Defensible Analytics Control Specification

Controls for Accountable Information and Defensible Decision Paths

Defensible Analytics Control Specification

Companion doctrine: The Defensible Analytics Control Specification Manifesto

Primary doctrine: Discovery is not certification.

Core assertion: If identity is unstable, meaning is ambiguous, relationships have not passed accountability controls, or AI outputs cannot be tested against a governed context contract, the decision path is not defensible.

Release status
Status: v1.4 Release Candidate. This release is published for public review and field validation. It clarifies responsibility assignment, public-facing terminology, and evidence-accountability language while preserving the DACS control IDs, control-result vocabulary, Gate readiness states, and core conformance model. It remains subject to revision before final v1.4 designation.

This release is not a legal certification instrument, product certification program, regulatory compliance scheme, or final DataVaultAlliance specification.

Document intent: Lean, implementable, binary, vendor-neutral, evidence-based control specification.

What Is DACS?

DACS is a control specification that combines mature disciplines without replacing them: data governance, metadata management, taxonomy, ontology, provenance, data quality, identity, analytics controls, AI output evaluation, drift detection, audit evidence, and decision-path reconstruction. DACS does not claim that those disciplines are absent or ineffective. It defines the control evidence required when their outputs are used in a stated decision scope.

Acknowledgments

DataVaultAlliance Holdings LLC may acknowledge reviewers who provide critique and subject-matter feedback during the review process. Reviewer feedback is advisory. DataVaultAlliance Holdings LLC retains editorial control over the specification and may revise, defer, reject, or reframe feedback based on DACS doctrine, field evidence, legal review, and release governance.

Abstract

The Defensible Analytics Control Specification, or ***DACS***, defines binary controls for determining whether decision evidence is ready for certified use within a stated decision scope. DACS is vendor-neutral and implementation-neutral. It is not a product category, software platform, consulting slogan, data model, governance program, or AI tool.

DACS exists because modern enterprise systems can connect, move, catalog, model, visualize, automate, and infer from information without, by themselves, proving that the identities, meanings, classifications, relationships, context, authority, and evidence used in a decision path are governed and defensible for the stated use.

DACS defines the controls and evidence obligations used to establish whether evidence is ready for certified use. Accountable authorities own the obligation. Governed human, procedural, or automated mechanisms execute the controls, record the results, and preserve the evidence needed to reconstruct and challenge the decision path when necessary.

DACS controls may be executed manually, procedurally, automatically, or through hybrid workflows. The implementation mechanism does not determine conformance. Conformance requires testable evidence, a recorded control result, and the applicable Gate readiness state for the stated decision scope.

Table of Contents

Abstract 2
Introduction 4
1. Specification Architecture 4
2. Scope 6
3. Normative Language and Conformance 6
4. Terms and Definitions 8
5. Profile 1: Core Decision-Scope Controls 9
6. Profile 2: Extended Taxonomy Controls 13
7. Profile 3: Extended Ontology Controls 17
8. Profile 4: AI Context Contract Controls 21
9. Evidence Model 24
10. Exceptions and Constraints 25
11. Recommended Practices (Informative) 25
12. Positioning Against Existing Methods and Tools 25
13. Annex A: MVP Control Checklist (Informative) 26
14. Annex B: Example Decision Scope (Informative) 27
15. Annex C: DACS Adoption Maturity Levels (Informative) 28
16. Annex D: Drafting Tests for Future DACS Controls 28
17. Annex E: External Reference Boundary and Evidence Alignment Rules 29
18. Annex F: Planned Companion Documents and Future Profiles (Informative) 30
19. Annex G: Public Comment Template 31
Closing Normative Boundary 31

Introduction

Enterprises increasingly rely on analytics, AI-assisted recommendations, automated decision paths, and agentic execution to support operational, financial, regulatory, and strategic decisions. These decisions depend on information moving through complex environments that include operational systems, SaaS platforms, data warehouses, lakehouses, data fabrics, data mesh domains, semantic layers, catalogs, BI tools, machine learning pipelines, workflow engines, and AI agents.

These technologies are valuable. They do not automatically make decisions defensible.

DACS begins with a clear doctrine: discovery is not certification. Discovery identifies candidate identities, classifications, relationships, patterns, signals, risks, and decision paths. Certification is the recorded determination that those candidates have satisfied defined controls and evidence requirements for a stated use.

The purpose of extending taxonomy and ontology is not documentation. The purpose is to create governed semantic-to-physical and relationship-to-physical maps that allow decision evidence, analytic outputs, AI outputs, generated classifications, inferred relationships, agentic actions, and drift conditions to be tested through Gates.

DACS permits discovery while separating discovery from certified decision use. Candidate evidence may be captured, explored, reviewed, remediated, or routed through additional Gates, but it must not be treated as certified evidence until the required controls pass or an approved constrained-use exception exists.

1. Specification Architecture

DACS is organized into conformance profiles. Profiles keep the specification narrow enough to apply to one decision scope while ensuring that material concepts, identities, relationships, AI behavior, and evidence are not left untested.

Profile	Applies when	Primary question	Control families
Core Decision-Scope Controls	Every DACS decision scope.	Is the decision scope bounded, evidenced, gated, and reconstructable?	Scope, Semantic Contract, identity, context, Gates, evidence, certification record.
Extended Taxonomy Controls	Material business concepts, terms, labels, classifications, identifiers, or meanings affect the decision path.	Can governed meaning be tied to the physical data estate and tested for the decision scope?	Classification, labels, semantic grain, physical anchors, source systems, identifiers, ownership, risk, usage boundaries.
Extended Ontology Controls	Material relationships or relationship paths affect the decision path.	Can governed relationship meaning be tied to physical relationship evidence and tested for the decision scope?	Relationship type, orientation, vector, provenance, joins, source evidence, permitted/prohibited paths, constraints, compatibility.
AI Context Contract Controls	AI, machine inference, generated classifications, generated relationships, agents, or AI-assisted recommendations affect the decision path.	Can AI behavior be tested against governed meaning, permitted relationships, valid context, and Gate criteria?	Binding AI Context Contract, AI inputs/outputs, drift, violations, execution trace, agent authority.

1.1 Document Architecture and Companion Materials

The DACS Specification is the normative control source. It defines what must be true, evidenced, gated, and reconstructable before evidence can be treated as ready for certified use within a stated decision scope.

Companion materials support use of this specification but do not replace it. The Manifesto explains doctrine; the Executive Brief explains sponsorship rationale; practitioner handouts, Gate templates, assessment workbooks, adoption guides, reference-alignment guidance, partner enablement materials, pilot kits, and future companion specifications provide examples, implementation patterns, training support, and maturity guidance. Partner-facing materials and pilot kits are designed to lower the cost of first adoption without relaxing normative control requirements.

Unless explicitly incorporated into a normative DACS control, companion materials are informative. A control passes only when the evidence required by the applicable control exists and satisfies the Pass condition for the stated decision scope.

1.2 Control Verification Method

Each normative DACS control is verified through evidence inspection and decision-scope comparison. The accountable authority owns the obligation. An assessor or governed human, procedural, or automated control mechanism shall determine applicability, inspect the required evidence, confirm scope binding, verify ownership or authority, check version or effective-period validity, compare the evidence to the Pass and Fail statements, record Pass, Fail, or Not Applicable with reason, apply the applicable Gate logic, and preserve evidence references in the Certification Record. DACS defines the control requirement and evidence criteria; it does not perform the assessment or create its own authority.

Each normative control is supported by companion remediation guidance that explains common failure modes, remediation options, repeatable-fix patterns, controlled-disposition paths, examples, and non-examples without modifying the control requirement.

Detailed examples, sampling methods, assessor checklists, and worked artifacts belong in the DACS Assessment Guide and Example Workbook. Training may teach application, but the normative test remains the control requirement, Pass condition, Fail condition, and evidence required by this specification. Examples, workbooks, pilot kits, and training materials illustrate how controls may be applied; they do not create, modify, or relax normative DACS requirements unless incorporated into a future DACS release.

1.3 Sparse Specification Principle

DACS is intentionally sparse. It does not attempt to restate adjacent standards, prescribe every implementation pattern, or teach every assessment technique. It defines the mandatory control points that must be evidenced when adjacent disciplines, tools, models, standards, or governance practices produce information used in a material decision path.

1.4 Low-Friction Adoption and Ecosystem Boundary

DACS is designed for low-friction adoption. A first DACS use may begin with one decision scope, one Gate, one evidence packet, and one readiness decision. This specification intentionally avoids requiring a complete enterprise implementation, a new platform, or full companion-specification adoption before first use.

Training partners, implementation partners, vendors, and internal teams may use DACS companion materials to teach, implement, pilot, or automate the controls. Those materials are informative unless incorporated into a normative control. Partner participation, training authorization, or tool support does not create DACS conformance by itself; conformance remains tied to evidence, control result, Gate result, readiness state, and certification record for a stated decision scope.

2. Scope

2.1 In Scope

- Determining whether decision evidence is ready for certified use within a stated decision scope.
- Binary control requirements for identity, meaning, classification, relationship paths, preserved context, Gate records, evidence records, and reconstructable decision paths.
- Conformance profiles for Core Decision-Scope Controls, Extended Taxonomy Controls, Extended Ontology Controls, and AI Context Contract Controls.
- Gate readiness states: ***Proceed, Caution, Stop,*** and ***Quarantined***.
- Implementation-neutral evidence requirements that may be satisfied through many technical or procedural mechanisms.
- Control records and certification records that can be inspected, queried, exported, or reconstructed by authorized reviewers or downstream systems.

2.2 Out of Scope

- Certification of a software product, platform, vendor, data model, or architecture as DACS-compliant in general.
- A legal guarantee that a decision is correct, risk-free, compliant with external law, or immune from challenge.
- Replacement of data governance, data quality, metadata management, taxonomy, ontology, lineage, AI governance, risk management, architecture, or stewardship disciplines.
- Mandating a specific physical implementation such as a graph database, catalog, semantic layer, data warehouse, lakehouse, data vault, or workflow platform.
- Defining a full organizational operating model, job family, training curriculum, or certification program.
- Establishing a legal or regulatory compliance scheme unless such authority is separately granted and published by DataVaultAlliance Holdings LLC.

3. Normative Language and Conformance

3.1 Normative Terms

The terms shall and must indicate mandatory requirements. The terms should, may, example, rationale, recommended practice, informative, or guidance indicate non-normative material unless explicitly referenced by a mandatory control.

3.2 Binary Rule

Every normative DACS control shall be testable as Pass or Fail for a stated decision scope. If a requirement cannot be tested as true or false, it shall not be used as a normative control until it is rewritten as an observable evidence requirement.

A control may be Not Applicable only when the profile or condition requiring the control is not in scope. Not Applicable is not a Pass. It must be recorded with the reason it does not apply.

An exception may allow constrained use, but it does not convert a failed control into a passed control. The certification record shall preserve the failed condition, exception authority, constraint, review date, and resulting readiness state.

3.3 Prohibited Subjective Sufficiency Language

Normative controls shall not rely on phrases such as accountable enough, trusted enough, appropriate enough, strong enough, sufficient enough, high quality, reasonable, adequate, or acceptable unless the control defines the evidence, threshold, rule, authority, or Gate result that makes the phrase testable.

3.4 Control Results and Gate Readiness States

Control results are Pass, Fail, or Not Applicable. Gate readiness states are Proceed, Caution, Stop, and Quarantined. These are separate concepts.

State	Meaning	Allowed use
Proceed	Applicable controls have passed for the stated scope.	Use is permitted within the approved scope.
Caution	Evidence may move forward only with recorded constraints, monitoring, remediation, or approved exception handling.	Use is constrained and must preserve the reason, authority, and review condition.
Stop	A control failure, prohibition, missing authority, invalid context, or contract violation prevents certified use for the stated decision scope.	Use is not permitted for the material decision scope.
Quarantined	Candidate evidence is known, discovered, inferred, generated, imported, retrieved, or available but has not passed required controls.	Evidence may be explored, reviewed, remediated, or routed through additional Gates but not relied on for material decisions.

Quarantined protects discovery by allowing candidate evidence to be captured and reviewed without treating it as certified. Stop protects decisions by preventing failed, prohibited, or unauthorized evidence from being used.

3.5 Conformance Rule

DACS conformance is determined for a stated decision scope, not for an enterprise, platform, vendor, model, or repository in general. Full DACS conformance for a decision scope requires all applicable mandatory controls to Pass or be recorded as Not Applicable with reason. A failed applicable control with an approved exception may allow constrained use and a Caution readiness state, but it shall not be represented as full DACS conformance until the failed control passes or is no longer applicable.

3.6 Adoption Maturity Is Informative

DACS separates control conformance from adoption maturity. Control conformance is binary for a stated decision scope. Adoption maturity describes how repeatably, broadly, automatically, and operationally the organization applies DACS over time.

The adoption maturity levels in Annex C are informative. They do not create certification status, legal compliance status, product certification, or vendor certification unless a separate DACS assessment or certification program is formally published. The DACS Adoption and Conformance Guide is the intended companion document for full maturity assessment patterns, artifacts, and progression guidance.

3.7 Principle of Non-Automatic Trust

Discovery may be automated. Certification shall not be automatic merely because discovery occurred. Certified use under DACS requires an evidence-backed Gate result anchored in approved meaning, authority, rules, thresholds, stewardship, or authorized operating procedures.

3.8 Public Claims Boundary

Public claims about DACS shall preserve the distinction between conformance, alignment, support, certification, training authorization, partner status, and vendor or product claims.

- DACS-conformant decision scope may be claimed only when the certification record shows all applicable mandatory controls Pass or are Not Applicable with reason for the stated decision scope.
- DACS-aligned may describe informative materials, practices, tools, or implementation efforts that intentionally follow DACS language but do not claim DACS conformance.
- DACS-supporting tool, platform, service, or evidence source means the tool or service may provide evidence, workflows, controls, or records used in DACS assessment or control execution. It does not mean the tool, platform, service, vendor, or implementation is broadly DACS-conformant or DACS-certified.
- DACS Certified, DACS-certified vendor, DACS-certified platform, DACS-certified product, DACS-compliant platform, and similar claims shall not be used unless DataVaultAlliance Holdings LLC has published an applicable certification, assessment, vendor-adherence, or claims program.
- Authorized training or partner status permits approved education, enablement, or delivery activity only within the scope granted. It does not create control conformance, product certification, vendor certification, or certification of a customer decision scope by itself.

4. Terms and Definitions

4.1 DACS. Defensible Analytics Control Specification. A vendor-neutral, implementation-neutral control specification for determining whether decision evidence is ready for certified use within a stated decision scope.

4.2 Defensible Analytics. Analytics, AI-assisted recommendations, automated actions, or decision outputs whose identity, meaning, classification, relationship path, context, Gate decisions, and evidence can be reconstructed and verified for a stated decision scope. DACS does not guarantee that every result is correct.

4.3 SIM. System of Information Management. The enterprise system that governs information as a business asset by managing meaning, identity, classification, relationships, context, continuity, readiness, controls, delivery, and accountability.

4.4 SIM-ZONE. A defined state or area of information readiness within SIM. Each SIM-ZONE has entry criteria, exit criteria, permitted uses, and Gate controls.

4.5 Gate. An enforceable control point that applies approved DACS control criteria or Gate logic to evidence and records a readiness state before information moves forward or is used for a stated decision scope. A Gate may be manual, procedural, automated, system-enforced, or hybrid. A Gate does not create its own authority; it operates under the responsible authority or approved rule.

4.6 Discovery. The identification of candidate identity, classification, relationship, pattern, signal, risk, output, or decision evidence that has not yet satisfied DACS controls for certified use.

4.7 Certification. The recorded determination that an identity, classification, relationship, context, evidence item, or decision path has satisfied applicable DACS controls and evidence requirements for a stated use.

4.8 Semantic Contract. The governed agreement that defines how an enterprise interprets business concepts, identifies instances of those concepts, classifies them, relates them, constrains their use, preserves their context, and tests their readiness for decision use.

4.9 Extended Taxonomy. A DACS Extended Taxonomy defines governed classification and physical semantic anchoring. It extends controlled business language into the physical data estate by binding approved concepts to source systems, physical attributes, business identifiers, semantic grain, ownership, provenance, and resolution rules that represent those concepts in real systems.

4.10 Extended Ontology. A DACS Extended Ontology defines governed relationship meaning and physical relationship anchoring. It extends ontology into the physical data estate by connecting approved relationship types, source systems, business identifiers, physical joins, relationship attributes, semantic grain, provenance, constraints, evidence, and permitted relationship paths.

4.11 Business Identity. A durable identity rule, stable business identifier, or approved resolution method used to distinguish a specific business instance across systems and time at a declared semantic grain.

4.12 Semantic Grain. The business level at which a concept, identity, classification, relationship, or count is unique, meaningful, and comparable for the stated decision scope.

4.13 Physical Attribution. Source-level evidence identifying where a value, code, event, record, document, assertion, relationship, or identifier came from. It may include source system, source domain, object, table, field, file, event, message, API, code set, reference package, stewardship record, or equivalent source reference.

4.14 Relationship Assertion. A declared, inferred, discovered, imported, or derived claim that two or more governed concepts or instances are related in a specific way for a stated decision scope.

4.15 Relationship Vector. A recorded evaluation of a material relationship containing Strength, Confidence, and Orientation for a stated decision scope.

4.16 Strength. The practical force or influence of a relationship for a stated decision scope, measured or assessed against defined criteria.

4.17 Confidence. The evidence quality, support, repeatability, recency, and reliability behind a relationship for a stated decision scope, measured or assessed against defined criteria.

4.18 Orientation. The directional nature of a relationship, such as authority, sequence, dependency, ownership, lineage, hierarchy, flow, support, inclusion, identification, reconciliation, constraint, or causality when causality has been separately established.

4.19 Binding AI Context Contract. The governed context contract used to test AI behavior for a stated decision scope. It combines Extended Taxonomy, Extended Ontology, Business Identity, preserved context, relationship vectors, permitted paths, prohibited paths, governance constraints, Gate criteria, drift rules, and evidence requirements.

4.20 Context Enforcement Point. A system, service, workflow, Gate, API layer, orchestration layer, semantic layer, governance process, or equivalent mechanism that applies DACS context rules before information, context, relationships, tools, actions, or AI outputs are used for a stated decision scope.

4.21 Decision Path. The recorded chain of identity, classification, relationships, context, Gate decisions, evidence, and output used to produce a material analytic, recommendation, action, or decision.

4.22 Decision Execution Trace. A structured evidence record that captures the request, actor or agent, inputs, context, tools or APIs where applicable, model or process version where applicable, governed concepts used, relationships traversed, Gate results, output, action, and certification or exception state.

4.23 Certification Record. A structured evidence record that captures decision scope, applicable profiles, control results, evidence references, Gate results, readiness state, responsible authority or approved rule reference, timestamp, and review condition.

5. Profile 1: Core Decision-Scope Controls

Purpose: Establish the minimum control foundation for any DACS decision scope. Core controls apply to every DACS conformance evaluation.

CORE-001: Decision Scope Is Declared

Requirement: Each DACS conformance evaluation shall declare the decision scope being evaluated.

Pass: Pass if the record identifies the business domain, business decision or use, stated grain, in-scope use, out-of-scope use, owner, and decision-scope identifier.

Fail: Fail if the scope, grain, owner, or boundaries of use are missing or ambiguous.

Evidence required: Decision-scope record, declared grain, owner, in-scope statement, out-of-scope statement.

Rationale: Controls cannot be tested unless the decision scope is explicit.

CORE-002: Semantic Contract Exists

Requirement: A decision scope shall have an identified Semantic Contract before evidence is certified for material use.

Pass: Pass if the Semantic Contract has an identifier, owner, version, decision-scope mapping, and referenced components required by the applicable profiles.

Fail: Fail if no Semantic Contract exists, ownership or version is missing, or it is not linked to the decision scope.

Evidence required: Semantic Contract record, owner, version, decision-scope mapping.

Rationale: Without a Semantic Contract, meaning, identity, relationship, context, and Gate controls cannot be tested consistently.

CORE-003: Applicable Profiles Are Declared

Requirement: Each conformance evaluation shall declare which DACS profiles apply.

Pass: Pass if the certification record identifies Core plus each applicable Extended Taxonomy, Extended Ontology, and AI Context Contract profile.

Fail: Fail if profile applicability is missing, ambiguous, or inconsistent with the decision path use of concepts, identities, relationships, AI, inference, automation, or agentic action.

Evidence required: Profile applicability record, decision-scope mapping, certification record.

Rationale: Profiles keep DACS narrow while preventing material controls from being skipped.

CORE-004: Business Identity Anchors Exist Where Required

Requirement: Each identity-bearing concept used in a material decision path shall have a Business Identity anchor.

Pass: Pass if each identity-bearing concept is linked to a stable business identifier, durable identity rule, composite identifier rule, approved resolution method, or equivalent identity evidence.

Fail: Fail if a concept requires identity for the decision scope and lacks an approved identity anchor.

Evidence required: Identity rule, business identifier mapping, composite identifier rule, identity-resolution record, or identity authority declaration.

Rationale: Without identity, the enterprise cannot reliably compare history, reconcile systems, reconstruct decisions, or defend analytics.

CORE-005: Semantic Grain Is Declared for Identity-Bearing Evidence

Requirement: Each material Business Identity shall declare the semantic grain at which the identity is unique and meaningful for the decision scope.

Pass: Pass if the identity record states the business level of uniqueness or aggregation and links that grain to the decision scope.

Fail: Fail if the identity is used without declaring the grain at which it is unique, meaningful, and comparable.

Evidence required: Identity record, semantic grain declaration, uniqueness expectation, decision-scope mapping.

Rationale: Identity failures often occur when different grains are treated as equivalent.

CORE-006: Physical Attribution Is Recorded Where Required

Requirement: Each material evidence item shall record the physical attribution required for the decision scope.

Pass: Pass if the evidence item records the source-level evidence required to locate, interpret, and test the evidence for the decision scope.

Fail: Fail if a material evidence item is used without required source-level evidence.

Evidence required: Source reference, source system or domain, object/table/file/API/event/document/field/code set or equivalent reference, decision-scope mapping.

Rationale: Material decision evidence must be traceable to its source at the level needed for the stated decision scope. DACS requires sufficient physical attribution for that traceability without requiring unnecessary low-level technical mapping.

CORE-007: Logical-to-Conceptual Binding Exists Where Required

Requirement: Each logical information element used in a material decision path shall map to an approved business concept.

Pass: Pass if each logical information element maps to an approved business concept with owner, version, source reference where required, and decision-scope applicability.

Fail: Fail if the logical element lacks a business concept mapping, maps only to a local term, or maps to an unapproved or ambiguous concept.

Evidence required: Logical-to-conceptual mapping record, business concept identifier, owner, version, source reference where required, decision-scope mapping.

Rationale: Logical meaning must be tied to governed business meaning before it supports certification.

CORE-008: Context Is Preserved

Requirement: Each certified decision path shall preserve the minimum context required to reconstruct the state of information at the time of use.

Pass: Pass if the record includes timestamp, source assertion, Semantic Contract version, taxonomy version, ontology version where applicable, identity rule, Gate decision, readiness state, and decision-scope identifier.

Fail: Fail if any required context element is missing or cannot be retrieved.

Evidence required: Context record, timestamps, source record, semantic version references, Gate record, readiness state.

Rationale: Without preserved context, the enterprise cannot explain why a decision was valid when made.

CORE-009: Gate Decision Is Recorded

Requirement: Each transition toward certified use shall produce a recorded Gate decision.

Pass: Pass if the Gate record includes Gate ID, decision scope, evaluated controls, result, timestamp, responsible authority or approved automated rule, and resulting readiness state.

Fail: Fail if the transition occurs without a Gate record or if the Gate record is incomplete.

Evidence required: Gate log, control results, timestamp, responsible authority or approved rule reference, readiness state.

Rationale: Gates convert governance from policy into operational control.

CORE-010: Decision Path Is Reconstructable

Requirement: Each certified analytic output, AI-assisted recommendation, automated action, or decision path shall be linked to a reconstructable decision path.

Pass: Pass if the decision path can reproduce or explain the identities, classifications, relationships where applicable, context, Gate decisions, evidence, output state, and applicable exceptions at the time of use.

Fail: Fail if any required element cannot be retrieved or if reconstruction depends solely on undocumented human memory.

Evidence required: Decision path record, identity references, taxonomy references, ontology references where applicable, context record, Gate records, output record, exception record where applicable.

Rationale: A result that cannot be reconstructed may be useful, but it is not defensible under DACS.

CORE-011: Certification Record Exists

Requirement: Each claim that evidence or a decision path is ready for certified use under DACS shall have a certification record.

Pass: Pass if the record includes decision scope, applicable profiles, applicable controls, pass/fail/not-applicable results, evidence links, readiness state, responsible authority or approved rule reference, timestamp, and review condition.

Fail: Fail if certified use under DACS is claimed without a certification record.

Evidence required: Certification record, control results, evidence links, responsible authority or approved rule reference, timestamp, review condition.

Rationale: A claim of certified use without an evidence record is an assertion, not a DACS conformance outcome.

CORE-012: Certification Record Is Structured

Requirement: Each certification record shall be structured so that decision scope, control IDs, control results, evidence references, readiness state, timestamp, and responsible authority or approved rule reference are machine-readable or exportable as a data object.

Pass: Pass if the record can be consumed, queried, exported, or exchanged as structured data by an authorized downstream process or reviewer.

Fail: Fail if certification exists only as unstructured narrative, slide content, email approval, or undocumented assertion.

Evidence required: Structured certification record, exportable control result object, metadata record, API response, table record, graph record, JSON/XML/YAML document, or equivalent structured evidence.

Rationale: A certification record must be actionable evidence, not merely a presentation artifact.

CORE-013: Material Semantic Binding Change Triggers Review

Requirement: Each certified decision path shall define change-detection rules for physical attribution, logical binding, conceptual binding, Semantic Contract, taxonomy, ontology, identity rule, or context changes that could affect certification.

Pass: Pass if material changes trigger review, Gate reassessment, readiness-state update, or certification-status update.

Fail: Fail if a certified decision path can continue as certified after a material binding change without detection, review, or Gate reassessment.

Evidence required: Change-detection rule, source-change event where applicable, mapping-change log, Semantic Contract version-change log, Gate reassessment record, status update.

Rationale: Semantic bindings can break silently when physical, logical, conceptual, taxonomy, ontology, identity, or context structures change.

CORE-014: Identity Resolution Produces Determinate Results

Requirement: Each identity-resolution method used in a certified decision path shall produce a determinate result for the same input, rule set, threshold, and decision scope.

Pass: Pass if the method returns the same identity result or the same unresolved/exception result when the same inputs, rules, thresholds, and scope are applied.

Fail: Fail if the method produces inconsistent identity outcomes without recorded reason, version change, threshold change, or exception handling.

Evidence required: Identity-resolution method, rule set, threshold, test result, exception record where applicable.

Rationale: Material decisions require repeatable identity outcomes.

CORE-015: Business Concept Is Not Assumed to Be Business Identity

Requirement: A business concept shall not be treated as a Business Identity unless identity evidence is recorded.

Pass: Pass if each identity-bearing use has a distinct identity rule, identifier, or approved resolution method beyond the existence of a concept label.

Fail: Fail if a concept name, taxonomy node, glossary term, or classification is used as identity evidence without an approved identity anchor.

Evidence required: Business concept record, identity rule, identifier mapping, resolution method, decision-scope mapping.

Rationale: A concept defines meaning; identity distinguishes a specific instance.

CORE-016: Discovered Evidence Is Quarantined Until Governed

Requirement: Discovered, inferred, generated, retrieved, imported, or available evidence shall not be treated as certified until applicable controls pass or an approved constrained-use exception is recorded.

Pass: Pass if candidate evidence is assigned Quarantined, reviewed through applicable Gates, or recorded with a constrained-use exception before material use.

Fail: Fail if candidate evidence is used as certified evidence without Gate results or approved exception handling.

Evidence required: Candidate evidence log, Quarantined state, Gate result, exception record where applicable, owner or review authority, next action.

Rationale: Quarantined protects discovery while preventing untested evidence from being treated as ready for certified use by default.

6. Profile 2: Extended Taxonomy Controls

Purpose: Determine whether governed business meaning and classification are sufficiently anchored to the physical data estate to support decision-scope use. Extended Taxonomy Controls apply when concepts, classifications, labels, identifiers, semantic grain, or physical representations materially affect the decision path.

ET-001: Taxonomy Scope and Purpose Are Declared

Requirement: Each Extended Taxonomy evaluation shall declare the taxonomy scope and purpose for the stated decision scope.

Pass: Pass if the record identifies the taxonomy scope, purpose, owner, version, applicable decision scope, and excluded meanings.

Fail: Fail if taxonomy scope or purpose is missing, ambiguous, or not linked to the decision scope.

Evidence required: Taxonomy scope record, purpose statement, owner, version, decision-scope mapping.

Rationale: Classification cannot be tested if its scope and purpose are not declared.

ET-002: Taxonomy Node Type Is Declared

Requirement: Each material taxonomy node shall declare its node type.

Pass: Pass if each node is identified as concept, category, domain, subdomain, classification, label, alias, deprecated term, code set, identifier concept, or other approved node type.

Fail: Fail if a material node lacks a declared type or uses an unapproved type.

Evidence required: Taxonomy node record, node type list, approval record.

Rationale: Node type controls how the node may be interpreted and used.

ET-003: Business Meaning Is Recorded

Requirement: Each material taxonomy node shall have recorded business meaning.

Pass: Pass if the record includes approved definition, semantic boundary, owner, version, and decision-scope applicability.

Fail: Fail if meaning is missing, ambiguous, only technical, only local, or not approved for the decision scope.

Evidence required: Definition record, semantic boundary, owner/steward approval, version, decision-scope mapping.

Rationale: Labels alone are insufficient evidence of governed business meaning or readiness for decision use.

ET-004: Controlled Label and Language Evidence Are Recorded

Requirement: Each material concept or classification shall record authoritative labels and non-authoritative variants.

Pass: Pass if preferred label, permitted synonyms, aliases, deprecated terms, local variants, and prohibited labels where applicable are recorded.

Fail: Fail if the decision path depends on labels that are unapproved, ambiguous, deprecated, or not linked to an approved concept.

Evidence required: Label record, synonym/alias record, deprecated/prohibited label record where applicable, approval record.

Rationale: Controlled language reduces semantic ambiguity across systems and decision paths.

ET-005: Semantic Domain and Boundary Are Declared

Requirement: Each material concept or classification shall declare its semantic domain and boundary.

Pass: Pass if the record states domain, boundary rules, included meanings, excluded meanings, and overlap/disjointness rules where material.

Fail: Fail if domain or boundary is missing where the distinction affects decision use.

Evidence required: Semantic domain record, boundary rule, overlap/disjointness rule where applicable.

Rationale: The enterprise must know where one meaning ends and another begins.

ET-006: Semantic Grain Is Declared Where Material

Requirement: Each material concept, identifier, classification, count, or integration point shall declare semantic grain when grain affects decision use.

Pass: Pass if the record states the business level at which the concept or identifier is unique, meaningful, counted, integrated, or compared.

Fail: Fail if concepts, identifiers, or counts with different grains are treated as equivalent without a declared and approved rule.

Evidence required: Semantic grain record, decision-scope mapping, equivalence rule where applicable.

Rationale: Same names do not guarantee same grain or same meaning.

ET-007: Physical Semantic Anchors Are Recorded Where Required

Requirement: Each material concept or classification shall record physical semantic anchors when physical representation affects the decision scope.

Pass: Pass if the record identifies source systems and physical representations such as tables, fields, files, messages, events, APIs, documents, code sets, or equivalent evidence objects required by the scope.

Fail: Fail if a material concept is certified for decision use without required physical representation evidence.

Evidence required: Source-system reference, physical attribute/object reference, data asset reference, code-set or reference-data evidence where applicable.

Rationale: The Extended Taxonomy closes the gap between governed meaning and real-world data.

ET-008: Business Identifier or Key Evidence Is Recorded Where Applicable

Requirement: Where a concept is represented by identifiers or keys, the Extended Taxonomy shall record identifier meaning and approved key evidence for the decision scope.

Pass: Pass if each material identifier records business meaning, semantic grain, source-system representation, value-format expectation where material, and authority or resolution rule.

Fail: Fail if identifier fields or keys are treated as equivalent by name alone or without required evidence.

Evidence required: Identifier record, source-key mapping, semantic grain record, authority or resolution rule.

Rationale: Business keys often differ by system even when they appear semantically similar.

ET-009: Source-System Representation Is Recorded Where Required

Requirement: Each material concept shall identify source-system representations required for the decision scope.

Pass: Pass if the record identifies source systems, local terms, local attributes, local codes, and representation differences required to test the decision scope.

Fail: Fail if the concept is certified without the source-system representation needed to support the decision path.

Evidence required: Source-system mapping, local term/attribute mapping, source representation notes, decision-scope mapping.

Rationale: A single governed concept may be represented differently across source systems.

ET-010: Resolution or Mastering Rule Is Recorded Where Applicable

Requirement: Where multiple source representations or identifiers must be treated as the same concept or instance, the resolution or mastering rule shall be recorded.

Pass: Pass if the record includes approved rule, authority, threshold where applicable, exception handling, and decision-scope applicability.

Fail: Fail if source representations are merged, counted, mastered, or treated as equivalent without an approved rule.

Evidence required: Resolution rule, mastering rule, authority record, threshold record where applicable, exception record.

Rationale: Integration requires tested equivalence, not assumed equivalence.

ET-011: Ownership and Stewardship Are Recorded

Requirement: Each material taxonomy node shall record business ownership or stewardship authority.

Pass: Pass if owner or steward, authority scope, approval responsibility, and review condition are recorded.

Fail: Fail if a material concept or classification lacks authority for approval, change, or dispute resolution.

Evidence required: Owner/steward record, authority scope, review condition.

Rationale: Accountability requires a recorded authority.

ET-012: Governance Constraints and Usage Boundaries Are Recorded

Requirement: Each material taxonomy node shall record governance constraints and usage boundaries required by the decision scope.

Pass: Pass if permitted use, prohibited use, constrained use, policy constraints, privacy/security constraints where applicable, and decision-scope boundaries are recorded.

Fail: Fail if a concept or classification is used outside approved boundaries or without required constraints.

Evidence required: Constraint record, usage-boundary record, policy reference where applicable, decision-scope mapping.

Rationale: A concept may be valid in one context and invalid in another.

ET-013: Provenance Is Recorded

Requirement: Each material taxonomy assertion shall record provenance.

Pass: Pass if the record identifies the source of the assertion, approving authority or approved rule reference, version, timestamp or effective period, and decision-scope applicability.

Fail: Fail if material meaning, label, classification, identifier, or boundary evidence lacks provenance.

Evidence required: Provenance record, responsible authority or approved rule reference, version, effective date or timestamp.

Rationale: Decision readiness depends on knowing where meaning came from and when it was valid.

ET-014: Readiness State Is Declared

Requirement: Each material taxonomy node used in a decision path shall have a recorded readiness state for the decision scope.

Pass: Pass if the node is assigned Proceed, Caution, Stop, or Quarantined with reason, responsible authority or approved rule reference, timestamp, and review condition where required.

Fail: Fail if a material node is used without a readiness state or if the state is unsupported by evidence.

Evidence required: Readiness state record, Gate result, reason, responsible authority or approved rule reference, timestamp, review condition.

Rationale: Governed meaning must have a decision-scope disposition.

ET-015: Semantic Risk Is Recorded Where Present

Requirement: Semantic risk shall be recorded when ambiguity, conflict, overlap, deprecated meaning, local variation, or known misuse may affect the decision scope.

Pass: Pass if each material semantic risk has a risk description, affected scope, readiness disposition, owner, and remediation or exception record.

Fail: Fail if known semantic risk affects the decision scope and is not recorded.

Evidence required: Semantic risk record, owner, readiness disposition, remediation or exception record.

Rationale: Unrecorded semantic risk can become hidden decision risk.

ET-016: Relationship Seeds Are Not Treated as Certified Relationships

Requirement: Candidate relationship evidence discovered during taxonomy work shall not be treated as a certified relationship until applicable Extended Ontology controls pass.

Pass: Pass if relationship seeds are recorded as candidate or Quarantined evidence and routed to Extended Ontology review when material.

Fail: Fail if a relationship seed is used as an approved relationship path without applicable ontology controls.

Evidence required: Relationship seed record, Quarantined state where applicable, ontology review record, Gate result.

Rationale: Taxonomy can expose possible relationships; ontology controls determine whether relationship use is defensible.

ET-017: Taxonomy Change Triggers Reassessment

Requirement: Material taxonomy changes shall trigger reassessment of affected decision scopes.

Pass: Pass if changes to meaning, label, boundary, grain, identifier, source representation, ownership, constraint, or readiness state trigger review or Gate reassessment for affected scopes.

Fail: Fail if certified decision paths continue after a material taxonomy change without review.

Evidence required: Taxonomy change log, impact analysis, Gate reassessment record, certification update.

Rationale: Meaning changes can invalidate previously certified evidence.

7. Profile 3: Extended Ontology Controls

Purpose: Determine whether material relationships and relationship paths are governed, evidenced, physically anchored, oriented, constrained, and ready for decision-scope use. Extended Ontology Controls do not prevent relationship discovery. They prevent discovered, inferred, imported, declared, or derived relationships from being treated as ready for certified use by default.

EO-001: Relationship Candidate Is Not Treated as Certified

Requirement: A relationship candidate shall not be treated as certified until applicable Extended Ontology controls pass or an approved constrained-use exception exists.

Pass: Pass if relationship candidates are recorded as Quarantined, reviewed, constrained, rejected, or approved through Gate evidence before material use.

Fail: Fail if a candidate, inferred, discovered, imported, or derived relationship is used as certified evidence without applicable Gate results.

Evidence required: Relationship candidate log, readiness state, Gate result, exception record where applicable.

Rationale: Discovery is valuable, but discovery does not establish readiness for certified use.

EO-002: Relationship Type Is Governed

Requirement: Each material relationship shall map to an approved relationship type for the decision scope.

Pass: Pass if the relationship type is defined, owned, versioned, and approved for the stated scope.

Fail: Fail if the relationship uses an undefined, ambiguous, prohibited, or unapproved type.

Evidence required: Relationship type record, owner, version, approval record, decision-scope mapping.

Rationale: A relationship cannot be tested if its type is not governed.

EO-003: Relationship Orientation Is Declared

Requirement: Each material relationship shall declare orientation.

Pass: Pass if orientation is recorded as direction, authority, sequence, dependency, ownership, lineage, hierarchy, flow, support, inclusion, identification, reconciliation, constraint, causality where separately established, or another approved orientation.

Fail: Fail if orientation is missing or if an oriented relationship is used as symmetrical without approval.

Evidence required: Orientation record, orientation type, approval record, decision-scope mapping.

Rationale: Many failures occur when association is mistaken for authority, sequence is mistaken for cause, or a one-way relationship is treated as symmetrical.

EO-004: Relationship Assertion Provenance Is Recorded

Requirement: Each material relationship assertion shall record provenance.

Pass: Pass if the assertion records whether it was declared, inferred, discovered, imported, derived, or generated, and includes source, method, responsible authority or approved rule reference, timestamp or effective period, and version.

Fail: Fail if provenance is missing or insufficient to determine how the assertion was created.

Evidence required: Assertion provenance record, source/method record, responsible authority or approved rule reference, timestamp/effective period, version.

Rationale: Relationship accountability requires knowing how the relationship entered the evidence stream.

EO-005: Physical Relationship Representation Is Recorded Where Required

Requirement: Each material relationship shall record physical representation required to test the decision scope.

Pass: Pass if the record identifies physical joins, relationship attributes, association tables, bridge structures, source-system links, events, messages, APIs, lineage references, documents, or equivalent evidence required by the scope.

Fail: Fail if a material relationship is certified without required physical representation evidence.

Evidence required: Physical relationship evidence, source reference, join/link/path record, relationship attribute record, decision-scope mapping.

Rationale: Extended Ontology closes the gap between governed relationship meaning and real relationship evidence.

EO-006: Related Identifier Alignment and Semantic Grain Are Tested

Requirement: Each material relationship shall test whether related identifiers and concepts are aligned at compatible semantic grain for the decision scope.

Pass: Pass if identifier alignment, semantic meaning, semantic grain, and equivalence or non-equivalence rule are recorded for each material relationship endpoint.

Fail: Fail if relationship endpoints are joined, traversed, counted, or inferred as compatible without required grain and identity evidence.

Evidence required: Endpoint identity record, semantic grain record, equivalence/non-equivalence rule, decision-scope mapping.

Rationale: A relationship path can fail because its endpoints identify different business things at different grains.

EO-007: Discovery, Inference, or Declaration Method Is Recorded

Requirement: Each material relationship shall record the method by which it was declared, discovered, inferred, imported, or derived.

Pass: Pass if the record includes method name or process, method owner or authority, input evidence, rule/model/version where applicable, and repeatability condition where applicable.

Fail: Fail if a material relationship is used without method evidence sufficient to review or reproduce the assertion path.

Evidence required: Method record, input evidence, authority, rule/model/version where applicable, repeatability evidence where applicable.

Rationale: DACS permits relationship discovery. Certified use requires enough method evidence to review or reproduce the assertion path where applicable.

EO-008: Relationship Vector Is Recorded for Material Relationships

Requirement: Each material relationship shall carry a relationship vector containing Strength, Confidence, and Orientation.

Pass: Pass if Strength, Confidence, and Orientation are recorded with measurement method or approval basis for the decision scope.

Fail: Fail if any vector component is missing for a material relationship.

Evidence required: Relationship vector record, Strength evidence, Confidence evidence, Orientation evidence, decision-scope mapping.

Rationale: The vector makes relationship evaluation testable rather than assumed.

EO-009: Minimum Vector Criteria Are Defined

Requirement: Each decision scope shall define minimum vector criteria for material relationship types or paths.

Pass: Pass if Strength, Confidence, and Orientation criteria or approved qualitative rules are defined before Gate evaluation.

Fail: Fail if relationship use is certified without defined criteria or approved qualitative rules.

Evidence required: Vector criteria record, threshold or qualitative rule, authority, decision-scope mapping.

Rationale: A vector only controls use when the decision scope defines what passes.

EO-010: Relationship Vector Meets Decision-Scope Criteria

Requirement: Each material relationship used for certified decision evidence shall meet the decision-scope vector criteria or have an approved constrained-use exception.

Pass: Pass if recorded vector evidence satisfies defined criteria or constrained-use exception handling is recorded.

Fail: Fail if the relationship is used as certified evidence while vector criteria fail, are missing, or are not evaluated.

Evidence required: Vector evaluation record, threshold result, exception record where applicable, Gate result.

Rationale: Relationship use must be controlled by evidence, not plausibility.

EO-011: Permitted and Prohibited Relationship Paths Are Declared

Requirement: Each decision scope shall declare permitted and prohibited relationship paths when relationship traversal affects the decision.

Pass: Pass if permitted paths, prohibited paths, path constraints, and traversal limits are recorded.

Fail: Fail if a decision path uses relationship traversal without approved path rules.

Evidence required: Permitted/prohibited path record, traversal rule, constraint record, decision-scope mapping.

Rationale: Path control prevents unauthorized semantic traversal.

EO-012: Relationship Constraints Are Applied

Requirement: Each material relationship shall apply relevant constraints for use.

Pass: Pass if required constraints such as domain, time, authority, source, privacy, policy, regulatory, contractual, risk, or purpose constraints are recorded and applied.

Fail: Fail if a relationship is used outside required constraints or without evaluating applicable constraints.

Evidence required: Constraint record, evaluation result, Gate result, exception record where applicable.

Rationale: A relationship may be valid in one context and invalid in another.

EO-013: Relationship Readiness State Is Declared

Requirement: Each material relationship shall have a readiness state for the stated decision scope.

Pass: Pass if the relationship is assigned Proceed, Caution, Stop, or Quarantined with reason, responsible authority or approved rule reference, timestamp, and review condition where required.

Fail: Fail if a material relationship is used without a readiness state or if the state is unsupported by evidence.

Evidence required: Relationship readiness record, Gate result, reason, responsible authority or approved rule reference, timestamp, review condition.

Rationale: Relationship evidence requires a decision-scope disposition.

EO-014: Relationship Conflict Resolution Rule Exists Where Applicable

Requirement: Where relationship evidence conflicts, the decision scope shall define a conflict resolution rule or assign Stop/Quarantined until resolved.

Pass: Pass if the conflict is resolved by an approved rule, constrained-use exception, or assigned Stop/Quarantined state.

Fail: Fail if conflicting relationships are used as certified evidence without resolution or disposition.

Evidence required: Conflict record, resolution rule, authority, Gate result, readiness state.

Rationale: Conflicting relationship evidence cannot support Defensible Analytics without disposition.

EO-015: Ontology Change Triggers Reassessment

Requirement: Material ontology changes shall trigger reassessment of affected decision scopes.

Pass: Pass if changes to relationship type, orientation, path, vector criteria, constraints, provenance, or permitted/prohibited path rules trigger impact analysis and Gate reassessment.

Fail: Fail if certified decision paths continue after a material ontology change without review.

Evidence required: Ontology change log, impact analysis, Gate reassessment record, certification update.

Rationale: Relationship rules can invalidate previously certified decision paths.

EO-016: Traversal Path Is Determinate Where Used

Requirement: A relationship traversal path used as certified decision evidence shall be determinate for the same input, rule set, version, and decision scope.

Pass: Pass if the traversal returns the same path result or same unresolved/exception result under the same inputs, rules, versions, and scope.

Fail: Fail if traversal produces inconsistent path results without recorded version, rule, threshold, or exception explanation.

Evidence required: Traversal rule, version, path record, test result, exception record where applicable.

Rationale: Decision-path reconstruction requires repeatable relationship traversal.

EO-017: Cross-Domain Semantic Compatibility Is Declared Where Applicable

Requirement: When a relationship crosses domains, functions, systems, or stewardship authorities, semantic compatibility shall be declared before certified use.

Pass: Pass if cross-domain relationships reference semantic domains, boundary rules, compatible grain, disjointness or overlap rules where material, and authority or stewardship process.

Fail: Fail if cross-domain relationships are certified without compatibility evidence.

Evidence required: Semantic domain references, boundary rules, compatibility record, grain rule, authority/stewardship record, decision-scope mapping.

Rationale: Cross-domain use requires more than local application meaning.

8. Profile 4: AI Context Contract Controls

Purpose: Determine whether AI-assisted decision scopes can be tested against governed meaning, approved identity, permitted relationships, valid context, Gate criteria, drift rules, and decision-scope evidence requirements. This profile does not certify model quality in general. It requires material AI behavior and AI-assisted evidence to be tested against the Binding AI Context Contract for the stated decision scope.

AI-001: Binding AI Context Contract Exists

Requirement: Each AI-assisted decision scope shall have a Binding AI Context Contract before AI outputs are certified for material use.

Pass: Pass if the contract references applicable Extended Taxonomy, Extended Ontology, Business Identity rules, preserved context, permitted paths, prohibited paths, relationship vector criteria, Gate criteria, drift rules, and evidence requirements.

Fail: Fail if AI output is certified without a contract or if the contract lacks required semantic, identity, relationship, context, Gate, or drift constraints.

Evidence required: Binding AI Context Contract record, taxonomy reference, ontology reference, identity rule, context rule, permitted/prohibited path list, vector criteria, Gate criteria, drift rules.

Rationale: AI cannot be governed against vague intent. It requires a concrete context contract.

AI-002: AI Inputs Conform to the Semantic Contract

Requirement: Each material input feature, retrieved field, prompt-supplied variable, tool-returned value, document excerpt, or context element used by an AI-assisted decision scope shall map to the applicable Semantic Contract.

Pass: Pass if each material AI input maps to approved taxonomy, Business Identity where applicable, physical attribution where required, context rule, and Gate status for the decision scope.

Fail: Fail if the AI-assisted decision uses unmapped, ambiguous, prohibited, unreviewed, or uncertified input evidence for a material input or context element.

Evidence required: AI input record, retrieval/prompt/tool context record, taxonomy reference, identity reference where applicable, physical attribution where required, Gate result, decision-scope mapping.

Rationale: Material information supplied to AI must be governed and traceable to the applicable Semantic Contract for the stated decision scope.

AI-003: AI Output Terms Conform to Extended Taxonomy or Are Quarantined

Requirement: Each material term, classification, or concept used in an AI-assisted output shall map to an approved Extended Taxonomy node or be assigned Quarantined before material use.

Pass: Pass if all material AI output terms map to approved taxonomy nodes for the decision scope or are routed as Quarantined evidence for review.

Fail: Fail if the output uses material terms, classifications, or concepts that are unmapped, ambiguous, prohibited, or unreviewed as if certified.

Evidence required: AI output record, term extraction or mapping record, taxonomy references, Quarantined/review record where applicable.

Rationale: AI outputs must use governed business language when they support Defensible Analytics.

AI-004: AI Output Relationships Conform to Extended Ontology or Are Quarantined

Requirement: Each material relationship asserted or used by an AI-assisted output shall map to approved Extended Ontology evidence or be assigned Quarantined before material use.

Pass: Pass if all material AI output relationships map to approved relationship types, permitted orientations, vector criteria, and path rules for the decision scope, or are routed as Quarantined evidence.

Fail: Fail if the AI output asserts or depends on an unmapped, prohibited, unsupported, or unreviewed relationship as if certified.

Evidence required: AI output record, relationship extraction or mapping record, ontology reference, vector record, orientation record, path rule, Quarantined/review record where applicable.

Rationale: AI relationship assertions must be tested, not accepted because they are plausible.

AI-005: AI Inference and Output Drift Are Tested

Requirement: Each AI-assisted decision scope shall test material AI outputs, inferred relationships, generated classifications, or context use for drift against the Binding AI Context Contract.

Pass: Pass if required drift-test records compare AI terms, classifications, relationships, orientations, context use, or actions against the contract and record test ID, contract version, tested output/action, result, timestamp, and responsible authority or approved drift-test rule.

Fail: Fail if AI output is certified without required drift testing where AI may generate or infer material terms, classifications, relationships, context, or actions.

Evidence required: Drift test record, AI output sample or production record, contract reference, taxonomy/ontology reference, drift result, readiness state.

Rationale: AI behavior can deviate from governed meaning and relationship rules. Drift must be testable against the contract.

AI-006: AI Context Contract Violation Has Consequence

Requirement: Each material violation of the Binding AI Context Contract shall result in Stop, Caution, Quarantined, remediation, approved exception handling, or contract review.

Pass: Pass if each violation produces a recorded Gate result, exception record, remediation record, review action, or readiness-state update.

Fail: Fail if AI output violates the contract and is still treated as certified without recorded consequence.

Evidence required: Violation record, Gate result, exception record, remediation record, review record, resulting readiness state.

Rationale: A binding contract is not binding unless violations have consequence.

AI-007: Context Enforcement Point or Equivalent Control Is Declared

Requirement: Each AI-assisted decision scope shall identify the point, process, or mechanism that enforces context eligibility before certified use.

Pass: Pass if a Context Enforcement Point or equivalent control is recorded and linked to the Semantic Contract, Gate criteria, permitted context, prohibited context, and decision scope.

Fail: Fail if AI context is used for certified output without an identified enforcement point or equivalent control.

Evidence required: Context Enforcement Point/control record, Gate rule, Semantic Contract reference, permitted/prohibited context record, decision-scope mapping.

Rationale: Context delivery is not context validity. A control point is required for the contract to operate.

AI-008: Decision Execution Trace Is Recorded Where AI or Automation Is Material

Requirement: Each material AI-assisted or automated decision path shall record a Decision Execution Trace.

Pass: Pass if the trace includes request, actor or agent, input context, material concepts, relationship paths where applicable, Gate results, tools or APIs where applicable, model/process/version where applicable, output or action, timestamp, and certification or exception state.

Fail: Fail if AI or automation materially affects a decision and no reconstructable execution trace exists.

Evidence required: Decision Execution Trace, execution log reference, Gate record, context record, output/action record, certification or exception record.

Rationale: Technical execution logs may supply useful evidence, but defensibility requires the decision-scope evidence defined by applicable DACS controls.

AI-009: Agentic Action Authority Is Declared Where AI Acts

Requirement: When AI or automation initiates or recommends a material action, the decision scope shall declare the authority under which that action is permitted.

Pass: Pass if agent identity, delegated authority, allowed action class, allowed tools or APIs, escalation rule, and Gate-before-action requirement are recorded where applicable.

Fail: Fail if an agent or automation can perform or recommend a material action without recorded authority and Gate criteria.

Evidence required: Agent identity, authority record, allowed action record, tool/API permission record, escalation rule, Gate result.

Rationale: An agent that acts requires scoped authority and accountability.

AI-010: Material Agentic Action Requires Gate-Before-Action

Requirement: A material agentic action shall not execute as certified unless applicable DACS Gates have passed or an approved constrained-use exception exists.

Pass: Pass if the action has a recorded Gate decision before execution or a documented exception allowing constrained execution.

Fail: Fail if a material action executes as certified without pre-action Gate evidence or approved exception.

Evidence required: Pre-action Gate record, action request, authority record, exception record where applicable, action result.

Rationale: For AI that acts, logging after the fact is not enough when material risk exists.

AI-011: AI-Generated Evidence Is Not Treated as Certified Without Gate Evidence

Requirement: AI-generated classifications, relationships, summaries, recommendations, code, mappings, or actions shall not be treated as certified evidence unless applicable DACS controls pass.

Pass: Pass if AI-generated evidence is either certified through applicable Gates or assigned Caution, Stop, or Quarantined with reason and next action.

Fail: Fail if AI-generated evidence is relied on for material decision use without Gate evidence or approved constrained-use exception.

Evidence required: AI-generated evidence record, Gate result, readiness state, exception/remediation record where applicable.

Rationale: AI can accelerate discovery and drafting, but it does not replace DACS evidence requirements.

9. Evidence Model

Evidence used to evaluate DACS controls shall be sufficient to test applicable controls as Pass or Fail. DACS does not prescribe where that evidence must be stored. Evidence may be implemented in catalogs, metadata repositories, relational systems, graph systems, governance platforms, workflow systems, semantic platforms, spreadsheets during early adoption, operational stores, warehouses, marts, lakes, lakehouses, observability tools, or other technologies.

A certification record shall include, at minimum:

- decision-scope identifier and version;
- applicable profile list;
- control IDs and control results;
- required evidence references;
- Gate ID and Gate result;
- readiness state;
- responsible authority, steward, or approved rule reference;
- timestamp or effective period;
- exception or constraint record where applicable;
- review condition or review date; and
- reconstruction reference for the decision path.

9.1 Example Readiness Signals (Informative)

Readiness signal	Observable evidence
Relationship readiness	Approved relationship type, permitted orientation, assertion provenance, vector criteria result, constraint disposition, conflict resolution where needed, and Gate state.
AI context readiness	Binding AI Context Contract test result for each material input, output, generated term, inferred relationship, drift test, action, or contract violation.
Gate readiness	Recorded state of Proceed, Caution, Stop, or Quarantined for each applicable control group or material path.
Evidence readiness	Certification record includes control ID, result, evidence reference, authority or rule, timestamp, and readiness state.
Quarantine visibility	Each discovered, inferred, generated, imported, retrieved, or available item not approved for certified use has Quarantined state, reason, owner or review authority, and next Gate/remediation action.

10. Exceptions and Constraints

DACS permits constrained-use exceptions, but exceptions must be explicit and evidenced. An exception does not make a failed control pass. It allows bounded use under recorded authority and conditions.

Each exception record shall include:

- control ID or Gate condition affected;
- reason for exception;
- decision scope and usage boundary;
- risk or constraint statement;
- approving authority or approved exception rule reference;
- readiness state;
- expiration or review condition;
- remediation owner and next action where applicable.

Constrained use shall be recorded as Caution unless the applicable Gate defines another readiness state. Evidence that has not passed required controls and lacks approved constrained use shall remain Quarantined or Stop depending on the condition.

11. Recommended Practices (Informative)

This section is informative. These practices do not determine conformance unless referenced by a mandatory control.

- **Start narrow.** Begin with one decision scope, one decision path, one Gate, and one evidence packet. Preserve the first-Gate entry point. Do not require a full enterprise program, platform migration, or complete companion-specification implementation before a first bounded DACS evaluation.
- **Classify every in-scope item.** Assign Proceed, Caution, Stop, or Quarantined to each material identity, concept, relationship, context item, and AI evidence item.
- **Do not automate ambiguity.** Manual evidence records are acceptable for early adoption if they are structured enough to test and reconstruct the decision path.
- Separate discovery from certified use. Use Quarantined to preserve discoveries without converting them into certified evidence.
- **Measure recurring failure patterns.** Track repeated Stop, Caution, and Quarantined outcomes to improve taxonomy, ontology, identity rules, source quality, and Gate design.
- **Keep external frameworks informative.** External standards, frameworks, and tools may supply evidence, but they do not automatically satisfy DACS controls unless the required DACS evidence exists.

12. Positioning Against Existing Methods and Tools

DACS does not criticize or replace existing platforms, methods, or governance disciplines. Many are essential to the modern enterprise environment. DACS clarifies their boundary for material decision use.

Tools can move, expose, document, model, observe, automate, and infer from information. DACS defines what must be true before that information is treated as decision-scope evidence for Defensible Analytics.

DACS does not assert that a data catalog, semantic layer, ontology tool, AI platform, lineage system, data fabric, data mesh, lakehouse, warehouse, or governance platform cannot provide useful evidence. It asserts only that DACS conformance requires the evidence specified by applicable DACS controls.

Existing AI guardrail systems, policy engines, semantic layers, catalogs, data-contract systems, lineage systems, model-monitoring systems, observability platforms, and governance tools may implement controls or supply evidence. ***DACS does not rename those capabilities as DACS. Evidence from those mechanisms may support a DACS control only when it contains the required evidence and is evaluated against the applicable decision-scope criteria***.

13. Annex A: MVP Control Checklist (Informative)

The following checklist is a practical entry point for a first DACS evaluation. It is informative and does not replace the control requirements above.

Core

- CORE-001 - Decision Scope Is Declared
- CORE-002 - Semantic Contract Exists
- CORE-003 - Applicable Profiles Are Declared
- CORE-004 - Business Identity Anchors Exist Where Required
- CORE-005 - Semantic Grain Is Declared for Identity-Bearing Evidence
- CORE-006 - Physical Attribution Is Recorded Where Required
- CORE-007 - Logical-to-Conceptual Binding Exists Where Required
- CORE-008 - Context Is Preserved
- CORE-009 - Gate Decision Is Recorded
- CORE-010 - Decision Path Is Reconstructable
- CORE-011 - Certification Record Exists
- CORE-012 - Certification Record Is Structured
- CORE-013 - Material Semantic Binding Change Triggers Review
- CORE-014 - Identity Resolution Produces Determinate Results
- CORE-015 - Business Concept Is Not Assumed to Be Business Identity
- CORE-016 - Discovered Evidence Is Quarantined Until Governed

Extended Taxonomy

- ET-001 - Taxonomy Scope and Purpose Are Declared
- ET-002 - Taxonomy Node Type Is Declared
- ET-003 - Business Meaning Is Recorded
- ET-004 - Controlled Label and Language Evidence Are Recorded
- ET-005 - Semantic Domain and Boundary Are Declared
- ET-006 - Semantic Grain Is Declared Where Material
- ET-007 - Physical Semantic Anchors Are Recorded Where Required
- ET-008 - Business Identifier or Key Evidence Is Recorded Where Applicable
- ET-009 - Source-System Representation Is Recorded Where Required
- ET-010 - Resolution or Mastering Rule Is Recorded Where Applicable
- ET-011 - Ownership and Stewardship Are Recorded
- ET-012 - Governance Constraints and Usage Boundaries Are Recorded
- ET-013 - Provenance Is Recorded
- ET-014 - Readiness State Is Declared
- ET-015 - Semantic Risk Is Recorded Where Present
- ET-016 - Relationship Seeds Are Not Treated as Certified Relationships
- ET-017 - Taxonomy Change Triggers Reassessment

Extended Ontology

- EO-001 - Relationship Candidate Is Not Treated as Certified
- EO-002 - Relationship Type Is Governed
- EO-003 - Relationship Orientation Is Declared
- EO-004 - Relationship Assertion Provenance Is Recorded
- EO-005 - Physical Relationship Representation Is Recorded Where Required
- EO-006 - Related Identifier Alignment and Semantic Grain Are Tested
- EO-007 - Discovery, Inference, or Declaration Method Is Recorded

- EO-008 - Relationship Vector Is Recorded for Material Relationships
- EO-009 - Minimum Vector Criteria Are Defined
- EO-010 - Relationship Vector Meets Decision-Scope Criteria
- EO-011 - Permitted and Prohibited Relationship Paths Are Declared
- EO-012 - Relationship Constraints Are Applied
- EO-013 - Relationship Readiness State Is Declared
- EO-014 - Relationship Conflict Resolution Rule Exists Where Applicable
- EO-015 - Ontology Change Triggers Reassessment
- EO-016 - Traversal Path Is Determinate Where Used
- EO-017 - Cross-Domain Semantic Compatibility Is Declared Where Applicable

AI Context Contract

- AI-001 - Binding AI Context Contract Exists
- AI-002 - AI Inputs Conform to the Semantic Contract
- AI-003 - AI Output Terms Conform to Extended Taxonomy or Are Quarantined
- AI-004 - AI Output Relationships Conform to Extended Ontology or Are Quarantined
- AI-005 - AI Inference and Output Drift Are Tested
- AI-006 - AI Context Contract Violation Has Consequence
- AI-007 - Context Enforcement Point or Equivalent Control Is Declared
- AI-008 - Decision Execution Trace Is Recorded Where AI or Automation Is Material
- AI-009 - Agentic Action Authority Is Declared Where AI Acts
- AI-010 - Material Agentic Action Requires Gate-Before-Action
- AI-011 - AI-Generated Evidence Is Not Treated as Certified Without Gate Evidence

14. Annex B: Example Decision Scope (Informative)

Example: Weekly Executive Dashboard - Active Customer Count.

- **Decision scope:** North America subscription-customer Active Customer Count for weekly internal executive dashboard use.
- **Decision use:** Internal executive review of customer growth, retention exposure, and operating priorities.
- **Grain:** One customer account as of reporting week end.
- **In scope:** Internal weekly trend discussion and operating review.
- **Out of scope:** External reporting, compensation, regulatory reporting, customer commitments.
- **Example Gate question:** Can Active Customer Count be used in the weekly executive dashboard for the stated internal-use scope?
- **Example readiness state:** Caution, because two source status codes remain Quarantined pending owner decision.

This example illustrates constrained decision-scope use. It does not certify the metric for external reporting or other uses.

15. Annex C: DACS Adoption Maturity Levels (Informative)

These maturity levels are informative. They are included to separate progressive adoption from binary control conformance. They are not a certification scheme, appraisal method, or legal compliance status.

Level	Name	Meaning
0	Unassessed	DACS language may be used, but no formal decision scope, Gate record, or evidence packet exists.
1	Scoped	One bounded decision scope has a decision-scope statement, evidence packet, Gate result, and readiness state.
2	Repeatable	DACS Gates are applied consistently across selected decision scopes using reusable evidence patterns.
3	Defined	Roles, evidence requirements, profiles, exceptions, Gate criteria, and review patterns are documented and governed.
4	Measured	Gate outcomes, exceptions, remediation, drift, Quarantined evidence, and reuse are measured over time.
5	Optimizing	DACS controls are continuously improved and may be embedded in workflows, platforms, automation, and AI-enabled decision paths.

A decision scope at any adoption maturity level must still pass applicable controls to claim DACS conformance for that scope.

16. Annex D: Drafting Tests for Future DACS Controls

A proposed DACS control shall satisfy all of the following tests before inclusion in the normative body:

- The control has a clear decision-scope applicability condition.
- The requirement uses mandatory language and can be tested as Pass or Fail.
- The Pass condition is observable and evidence-based.
- The Fail condition is explicit.
- Required evidence is listed.
- Subjective language is replaced with thresholds, criteria, rule references, authority, or Gate results.
- The control does not require a specific vendor, platform, tool, data model, or implementation pattern unless that implementation is itself the declared scope.
- The control separates discovery, review, Quarantined evidence, constrained use, and certified use.

The control addresses a DACS decision-scope control gap directly or states how adjacent standards, frameworks, tools, or records may supply evidence without becoming automatic substitutes for DACS conformance.

17. Annex E: External Reference Boundary and Evidence Alignment Rules

External standards, frameworks, methods, and tools may be referenced in future DACS guidance. Unless explicitly incorporated into a normative DACS control, such references are informative by default.

- **No hidden conformance.** A claim of alignment with another standard does not automatically satisfy a DACS control.
- No automatic substitution. A tool-generated artifact satisfies a DACS control only when it contains the evidence required by that control.
- **Implementation neutrality.** DACS does not require a specific tool, platform, schema, graph, model, workflow engine, or repository.
- **Evidence boundary.** External frameworks may provide evidence inputs; DACS defines the criteria and result vocabulary used to evaluate those inputs for the stated decision scope.

Guardrail boundary. AI guardrail systems, policy engines, retrieval filters, model monitors, security controls, runtime validation mechanisms, and similar implementation mechanisms may support DACS-relevant checks or produce DACS evidence. They do not satisfy a DACS control by label or existence. They satisfy a DACS control only when they record the required evidence, scope binding, Gate result, readiness state, and exception or violation consequence required by the applicable control.

DACS is designed to operate alongside adjacent standards, frameworks, and tools. Adjacent references may supply evidence for data quality, metadata, controlled vocabulary, provenance, graph constraints, lineage, AI risk, AI management systems, audit controls, security/privacy controls, process maturity, or governance operating models. DACS defines the criteria used to evaluate that evidence against the applicable decision-scope controls. The assessor or governed control process applies those criteria and records the control result.

DACS focuses on decision-readiness boundaries that can remain between adjacent disciplines when their artifacts are used for material decision paths:

- business meaning is not physically anchored to source systems, attributes, identifiers, semantic grain, and resolution rules;
- relationship meaning is not physically anchored to relationship evidence, orientation, vectors, permitted paths, and constraints;
- discovered, inferred, generated, imported, or retrieved evidence is treated as ready for certified use before Gate controls pass;
- AI outputs are evaluated without a governed context contract, permitted relationship paths, drift rules, or enforceable consequences;
- technical lineage exists but the decision path cannot be reconstructed from identity, meaning, relationship, context, Gate, and evidence records;
- governance documentation exists but cannot be observed, tested, evidenced, or translated into a Gate readiness state;
- adoption maturity is confused with binary control conformance for a stated decision scope.

These evidence-alignment rules are informative. Future DACS reference-alignment guidance may map DACS controls to external standards and frameworks, but no external artifact satisfies a DACS control unless the required DACS evidence exists.

18. Annex F: Planned Companion Documents and Future Profiles (Informative)

The following documents are planned or candidate companion materials. They support adoption, assessment, remediation, training, implementation, reference alignment, claims governance, and ecosystem development. They do not create normative requirements unless incorporated by a future DACS release.

F.1 Companion Specifications

DACS Extended Taxonomy Specification: expands requirements for physical semantic anchoring, business identifiers, semantic grain, source-system representation, authority, provenance, readiness, risk, and usage boundaries.

DACS Extended Ontology Specification: expands requirements for governed relationship meaning, physical relationship anchoring, relationship vectors, orientation, permitted and prohibited paths, relationship discovery, assertion provenance, constraints, and decision-scope readiness.

DACS Evidence Object and Gate Certificate Specification: defines structured evidence objects, Gate records, certification records, readiness-state payloads, review conditions, export expectations, and exchange patterns.

DACS AI Context Contract and Context Enforcement Specification: defines Binding AI Context Contract structure, context enforcement patterns, permitted and prohibited paths, AI input/output evidence, drift testing, violations, and consequences.

F.2 Assessment, Remediation, and Adoption Materials

DACS Pass/Fail and Remediation Catalog: provides control-by-control test procedures, pass/fail interpretation, acceptable evidence patterns, common failure modes, remediation paths, repeatable-fix patterns, examples, non-examples, and readiness-state guidance without replacing the normative controls.

DACS Assessment Guide and Example Workbook: provides worked examples, sample evidence packets, assessor prompts, sampling patterns, Gate examples, Quarantined, Caution, and Stop examples, and hands-on verification exercises.

DACS First Gate Pilot Kit: provides a low-friction entry package for one decision scope, one Gate, one evidence packet, one filled example, and one readiness decision. It supports early field validation without replacing the normative controls.

DACS Practitioner Playbook and Adoption Guide: provides implementation patterns, first-Gate exercises, stakeholder roles, workshop guidance, operating cadence, remediation loops, evidence review patterns, and practical adoption sequences.

DACS Adoption and Conformance Guide: defines progressive adoption maturity levels, assessment patterns, evidence expectations, and organizational progression from one scoped decision path toward repeatable, measured, and optimized control execution. This guide does not replace binary control conformance in this specification.

F.3 Ecosystem, Claims, and Reference Alignment Materials

DACS Public Claims and Terminology Use Guide: defines approved and prohibited uses of DACS terms, including DACS conformance, DACS alignment, certified-use claims, vendor adherence, tool-support claims, partner claims, training authorization, and certification claims.

DACS External Reference Alignment Guide: maps DACS controls to adjacent standards, frameworks, and implementation artifacts and clarifies when external artifacts may serve as evidence inputs for DACS controls.

DACS Vendor Adherence Specification: defines how tools, platforms, vendors, and service providers may evidence support for DACS controls without claiming broad product certification unless such a program is separately published.

DACS Authorized Training and Partner Enablement Guide: provides partner-onboarding expectations, authorized delivery patterns, instructor enablement, feedback collection, co-marketing boundaries, and field-validation reporting guidance. It does not create control conformance, vendor certification, or product certification by itself.

F.4 Future Profiles

DACS Agentic Operation Profile: defines additional controls for AI agents or automated workflows that recommend, initiate, route, approve, or execute material actions.

19. Annex G: Public Comment Template

Field	Submitter entry
Submitter name	
Organization	
Section or control ID	
Comment type: defect / clarity / scope / testability / evidence / implementation / legal / other	
Comment	
Proposed change	
Reasoning	
Severity: blocking / material / minor / editorial	

Closing Normative Boundary

DACS defines the controls and evidence obligations used to determine whether evidence and decision paths are ready for certified use within a stated decision scope. Accountable authorities own the obligation. Governed human, procedural, or automated mechanisms execute the applicable controls and record the results. Gate and Certification Records preserve the resulting determination. DACS does not guarantee that every result is correct, lawful, optimal, or risk-free.

Discovery is not certification. Connectivity is not accountability. If identity is unstable, meaning is ambiguous, relationships have not passed accountability controls, or AI outputs cannot be tested against a governed context contract, the decision path is not defensible under DACS.