestamp	string; format date-time	Reject
VAL-T03	deduplication_hash	string; exactly 64 hexadecimal characters	Reject
VAL-T04	incident_title	string; length 5-255	Reject
VAL-T05	incident_summary / exploit_path_description	string; length 20-4000	Reject
VAL-T06	severity_analytical_score / severity_presentation_score	number; range 0.0-10.0. One-decimal precision is tested separately as VAL-M01.	Reject schema range/type violations
VAL-T07	severity_level / reporter_confidence_level	integer; range 1-5	Reject
VAL-T08	cumulative_bias_index	number; range 0.0-1.0	Reject
VAL-T09	exposure_duration_hours	number; minimum 0	Reject
VAL-T10	jurisdiction_country_code	pattern <code>^[A-Z]{2}(-[A-Z0-9]{1,3})?\$</code>	Reject
VAL-T11	nace_code_actual	pattern <code>^[A-Z](\d{2}(\.\d{1,2}))?\$</code>	Reject
VAL-T12	naics_code_actual	pattern <code>^\d{2,6}\$</code>	Reject
VAL-T13	atlas_technique_id	pattern <code>^AML.T[0-9]{4}(\.[0-9]{3})?\$</code>	Reject
VAL-T14	severity_rationale.calibration_source	string URI or null	Reject
VAL-T15	extensions	array of unique string items; each item must be an approved extension value	Reject
VAL-T16	realized_harm_categories / regulatory_obligations	array; at least one item; unique items; each item must be in its controlled vocabulary	Reject

4. Class 3 - Controlled Vocabulary Rules

ID	Field	Permitted values / rule
VAL-E01	remediation_status	Detected, Investigating, Mitigated, Resolved
VAL-E02	record_type	Incident, Vulnerability
VAL-E03	profile	Core, Enterprise, Regulatory
VAL-E04	extensions	SOC_SIEM, AI_Security
VAL-E05	root_cause_primary_domain	Human, System, Data, External
VAL-E06	root_cause_specific_type	15 named values or an x_-prefixed custom value matching the canonical pattern
VAL-E07	root_cause_confidence / trigger_confidence	LOW, MEDIUM, HIGH
VAL-E08	ai_system_type	LLM, VLM, RAG_Pipeline, Agentic, Multi_Agent, Traditional_ML, Other
VAL-E09	sector_code	19 canonical UAIF sector codes
VAL-E10	regulatory_obligations items	EU_AI_Act_Article_73, GDPR_Article_33, NIS2_Article_23, DORA_Article_19, Sectoral_Reporting, None
VAL-E11	harm-category fields	Physical_Harm, Environmental_Harm, Security_Integrity, Privacy_Violation, Financial_Loss, Psychological_Harm, Property_Damage, Reputational_Harm
VAL-E12	severity_rationale.calibration_status	provisional, sector_validated, custom

5. Class 4 - Conditional, Profile and Extension Rules

ID	Trigger / condition	Requirement / prohibition	Expected result
VAL-C10	record_type = "Incident"	Require severity_analytical_score, severity_presentation_score, severity_level, severity_rationale.	Reject; report missing field(s).
VAL-C11	record_type = "Incident" AND profile in {Enterprise, Regulatory}	Additionally require realized_harm_categories.	Reject; report missing field.
VAL-C12	profile = "Core"	Prohibit harm_acute, harm_chronic_proxy, realized_harm_categories, cumulative_bias_index, linked_vulnerability_id, exposure_duration_hours.	Reject if any prohibited L3/L4 field is present.
VAL-C13	atlas_technique_id present	extensions must explicitly contain SOC_SIEM.	Reject.

ID	Trigger / condition	Requirement / prohibition	Expected result
VAL-C14	Any AI-Security L5 field present	extensions must explicitly contain AI_Security for ai_system_type, non_adversarial_failure_type, agent_escalation_chain, mcp_endpoint_ids, oauth_pivot_chain, policy_enforcement_point.	Reject.
VAL-C15	regulatory_trigger key present (true or false)	Require trigger_confidence and human_review_recommended.	Reject; report missing companion field(s).
VAL-C16	root_cause_specific_type = "Adversarial_Attack"	Require exploit_path_description.	Reject; report missing field.
VAL-C17	severity_rationale.calibration_status = "provisional"	Require severity_rationale.weight_provisional_notice.	Reject; report missing inner field.

6. Class 5 - severity_rationale Nested-Object Rules

ID	Rule	Expected result on violation
VAL-N01	severity_rationale.calibration_status is the only unconditionally required inner field.	Reject if severity_rationale is present without calibration_status.
VAL-N02	context_modifiers_applied must be an array of objects.	Reject type violations.
VAL-N03	Each context_modifiers_applied item requires context, base_value, contribution_factor and effective_contribution.	Reject item; report missing sub-field(s).
VAL-N04	Each context_modifiers_applied item is closed (additionalProperties: false).	Reject item; report unexpected property.
VAL-N05	severity_rationale itself is open (additionalProperties: true).	Accept additional rationale keys unless another governing rule restricts them.
VAL-N06	dominant_harm and secondary_harms items use the canonical eight-category harm vocabulary.	Reject invalid enum values.

7. Class 6 - Semantic Precision Rule

ID	Applies to	Rule	Validation method
VAL-M01	severity_analytical_score; severity_presentation_score	Scores SHALL be represented to one decimal place using Decimal ROUND_HALF_UP. This is normative but intentionally not encoded as JSON Schema multipleOf: 0.1.	Reference implementation or equivalent semantic/conformance tooling; generic schema validation alone is insufficient.

8. Verification Method and Evidence

The corrected catalogue was reconciled against the canonical schema and the reviewed v1.0.0 repository. Repository verification was rerun with Draft 2020-12 validation and format checking.

Check	Observed result	Status
Canonical schema SHA-256	55056e7cfa4fcf4b76cc4656833cb5b360a1b40fa90f23488d488409ccebceca	PASS
Valid fixture set	6/6 accepted	PASS
Invalid fixture set	14/14 rejected for the intended rule marker	PASS
Repository automated tests	23/23	PASS
Frozen architecture checks	record_type, profile, extensions, removed severity_justification, closed top-level object	PASS
Semantic score precision	Separate conformance rule; not claimed as generic JSON Schema enforcement	PASS

The 20 repository fixtures (6 valid + 14 invalid) are repository regression fixtures. They are not the separate 15-case normative conformance corpus used for the v1.0 Final Publication release gate.

9. Notably Absent

- No Observation record type. Observation belongs to upstream detection/case-management workflow until classified as Incident or Vulnerability.
- No severity_justification field. severity_rationale is the sole canonical severity explanation.
- No requirement that every Incident carry realized_harm_categories; only Enterprise and Regulatory Incidents do, while Core prohibits that L3 field.
- No assumption that SOC_Siem or AI_Security fields are valid unless the corresponding extension is explicitly declared.

- No claim that JSON Schema alone enforces one-decimal score precision.
- No rule set for sector-specific x_extensions vocabularies; those belong to separately validated sector packages.
- No legal, regulatory, certification, external-assurance or production-maturity status is created by passing these validation rules.
- Certification is not currently offered. Any future UAIF certification programme would require separate approved and published governance.

10. Revision Note - 04 October 2026

This corrected reissue preserves legacy document identifier TCR-UAIF-015 for citation continuity and replaces the withdrawn July schema basis with the frozen canonical uaif-core-v1.0.json schema (SHA-256 55056e7cfa4fcf4b76cc4656833cb5b360a1b40fa90f23488d488409ccebceca). It removes Observation and severity_justification; adds profile and extensions; corrects the 12-field required set; separates universal Incident severity requirements from Enterprise/Regulatory harm-category requirements; adds the Core L3/L4 prohibition; adds SOC_SIEM and AI_Security extension gating; corrects one-decimal score precision from a schema multipleOf rule to a separate semantic conformance rule; updates repository verification from the obsolete 11-fixture set to 6 valid + 14 invalid intended-rule fixtures and 23/23 automated tests; updates contact/classification wording; and removes the incorrect statement that the normative severity calculation is unpublished/controlled. No new UAIF normative behavior is introduced.

GAISSF Ecosystem developed by ODA3 Institute, licensed under GEL v1.0.