

ODA3 INSTITUTE

TECHNICAL REFERENCE

UAIF Data Dictionary

Field-Level Reference for the Canonical UAIF™ v1.0 Schema

TCR-UAIF-014 | Public

© ODA3 Pvt Ltd

Document Control

Item	Value
Document Identifier	TCR-UAIF-014 (legacy identifier retained for citation continuity)
Doc Type	Technical Reference - Data Dictionary
Framework Tag	UAIF™ v1.0
Canonical Schema	uaif-core-v1.0.json (JSON Schema Draft 2020-12)
Canonical SHA-256	55056e7cfa4fc4b76cc4656833cb5b360a1b40fa90f23488d488409ccebeeca
Authoritative Schema Specification	ODA3-2026-06-TCR-STD-003 - UAIF™ v1.0 Schema Specification
Publication History	Issued 14 July 2026; updated 04 October 2026
Review Cycle	On every schema correction; otherwise annual
Audience	Implementers, integrators, SOC/GRC engineers, schema validators
Licence	GAISSF Ecosystem Licence (GEL) v1.0
Contact	contact@oda3.org
Classification	Public

GENERATION NOTICE

This corrected edition was regenerated from the frozen canonical schema uaif-core-v1.0.json (SHA-256 55056e7cfa4fc4b76cc4656833cb5b360a1b40fa90f23488d488409ccebeeca). The canonical schema contains 43 top-level properties, 12 unconditionally required fields, and 8 conditional rule blocks. The schema remains normative; this dictionary is an explanatory reference and must be regenerated after any future schema correction.

1. Purpose and Scope

This dictionary documents every top-level property in the canonical UAIF™ v1.0 schema, including its type, unconditional requirement status, and machine-enforced constraints. Conditional requirements and prohibitions are listed separately because they depend on record content, profile, or declared extensions.

Where this dictionary differs from ODA3-2026-06-TCR-STD-003 or the canonical uaif-core-v1.0.json file, the canonical schema and governing normative specification prevail. The one-decimal score-precision rule is normative but intentionally enforced outside generic JSON Schema validation.

2. Field Reference

Fields are listed in canonical schema declaration order. 'Required' below means unconditionally required at the top level; conditional and profile/extension rules are shown explicitly.

Field	Type	Requirement	Constraints
incident_uuid	string	Required	format: uuid
incident_title	string	Required	length 5-255
incident_summary	string	Required	length 20-4000
reporting_timestamp	string	Required	format: date-time
reporter_confidence_level	integer	Optional	range 1-5
deduplication_hash	string	Required	pattern: ^[a-fA-F0-9]{64}\$
remediation_status	string	Required	enum: Detected, Investigating, Mitigated, Resolved
record_type	string	Required	enum: Incident, Vulnerability
profile	string	Required	enum: Core, Enterprise, Regulatory
extensions	array<string>	Optional	unique items; item enum: SOC_SIEM, AI_Security
root_cause_primary_domain	string	Required	enum: Human, System, Data, External

Field	Type	Requirement	Constraints
root_cause_specific_type	string	Required	pattern: ^(Adversarial_Attack Prompt_Injection Model_Poisoning Data_Poisoning RAG_Leakage Hallucination Agent_Escalation Policy_Violation System_Failure Human_Error Supply_Chain_Compromise Unauthorised_Access Data_Breach Denial_of_Service Misuse)x_[A-Za-z0-9_]+\$
root_cause_confidence	string	Optional	enum: LOW, MEDIUM, HIGH
exploit_path_description	string	Conditional: Adversarial_Attack	length 20-4000
severity_analytical_score	number	Conditional: Incident	range 0.0-10.0; one-decimal precision is a normative semantic rule; not enforced by JSON Schema multipleOf
severity_presentation_score	number	Conditional: Incident	range 0.0-10.0; one-decimal precision is a normative semantic rule; not enforced by JSON Schema multipleOf
severity_level	integer	Conditional: Incident	range 1-5
severity_rationale	object	Conditional: Incident	open object; calibration_status required
harm_acute	boolean	Optional; prohibited in Core	-
harm_chronic_proxy	boolean	Optional; prohibited in Core	-
realized_harm_categories	array<string>	Conditional: Enterprise/Regulatory Incident; prohibited in Core	minItems 1; unique items; item enum: Physical_Harm, Environmental_Harm, Security_Integrity, Privacy_Violation, Financial_Loss, Psychological_Harm, Property_Damage, Reputational_Harm
cumulative_bias_index	number	Optional; prohibited in Core	range 0.0-1.0
linked_vulnerability_id	string	Optional; prohibited in Core	-
exposure_duration_hours	number	Optional; prohibited in Core	minimum 0
ai_system_type	string	Extension-gated: AI_Security	enum: LLM, VLM, RAG_Pipeline, Agentic, Multi_Agent, Traditional_ML, Other
non_adversarial_failure_type	string	Extension-gated: AI_Security	-
agent_escalation_chain	array<string>	Extension-gated: AI_Security	string items
mcp_endpoint_ids	array<string>	Extension-gated: AI_Security	string items
oauth_pivot_chain	array<string>	Extension-gated: AI_Security	string items
policy_enforcement_point	string	Extension-gated: AI_Security	-
atlas_technique_id	string	Extension-gated: SOC_Siem	pattern: ^AML\.T[0-9]{4}(\.[0-9]{3})?\$
sector_code	string	Required	enum: ENERGY, TRANSPORT, BANKING, FINANCIAL_MARKETS, HEALTH, DRINKING_WATER, WASTE_WATER, DIGITAL_INFRA, ICT_SERVICES, PUBLIC_ADMIN, SPACE, POSTAL, WASTE_MGMT, CHEMICALS, FOOD, MANUFACTURING, TELECOM, RESEARCH, OTHER
nace_code_actual	string	Optional	pattern: ^[A-Z](\d{2}(\.\d{1,2}))?\$
naics_code_actual	string	Optional	pattern: ^\d{2,6}\$
jurisdiction_country_code	string	Required	pattern: ^[A-Z]{2}(-[A-Z0-9]{1,3})?\$
regulatory_obligations	array<string>	Optional	minItems 1; unique items; item enum: EU_AI_Act_Article_73, GDPR_Article_33, NIS2_Article_23, DORA_Article_19, Sectoral_Reporting, None
regulatory_trigger	boolean	Optional	-
trigger_confidence	string	Conditional: regulatory_trigger present	enum: LOW, MEDIUM, HIGH
human_review_recommended	boolean	Conditional: regulatory_trigger present	-
sensitive_data	boolean	Optional	-
critical_sector	boolean	Optional	-
vulnerable_population	boolean	Optional	-
x_extensions	object	Optional	open object for extension data

3. Conditional Requirements and Prohibitions

Trigger / condition	Schema consequence
Incident record	Requires severity_analytical_score, severity_presentation_score, severity_level and severity_rationale.
Enterprise or Regulatory Incident	Additionally requires realized_harm_categories.
Core profile	Prohibits harm_acute, harm_chronic_proxy, realized_harm_categories, cumulative_bias_index, linked_vulnerability_id and exposure_duration_hours.
atlas_technique_id present	extensions must explicitly contain SOC_SIEM.
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 or policy_enforcement_point.
regulatory_trigger present (true or false)	Requires trigger_confidence and human_review_recommended.
root_cause_specific_type = Adversarial_Attack	Requires exploit_path_description.
severity_rationale.calibration_status = provisional	Requires severity_rationale.weight_provisional_notice.

4. Controlled Vocabularies

Vocabulary	Canonical values
record_type	Incident, Vulnerability
profile	Core, Enterprise, Regulatory
extensions	SOC_SIEM, AI_Security
remediation_status	Detected, Investigating, Mitigated, Resolved
root_cause_primary_domain	Human, System, Data, External
root_cause_specific_type	Adversarial_Attack, Prompt_Injection, Model_Poisoning, Data_Poisoning, RAG_Leakage, Hallucination, Agent_Escalation, Policy_Violation, System_Failure, Human_Error, Supply_Chain_Compromise, Unauthorised_Access, Data_Breach, Denial_of_Service, Misuse, x_[custom]
realized_harm_categories	Physical_Harm, Environmental_Harm, Security_Integrity, Privacy_Violation, Financial_Loss, Psychological_Harm, Property_Damage, Reputational_Harm
sector_code	ENERGY, TRANSPORT, BANKING, FINANCIAL_MARKETS, HEALTH, DRINKING_WATER, WASTE_WATER, DIGITAL_INFRA, ICT_SERVICES, PUBLIC_ADMIN, SPACE, POSTAL, WASTE_MGMT, CHEMICALS, FOOD, MANUFACTURING, TELECOM, RESEARCH, OTHER
regulatory_obligations	EU_AI_Act_Article_73, GDPR_Article_33, NIS2_Article_23, DORA_Article_19, Sectoral_Reporting, None

5. The severity_rationale Object

severity_rationale is the sole canonical severity-explanation object. It is required for Incident records. Its only unconditionally required inner field is calibration_status. The object is open (additionalProperties: true), while context_modifiers_applied entries are closed objects.

Inner field	Type	Requirement	Constraints / notes
dominant_harm	string	Optional	enum: Physical_Harm, Environmental_Harm, Security_Integrity, Privacy_Violation, Financial_Loss, Psychological_Harm, Property_Damage, Reputational_Harm
dominant_weight	number	Optional	-
secondary_harms	array<string>	Optional	item enum: Physical_Harm, Environmental_Harm, Security_Integrity, Privacy_Violation, Financial_Loss, Psychological_Harm, Property_Damage, Reputational_Harm
secondary_contribution	number	Optional	-
context_modifiers_applied	array<object>	Optional	each item requires context, base_value, contribution_factor, effective_contribution; no additional properties per item
context_modifier_sum	number	Optional	-

Inner field	Type	Requirement	Constraints / notes
population_multiplier	number	Optional	-
blast_radius_multiplier	number	Optional	-
impact_scale	number	Optional	-
confidence_factor	number	Optional	-
temporal_reduction	number	Optional	-
temporal_adjustment	number	Optional	-
calibration_status	string	Required	enum: provisional, sector_validated, custom; drives provisional notice condition
calibration_source	string / null	Optional	format: uri
weight_provisional_notice	string / null	Conditional: provisional	-
assumptions	array<string>	Optional	string items
precision_notes	string	Optional	-

6. Scoring Precision Boundary

severity_analytical_score and severity_presentation_score are JSON numbers constrained to 0.0-10.0. UAIF™ v1.0 additionally requires one-decimal-place precision using Decimal ROUND_HALF_UP as a normative semantic/conformance rule. The canonical JSON Schema deliberately does not use multipleOf: 0.1 because binary floating-point behavior can create validator-dependent false negatives. Precision is therefore checked by reference/conformance tooling rather than generic JSON Schema alone.

7. x_extensions

x_extensions is an open object for sector-specific or organisation-specific extension data that has not been promoted into the core schema. The top-level UAIF object is closed by unevaluatedProperties: false, so undeclared top-level fields fail validation. Extension-gated top-level fields remain subject to the SOC_SIEM and AI_Security declaration rules above.

8. Notably Absent

- Observation is not a normative record_type in UAIF™ v1.0. Unclassified observations remain in upstream detection/case-management workflows until classified as Incident or Vulnerability.
- severity_justification is not a valid field. severity_rationale is the sole canonical severity explanation.
- The dictionary does not make realized_harm_categories mandatory for every Incident; it is additionally required only for Enterprise and Regulatory Incident records and is prohibited under Core.
- The one-decimal precision rule is not represented as JSON Schema multipleOf: 0.1.
- The dictionary does not replace the canonical schema or the normative calculation semantics published in ODA3-2026-06-TCR-STD-002.
- No schema use establishes legal compliance, certification, external assurance, regulator approval, or production maturity.

9. Revision Note - 04 October 2026

This corrected reissue preserves legacy document identifier TCR-UAIF-014 for citation continuity and regenerates the dictionary against the frozen canonical uaif-core-v1.0.json schema (SHA-256 55056e7cfa4cf4b76cc4656833cb5b360a1b40fa90f23488d488409ccebeeca). It replaces the withdrawn July schema filename/checksum, removes Observation and severity_justification, adds profile and extensions, corrects the Incident/Enterprise/Core conditional model, adds SOC_SIEM and AI_Security extension gating, corrects the score-precision description, 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.