DACS Pass/Fail and Remediation Catalog

Operational guidance for testing, remediating, and retesting DACS controls

v1.1 Release Candidate

Aligned to DACS Specification v1.14 Release Candidate

Available at: https://dacs.datavaultalliance.com/documents/dacs-pass-fail-and-remediation-catalog/

Purpose

This catalog helps practitioners inspect DACS evidence, assess each control, diagnose failed conditions, plan corrective work, apply the recorded Gate disposition, and retest for closure.

Normative boundary

DACS Specification v1.13 defines the mandatory controls and governing assessment rules. This catalog is informative companion guidance aligned to that version. It adds no requirement and grants no authorization. The exact Specification version used by an assessment governs; a later version does not rewrite historical results.

Published by DataVaultAlliance Holdings LLC

DataVaultAlliance maintains the authoritative DACS Specification and official DACS publications. Redistributed copies may become outdated. Verify the current authoritative version at dacs.datavaultalliance.com before relying on this publication.

Table of Contents

1. Purpose and operating boundary....3
2. How to use this catalog....4
3. Testable, implementable, and executable controls....5
4. Remediation doctrine....6
5. Controlled disposition guidance....6
6. Reusable remediation patterns....8
7. Core Decision-Scope Controls....9
8. Extended Taxonomy Controls....61
9. Extended Ontology Controls....96
10. AI Context Contract Controls....131
11. Remediation record template....157
12. Closing guidance....159

1. Purpose and operating boundary

The DACS Pass/Fail and Remediation Catalog is an operational companion to the Defensible Analytics Control Specification. It answers a narrow practitioner question: when a control is evaluated, what evidence should be inspected, what constitutes Pass or Fail, and what must happen next when the control does not pass?

DACS defines the controls and evidence requirements used to determine whether evidence is ready for stated use within a stated decision scope. It does not establish universal truth, prove that a decision is correct, or replace the governance, data-management, risk, audit, security, privacy, or AI-management disciplines that may supply evidence to the control process.

This catalog preserves the DACS distinction between control result and Gate readiness state. A control result is Pass, Fail, or Not Applicable. A Gate readiness state is Proceed, Caution, Stop, or Quarantined. An exception may permit constrained use, but an exception does not convert a failed control into a passed control.

Primary operating question

What does the reader need to do next, and what evidence must exist when they are done?

Document responsibility and depth boundary

This catalog covers the control-assessment boundary. It tells a practitioner how to inspect evidence, execute the assessment, determine Pass, Fail, or Not Applicable, remediate a failed condition, apply a controlled disposition while unresolved, and retest for closure. It does not prescribe organizational rollout, team design, workshop methods, operating cadence, or broader implementation architecture. Those belong in the DACS Practitioner Playbook and Adoption Guide. Worked evidence packages, sampling exercises, and assessor practice belong in the DACS Assessment Guide and Example Workbook. First-adoption sequencing belongs in the DACS First Look Pilot Kit.

© 2026 DataVaultAlliance Holdings LLC. All rights reserved.

2. How to use this catalog

Establish the decision scope, bind the governing rules, and determine applicable profiles. Then assess controls in the dependency order defined by the Specification. Each card reproduces the immediate Prerequisites entry from Specification v1.13. The DACS Control Dependency Map v0.3 shows immediate and inherited dependencies and their required statuses; the Specification governs.

Pass required means the listed control has an evidence-backed Pass for the same applicable scope, relevant evidence, and effective versions. Recorded result required means its evidence-backed Pass, Fail, or Not Applicable with reason and supporting records are available. A recorded Fail can support a handling or recording test; it does not grant permission for use or satisfy a separate Pass requirement.

The lists retain the nearest necessary prerequisites. They omit earlier controls only where a retained path guarantees the required status and evidence. Independent branches remain listed. A control number does not establish dependency coverage. Resolve conditional dependencies through the recorded Applicability Rule; Not Applicable is not Pass and does not automatically remove another requirement.

Evaluate a control when its required evidence exists or its declared completion deadline expires. Required execution or persistence follow-up evaluations remain separate from controls already assessed before action. An incomplete evaluation is not Pass, Not Applicable, or a fourth control result. Do not claim full decision-scope conformance before every mandatory evaluation is complete. Section 9.1 governs Buffered Gate Capture; complete authorization and capture precede action even when durable persistence is delayed.

#	Action	Evidence outcome
1	**Determine applicability**	Use the recorded Applicability Rule and scope facts. Record Not Applicable only when the rule evaluates false, with reason and supporting evidence. Unresolved applicability is Fail.
2	**Inspect evidence**	Retrieve required evidence for the scope and effective versions being assessed. Inspect attribution, authority, integrity, and timing where required.
3	**Evaluate**	Compare the evidence to the Requirement, Pass condition, Fail condition, authority, rule, threshold, version, or other control criterion.
4	**Record result**	Record Pass, Fail, or Not Applicable. Do not use a readiness state as a substitute for the control result.
5	**Classify the failure**	Identify whether the problem is missing evidence, ambiguity, missing authority, conflict, threshold failure, drift/change, unsupported discovery, prohibition, or missing execution record.
6	**Remediate or disposition**	Correct the failed condition through governed evidence or a repeatable mechanism. Apply the actual Gate disposition under recorded authority while correction remains incomplete.

7	**Retest**	Assess the corrected condition under its recorded effective versions. Preserve original evidence and results; create a new linked retest event.
8	**Update Gate and conformance evidence**	Create linked new Gate and Conformance Records where reassessment is required. Preserve historical determinations and verify any new permission for use.

Universal card rules. The applicability, evidence-recording, result-recording, remediation, disposition, execution, and closure rules in Sections 2 through 5 apply to every control card. The cards intentionally repeat only control-specific instructions.

Evidence sufficiency baseline. Retrieve the required evidence for the stated scope and the version or effective state being assessed. Check its authority and integrity where required. An artifact's existence does not establish that its control criteria are met. The Specification requirement, Prerequisites, Evidence to inspect, and Pass/Fail text are reproduced from v1.13. Other card fields are informative guidance; they do not add requirements or replace the global rules. Examples illustrate a point and are not complete evidence packages.

3. Testable, implementable, and executable controls

At a completed assessment, record Pass only when every applicable mandatory criterion and required evidence element is satisfied, including the listed prerequisite statuses. Otherwise record Fail. Record Not Applicable only when a recorded Applicability Rule evaluates false, with its reason, rule reference, and supporting facts. Unresolved applicability is Fail, not Not Applicable. Evidence collection, evaluation, Gate authorization, and record completion are separate activities under Specification Section 3.2.6; no later completion reference creates an earlier circular prerequisite.

Testable	The required evidence can be inspected and compared against the Requirement, Pass condition, Fail condition, decision scope, authority, rule, threshold, version, or Gate readiness state.
Implementable	A real team can satisfy the control through a manual procedure, workflow, governed record, rule engine, metadata repository, catalog, semantic layer, data-quality process, identity process, stewardship process, API, automation, or hybrid mechanism.
Executable	The control has a repeatable evaluation path, recorded evidence, an accountable authority, an approved rule reference where applicable, and the required control result and Gate readiness state where applicable. Executable does not require software code.

Do not use executable to imply that AI output is inherently deterministic, that a prompt is sufficient as a control, or that a model can establish its own DACS conformance.

Preferred operating statement

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

Authority and execution in the control cards. Every card identifies the accountable authority for the control. Execution guidance appears only when timing, repeatability, enforcement, sequencing, or evidence capture is material to the control. If no Execution entry appears, the universal execution rule above applies. Generic tool lists are intentionally not repeated in every card.

4. Remediation doctrine

Remediation corrects a failed condition through verifiable evidence, an approved rule, a governed mapping, valid authority, or another repeatable mechanism. Containment and exception handling can govern the use while correction is incomplete. They do not by themselves close the failed control.

Quarantined may hold candidate evidence during review. **Stop** prevents prohibited or unauthorized use. Where a failed control's evidence is permitted for bounded use, **Caution** requires a valid authorizing exception with the required scope, constraints, authority, and expiration or review condition. The failed result stays **Fail**.

Human review is not automatically non-repeatable. When a human adjudication is material, the adjudication should become governed evidence: for example, a versioned mapping, approved tie-break rule, exception record, classification decision, or authoritative disposition that can be applied or inspected again.

Close a failed finding only after the control is retested and the new evidence-backed result is recorded. If a new recorded Applicability Rule establishes Not Applicable, preserve its reason and supporting facts; do not narrow scope merely to conceal a failed mandatory obligation. Create new linked evaluations and Gate or Conformance Records where required. Preserve the original result, evidence, rule versions, and Gate state under the applicable integrity and lawful-retention rules.

Recover historical evidence only from verifiable contemporaneous records. A later approval, changed threshold, current artifact, or new execution does not prove what was authorized or used earlier. A changed rule or scope takes effect prospectively and belongs to a new assessment. These history and closure rules apply to every card.

Failure-to-remediation linkage. Common failure modes are diagnostic clues, not new control results. When a control can fail for different reasons, match each observed failure condition to the corresponding remediation action in the card. If more than one failure condition is present, remediate each affected condition before retest.

Retest scope after remediation. Retest the failed control and any other applicable controls affected by the change. Re-run the full Gate when the remediation changes evidence, meaning, identity, relationships, context, authority, constraints, or another condition that may affect the Gate outcome. A local correction does not require unrelated controls to be rerun.

5. Controlled disposition guidance

Use the applicable Gate logic under its recorded authority to determine readiness. The states below follow Specification v1.13 Section 3.4. The disposition patterns support diagnosis; they do not independently grant permission for use.

Proceed	All controls applicable to the Gate are Pass; controls that do not apply are recorded Not Applicable with reason. No failed control is being overridden for use. Use is permitted only within the recorded scope and while the readiness validity condition remains true.
Caution	One or more conditions require explicit constraint, monitoring, remediation, or an approved constrained-use exception. Any failed control remains Fail. Use is permitted only within the recorded constraint, authority, and readiness validity condition. Caution never converts Fail into Pass.
Stop	A completed evaluation identifies a failed control, prohibition, missing authority, invalid context, contract violation, or other rule that prohibits stated use. Use is not permitted for the stated material decision scope.
Quarantined	Candidate evidence has not completed the required evaluation or is held pending review or remediation and is not ready for stated use. Evidence may be explored, reviewed, remediated, or routed through additional Gates but shall not be relied on for material decisions.

Critical distinction

A control testing containment, testing, recording, or enforcement may Pass while another control remains Fail. Stop or Quarantined is not an automatic Fail for that handling control. A repeatable unresolved outcome is not permission for use. Full decision-scope conformance requires all applicable mandatory controls to Pass or be Not Applicable with reason; a permitted Caution exception does not establish it.

5.1 Reusable disposition patterns.

Each card uses a Disposition reference label to point to one of the D-01 through D-06 patterns below. The sentence that follows the reference explains why that pattern applies to that specific control. The reference does not change the control result and does not replace the Gate logic in the DACS Specification.

D-01 Missing prerequisite	Apply the status stated in the control's Prerequisites entry. A missing required Pass prevents dependent Pass; a Recorded result requirement may be met by an evidence-backed Fail or Not Applicable with reason. Block material use unless the applicable Gate explicitly permits it under valid authority. Diagnosis and

	containment may continue.
D-02 Unresolved governed evidence	Keep unresolved evidence out of material reliance. Use the applicable Gate to establish Quarantined for held candidates or Stop where a completed finding prohibits use. Caution requires valid authority for the exact bounded use; it does not close the failed finding.
D-03 Ungoverned candidate evidence	Hold candidate evidence as Quarantined until Gate evidence permits its stated use. Any authorized constrained use follows Caution and its valid exception bounds. Correct containment may satisfy a handling control without promoting the candidate or changing other failed results.
D-04 Change or reassessment	Reassess affected active or prospective reliance when a material change or validity trigger requires it. Invalidate or suspend prior permission for new reliance as defined. Preserve historical determinations and create linked replacement evaluations.
D-05 Threshold, constraint, or conflict	Apply the Gate to the recorded failed threshold, ignored constraint, or unresolved conflict. Caution permits only a valid bounded exception granted by competent authority. An exception cannot invent legal or policy authority or convert the underlying failed result to Pass.
D-06 Determinacy or repeatability	Test unchanged inputs, rules, thresholds where used, versions, and scope. Different outcomes under unchanged conditions Fail. The same governed unresolved or exception outcome may satisfy repeatability while material reliance remains withheld under the applicable Gate.

6. Reusable remediation patterns

Pattern references identify reusable classes of corrective action. They do not change a control result, create a severity level, or replace the control-specific remediation procedure. A control card may cite more than one pattern when different corrective-action classes apply.

Pattern	Use when
R-01 Missing evidence	Retrieve or create the required record for the assessed scope and version, then retest. For a historical finding, recover only verifiable contemporaneous evidence; a new record does not invent the missing past fact.
R-02 Ambiguous meaning	Resolve competing definitions or boundaries through the accountable semantic authority. Version the approved meaning and update affected mappings.

R-03 Unstable identity or grain	Establish the authoritative identifier or resolution rule, declare semantic grain, add crosswalks/tie-breakers where required, and replay the case.
R-04 Missing authority	Identify the accountable business, stewardship, risk, or operational authority. Do not substitute technical ownership or system permission for business authority.
R-05 Conflicting evidence	Preserve the conflict, apply an approved precedence/adjudication rule, record the resolution and losing evidence, or assign Stop/Quarantined until resolved.
R-06 Threshold or rule failure	Correct the evidence or use, or obtain a valid bounded exception. Any justified threshold or scope change is authorized, versioned, and effective prospectively; create a new assessment and preserve the original result.
R-07 Unsupported discovery	Keep candidate evidence Quarantined and route it through the applicable taxonomy, ontology, identity, or AI controls before stated use.
R-08 Material change or drift	Identify affected active or prospective scopes, invalidate readiness as defined, reassess applicable controls and Gates before new reliance, and create linked new records. Preserve prior versions and determinations.
R-09 Missing execution record	Recover verifiable contemporaneous execution evidence where available. If the historical step cannot be established, retain its failed finding or limitation. A rerun is a new execution, not retrospective proof. Add evidence capture for future use.
R-10 Prohibited or out-of-scope use	Stop the prohibited use. Any justified new scope or permitted-use change requires valid competent authority, a prospective version, and new assessment. Do not exclude mandatory obligations to hide failure. An exception supports only the bounded use the authority may lawfully grant.
R-11 Human adjudication	Convert the decision into governed evidence: a mapping, resolution rule, classification, exception, authority decision, or other versioned record with effective period and review condition.
R-12 Automated or AI-assisted control	Use automation to execute the control only when the rule, context, evidence capture, authority, and consequence are explicit. Automation may evaluate evidence; it does not create authority or self-conformance.
R-13 External boundary evidence	When direct inspection is legitimately unavailable, complete the Boundary Evidence Anchor with exact evidence identity, interface/version, time, inaccessible boundary, and scope mapping. Include fingerprints where possible and supporting references where available; attestation alone is insufficient.
R-14 Version and integrity hardening	Pin the exact DACS/artifact/rule version and add verifiable integrity evidence before retest.
R-15 Prospective rule	Correct the governing rule prospectively with authority/effective

correction	dating; preserve the prior rule and prior result; create a new evaluation rather than rewriting history.
R-16 Runtime fail-closed control	Block material action on enforcement failure or use only a previously authorized bounded degraded mode; never improvise fail-open behavior.
R-17 Lawful evidence preservation	Apply the lawful retention/deletion rule and preserve the strongest legally permitted reconstruction anchor; constrain reconstruction claims when the law prevents retention.
R-18 Append-only retest history	Create a new linked evaluation event after remediation; preserve prior failures, Gate states, exceptions, and evidence rather than overwriting them.

7. Core Decision-Scope Controls

Core controls apply to every DACS decision scope. These cards operationalize the Core controls without changing their normative meaning.

Card boundary

The Specification requirement, Prerequisites, Evidence to inspect, and Pass/Fail text below reproduce DACS Specification v1.13. Sections 2 through 5 explain its global assessment and closure rules. Procedures, failure modes, remediation, and examples are informative guidance. Apply the exact Specification version governing the assessment; the catalog does not add criteria or override it.

CORE-001: Decision Scope Is Declared

Prerequisites	None.
Specification requirement	Before evaluating dependent controls, record the specific business decision or use that will be reviewed and the boundary of that review. The decision-scope record identifies what is included, what is excluded, the business level being assessed, and the accountable owner. An initial Bootstrap Scope Record may be used to collect these facts; it does not authorize material use.
Why this control exists	A shared review boundary lets managers, practitioners, and assessors test the same decision and evidence. Without it, teams may assess different uses, compare different grains, or apply approval beyond the use actually reviewed.
When this applies	At initialization of every DACS decision scope and whenever the decision boundary changes. A Bootstrap Scope Record may be used only to collect evidence for CORE-001/CORE-002 and never authorizes material reliance.
Evidence to inspect	Decision-scope record or completed Bootstrap Scope Record, business domain, decision/use statement, grain boundary, owner, in-scope statement, out-of-scope statement, stable scope identifier, and version.
Evidence sufficiency	The record identifies the specific decision or use, domain, grain or multi-grain boundary, included and excluded uses, accountable owner, stable scope identifier, and record version. The recorded boundaries identify which evidence belongs in this review. **Insufficient:** A project, dataset, dashboard, or subject-area name does not establish the decision, evidence boundary, grain, or authority being assessed.
Assessment procedure	1. Retrieve the decision-scope record or completed Bootstrap Scope Record. 2. Check every required field, including the stable identifier and record version. 3. Confirm that the decision, included and excluded uses, and grain describe the same review boundary. 4. Check that the initial collection record has not been used as permission for material reliance.
Control-result determination	**Pass:** The completed record identifies the business domain; the specific decision or use; the grain, or declared boundary covering multiple grains; in-scope use; out-of-scope use; accountable owner; stable scope identifier; and record version. Every required field is present. The recorded decision, included and excluded uses, and grain define which evidence is included in this review. These criteria also apply when the completed record originated as a Bootstrap Scope Record. **Fail:** A required scope field is missing or ambiguous; the scope identifier or version is missing; or an initial scope record is treated as permission for material reliance.

Common failure modes	• Bootstrap record treated as approval to proceed. • Scope lacks stable identifier/version. • Decision/use or grain boundary is ambiguous. • Ownership or permitted/excluded use is missing.
Remediation procedure	**Pattern references:** R-01, R-02, R-04, R-10 **If the record names only a project or dataset:** state the specific decision or use and its evidence boundary. **If grain or use boundaries are missing:** record the business level, included uses, and excluded uses. **If ownership is divided or implicit:** identify the accountable owner and recorded authority. **If identifier or version is missing:** assign a stable scope identifier and version the completed record. **If an initial collection record was used as approval:** stop the unsupported reliance and evaluate the proposed use through the applicable controls and Gate.
Repeatable fix	A reusable decision-scope template requires the same minimum fields and named authority for every evaluation.
Controlled disposition	***Disposition reference:*** **D-01, Missing prerequisite.** Use this reference when the decision scope itself is missing, incomplete, or ambiguous.
Example	A weekly executive Active Customer Count is bounded to North America, account grain, internal operating review, with explicit exclusions.
Non-example	“Customer reporting” with no grain, owner, or permitted-use boundary.
Authority and execution	**Authority:** Business owner owns the decision boundary; governance or stewardship authority resolves scope and grain disputes.
Retest	Reinspect all required scope fields, including identifier and version. Confirm that the recorded boundaries identify the evidence being reviewed and that any material reliance has separate Gate authority.

CORE-002: Materiality and Conditional Applicability Are Bound Before Dependent Controls

Prerequisites	Pass required: CORE-001.
Specification requirement	The decision scope shall establish recorded rules or authority references for every materiality, applicability, approval, authorization, equivalence, compatibility, multi-value, or other conditional predicate it uses. Each rule shall exist independently of the result it governs.
Why this control exists	Binary controls require deterministic predicates and a deterministic evaluation order. Conditional language cannot be left to assessor discretion, and a predicate cannot be justified by a downstream result that depends on that same predicate.
When this applies	Immediately after the decision scope is established and before profile selection or any control containing a conditional predicate.
Evidence to inspect	The recorded rules and authority references needed for the predicates used in this scope, with observable criteria, authority, version, effective period, scope mapping, applicable reassessment triggers, and dependency references. Include Materiality, Applicability, Equivalence, and Multi-Value Rules when the corresponding condition is used; do not require an unused rule merely because it appears in this list.
Evidence sufficiency	Every materiality/applicability/equivalence/multi-value/authority predicate needed by downstream controls has a recorded rule with observable criteria, authority, version, effective period, and scope mapping. No rule may depend on the result it governs.
Assessment procedure	1. List each conditional predicate used by the decision scope. 2. Locate its governing rule/authority and verify completeness. 3. Confirm the rule predates the dependent evaluation and contains no Circular Reliance. 4. Record unresolved predicates as Fail; do not invent a fallback threshold.
Control-result determination	**Pass:** Every conditional predicate required by the decision scope has a recorded rule or authority reference with identifier, owner/authority, version, effective period, observable condition or threshold, decision-scope mapping, and reassessment trigger where applicable; each predicate can be evaluated from recorded facts without assessor invention; no predicate relies on Circular Reliance; and no DACS fallback threshold is required because the organization has supplied the governing rule. **Fail:** A required predicate rule is missing, incomplete, expired, subjective, created from the dependent result, dependent on Circular Reliance, or cannot resolve the predicate from recorded facts. DACS does not supply a fallback materiality or vector threshold.

Common failure modes	• Materiality is decided by assessor judgment. • A profile trigger has no applicability rule. • A threshold is created after seeing the evidence. • A rule relies on the Gate or Conformance Record whose validity depends on that rule.
Remediation procedure	Create or correct the missing rule under accountable authority, version it, give it an effective period, bind it to the decision scope, remove any circular dependency, and retest before evaluating dependent controls.
Repeatable fix	Use a controlled predicate-rule registry/template that requires scope, observable condition/threshold, authority, version, effective period, and reassessment trigger.
Controlled disposition	Disposition reference: D-01, Missing prerequisite. Dependent controls shall not be evaluated as Passed while their required predicate remains unresolved.
Example	A materiality rule approved before evaluation declares that any evidence capable of changing customer eligibility, legal rights, financial exposure, safety, or the primary decision outcome is material for the scope.
Non-example	The assessor decides during review that a difficult relationship is “not material” because including it would cause another control to fail.
Authority and execution	**Authority:** The accountable decision-scope authority approves the governing rules and authority references. Component rule owners remain accountable for their rules. **Execution:** Establish governing predicates independently of their dependent results. Apply each card’s listed prerequisite status; failure diagnosis and containment may continue while permission for material use remains withheld.
Retest	Re-evaluate every previously unresolved predicate from the corrected rule, then evaluate affected downstream controls in dependency order.

CORE-003: Applicable Profiles Are Declared

Prerequisites	Pass required: CORE-002.
Specification requirement	Each conformance evaluation shall record which DACS profiles apply to the stated decision scope, using the recorded profile Applicability Rules.
Why this control exists	Profiles keep DACS narrow while preventing material controls from being skipped.
When this applies	When the decision scope is established or changed in a way that could add or remove Extended Taxonomy, Extended Ontology, or AI Context Contract applicability.
Evidence to inspect	Profile Applicability Rules, profile-applicability record, scope mapping, and reasons for excluded profiles.
Evidence sufficiency	The profile-applicability record identifies Core and each additional profile whose recorded rule evaluates true. Each excluded profile has a false applicability result, reason, rule reference, and supporting scope facts. **Insufficient:** A selected profile list does not establish applicability when exclusions are based on preference, unresolved facts, or the final Conformance Record's unsupported claim.
Assessment procedure	1. Retrieve the profile Applicability Rules and independently recorded scope facts. 2. Apply each profile rule and record its true or false result. 3. Include Core and every additional profile whose rule is true; record the reason and supporting facts for every exclusion. 4. Check that no applicability determination depends on the conformance claim it will support.
Control-result determination	**Pass:** The profile-applicability record identifies Core and every additional profile whose recorded Applicability Rule evaluates true. Each excluded profile has a recorded false applicability result and reason. The determination uses recorded scope facts without assessor inference or Circular Reliance. **Fail:** A profile Applicability Rule is missing or unresolved; a required profile is omitted; an excluded profile lacks a recorded false applicability result and reason; or the determination contains Circular Reliance.
Common failure modes	• Only Core is declared by default. • A profile is omitted because the evidence is inconvenient to assess. • AI or inferred relationships are present but not recognized as profile triggers. • Applicability rationale is undocumented.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-10 - Prohibited or out-of-scope use **If only the Core profile was declared without examining the actual decision path:** trace the material decision path and declare every DACS profile triggered by its use of concepts, relationships, AI, inference, automation, or agentic action **If a profile was omitted because its evidence is difficult or inconvenient to assess:** restore the profile when its triggering condition is present and assess its controls normally **If AI, inference, or material relationships are present but were not recognized as profile triggers:** add the applicable AI Context Contract or Extended Ontology profile and evaluate the affected controls **If the reason for including or excluding a profile is not recorded:** record the applicability rationale for each profile decision
Repeatable fix	A profile-applicability checklist is completed at scope creation and rerun when the decision path changes.
Controlled disposition	***Disposition reference:*** **D-01, Missing prerequisite.** Use this reference when the applicable DACS profiles have not been established from the actual decision path.
Example	Core, Extended Taxonomy, and Extended Ontology are declared; AI Context Contract is Not Applicable because no AI affects the path.
Non-example	Only Core is selected because it is easier, although inferred relationships materially affect the result.
Authority and execution	**Authority:** Decision-scope owner and governance authority determine applicability from the actual decision path, not convenience.
Retest	Reapply the recorded profile rules to the scope facts. Confirm all required profiles are included, each exclusion is supported by a false rule result and reason, and the determination is independently established before it is linked to the final assessment record.

CORE-004: Semantic Contract Exists

Prerequisites	Pass required: CORE-003.
Specification requirement	A decision scope shall have an identified Semantic Contract before evidence is relied on for material use.
Why this control exists	Without a Semantic Contract, meaning, identity, relationship, context, and Gate controls cannot be tested consistently.
When this applies	Before material evidence in the decision scope is treated as ready for stated use, and whenever the governing Semantic Contract changes.
Evidence to inspect	Semantic Contract record, identifier, owner, version, decision-scope mapping, and references to every component required by the applicable profiles.
Evidence sufficiency	The Semantic Contract evidence must identify the contract, its owner and version, the decision scope it governs, and the component references required by every applicable DACS profile. The contract must be the governed agreement for this scope, not a collection of loosely related documentation. ***Insufficient:*** A glossary, data dictionary, semantic layer, prompt, or architecture document is not sufficient by itself unless it is part of, or is explicitly referenced by, the governed Semantic Contract for the stated decision scope.
Assessment procedure	**1.** Inspect the Semantic Contract record. **2.** Verify identifier, owner, version, decision-scope mapping, and each component reference required by the profiles declared for this scope.
Control-result determination	**Pass:** The Semantic Contract has an identifier, owner, version, decision-scope mapping, and referenced components required by the applicable profiles. **Fail:** No Semantic Contract exists, ownership or version is missing, or it is not linked to the decision scope.
Common failure modes	• A glossary, data dictionary, or semantic layer is treated as the whole Semantic Contract. • The contract has no owner or version. • Required profile components are referenced informally. • Scope mapping is missing.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-04 - Missing authority **If a glossary, data dictionary, semantic layer, prompt, or architecture document is being treated as the entire Semantic Contract:** establish or identify the governed Semantic Contract and explicitly reference the supporting artifacts that form part of it **If the contract has no owner or version:** assign the accountable owner and record the applicable version **If required profile components are only referenced informally:** add explicit governed references to the components required by the applicable DACS profiles **If the contract is not mapped to the decision scope:** bind the Semantic Contract to the stated decision scope before stated use
Repeatable fix	A version-controlled Semantic Contract record is created through the same approval and change process for each scope.
Controlled disposition	***Disposition reference:*** **D-01, Missing prerequisite.** Use this reference when the required Semantic Contract is missing, incomplete, unowned, unversioned, or not bound to the decision scope.
Example	SC-CUST-014 v3 is owned by Customer Operations and mapped to the dashboard decision scope and its taxonomy, ontology, and identity references.
Non-example	A glossary link is treated as the Semantic Contract even though it has no owner, version, or scope mapping.
Authority and execution	**Authority:** Semantic Contract owner approves the contract; component owners remain accountable for referenced evidence.
Retest	Reinspect the revised Semantic Contract. Confirm its identifier, owner, version, decision-scope mapping, and all component references required by the applicable profiles.

CORE-005: Physical Attribution or Boundary Evidence Anchor Is Recorded Where Required

Prerequisites	Pass required: CORE-002.
Specification requirement	Each material evidence item shall record the physical attribution required for the decision scope. When an external, legacy, proprietary, or third-party source prevents direct source-level inspection, a Boundary Evidence Anchor may satisfy the attribution requirement only when the unavailable boundary is explicit and the anchor identifies the exact external evidence actually consumed.
Why this control exists	Material evidence must be traceable without making conformance impossible when the organization cannot lawfully or technically inspect a third-party or legacy internal schema.
When this applies	When material evidence requires source attribution, including evidence obtained from external, proprietary, SaaS, legacy, or otherwise inaccessible systems.
Evidence to inspect	Source reference and source-level locator; or Boundary Evidence Anchor containing external source/vendor identity, interface/API/feed/contract identifier and version, payload/event/message/document identifier, acquisition timestamp/effective period, content hash or equivalent fingerprint where possible, supporting contract/SLA/attestation where available, inaccessible-boundary statement, and decision-scope mapping.
Evidence sufficiency	For directly inspectable evidence, the locator identifies the source-level evidence needed to locate, interpret, and test the item. Where visibility is legitimately unavailable, a complete Boundary Evidence Anchor identifies the exact evidence consumed, its source and interface/version, payload identity, time, inaccessible boundary, and scope. Inspect fingerprints where technically possible and supporting contract/SLA/attestation references where available. **Insufficient:** Vendor attestation alone, an unspecified feed, or a reference to current data does not identify the exact evidence consumed.
Assessment procedure	1. Trace each material evidence item to its source-level locator. 2. If direct source-level visibility is legitimately unavailable, verify every required Boundary Evidence Anchor field and the inaccessible-boundary statement. 3. Verify the exact payload/event/message/document identity, interface or contract version, acquisition time, and decision-scope mapping. 4. Inspect the fingerprint where technically possible and supporting references where available; do not treat attestation alone as attribution.

Control-result determination	**Pass:** The evidence item records source-level attribution sufficient to locate, interpret, and test the evidence for the decision scope; or, when direct source-level visibility is legitimately unavailable, a Boundary Evidence Anchor records external source identity, interface/feed/contract identifier and version, payload/event/message/document identifier, acquisition timestamp or effective period, content hash or equivalent immutable fingerprint where technically possible, contract/SLA/attestation reference where available, the inaccessible boundary, and decision-scope mapping. Vendor attestation alone is not sufficient. **Fail:** Material evidence cannot be tied to source-level evidence or a complete Boundary Evidence Anchor, the inaccessible boundary is not declared, or a vendor statement is used as the sole attribution evidence.
Common failure modes	• Vendor name is recorded but not the exact feed/API/payload. • A compliance letter is treated as the sole source anchor. • Proprietary schema is unavailable and no immutable payload reference is preserved.
Remediation procedure	**Pattern references:** R-01, R-13 **If source attribution is missing:** locate the required source-level evidence and preserve its exact reference. **If direct visibility is legitimately unavailable:** create a complete Boundary Evidence Anchor and state the inaccessible boundary. **If the anchor identifies only a vendor or feed:** add the exact interface/version, payload identity, time, and scope mapping. **If attestation is the only support:** obtain the remaining required anchor evidence, including a fingerprint where technically possible and supporting references where available. **If the historical evidence cannot be established:** record the limitation and retain the failed finding.
Repeatable fix	External-source onboarding requires a Boundary Evidence Anchor whenever direct source-level inspection is unavailable.
Controlled disposition	Disposition reference: D-02, Unresolved governed evidence. Candidate evidence remains out of stated use until direct attribution or a complete Boundary Evidence Anchor exists.
Example	A bureau API response is preserved with vendor, endpoint/version, request/response ID, acquisition time, payload hash, contract reference, and a statement that the provider's internal tables are not inspectable.
Non-example	"Credit bureau data" plus a vendor SOC report, with no record of the exact response used.

Authority and execution	Authority: Source custodian and decision-scope owner approve the boundary; legal/procurement evidence may support but not replace the anchor.
Retest	Trace each affected item to its source evidence or verify every required field of the permitted Boundary Evidence Anchor. Confirm exact consumed-evidence identity and the conditional fingerprint and supporting-reference obligations.

© 2026 DataVaultAlliance Holdings LLC. All rights reserved.

CORE-006: Logical-to-Conceptual Binding Exists Where Required

Prerequisites	Pass required: CORE-004, CORE-005.
Specification requirement	Each logical information element used in a material decision path shall map to an approved business concept.
Why this control exists	Logical meaning must be tied to governed business meaning before it supports DACS conformance for the stated scope.
When this applies	When a material logical information element contributes to the decision path and its governed business meaning must be established.
Evidence to inspect	Logical-to-conceptual mapping record, business concept identifier, owner, version, source reference where required, decision-scope mapping.
Evidence sufficiency	The mapping evidence must identify the approved business concept for each material logical information element and include the owner, version, decision-scope applicability, and source reference where the control requires one. ***Insufficient:*** A local field name, technical label, or unapproved term is not sufficient evidence of business meaning unless it is explicitly bound to the approved business concept used by the stated decision scope.
Assessment procedure	**1.** Enumerate material logical information elements. **2.** Verify that each material item maps to an approved business concept with the required owner, version, source reference where required, and decision-scope applicability.
Control-result determination	**Pass:** Each logical information element maps to an approved business concept with owner, version, source reference where required, and decision-scope applicability. **Fail:** The logical element lacks a business concept mapping, maps only to a local term, or maps to an unapproved or ambiguous concept.
Common failure modes	• Logical fields map only to local technical names. • Several logical elements map to one concept without boundary rules. • Mappings are out of date or unowned. • An unapproved concept is used because names appear similar.

Remediation procedure	**Pattern references:** R-02 - Ambiguous meaning; R-01 - Missing evidence; R-04 - Missing authority **If logical fields map only to local or technical names:** map each material logical element to an approved business concept **If several logical elements map to one concept without boundary rules:** record the conditions or boundaries that explain when each mapping is valid **If a mapping is outdated or has no accountable owner:** assign ownership, update the mapping, and record the applicable version or effective period **If a concept was selected because its name appears similar:** obtain semantic-authority approval for the mapping or reject the mapping until the business meaning is proven
Repeatable fix	Logical mappings retain the approved concept, owner, version, decision-scope applicability, and source reference where required.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material logical element is not yet bound to an approved business concept.
Example	logical_customer_status maps to the approved Customer Status concept version used by the decision scope.
Non-example	A warehouse column named cust_type is assumed to mean the enterprise Customer Type concept.
Authority and execution	**Authority:** Semantic authority approves the business concept; mapping owner maintains the logical-to-conceptual binding.
Retest	Recheck each material logical information element. Confirm that it now maps to the approved business concept with the required owner, version, source reference where required, and scope applicability.

CORE-007: Business Identity Anchors Exist Where Required

Prerequisites	Pass required: CORE-004.
Specification requirement	Each identity-bearing concept used in a material decision path shall have a Business Identity anchor.
Why this control exists	Without identity, the enterprise cannot reliably compare history, reconcile systems, reconstruct decisions, or defend analytics.
When this applies	When the material decision path must distinguish a specific business instance across systems, sources, or time.
Evidence to inspect	Identity evidence used for the stated scope: the stable business identifier mapping, durable or composite identity rule, approved resolution record, or equivalent identity evidence permitted by the Pass criterion.
Evidence sufficiency	The identity evidence must show, for every identity-bearing concept in the material decision path, which business identifier, identity rule, composite rule, or approved resolution method is authoritative for the stated semantic grain and decision scope. ***Insufficient:*** A source-system key, local identifier, display value, or match result is not sufficient by itself unless it has been approved as the Business Identity anchor, or as part of the governed identity-resolution method, for the stated grain and decision scope.
Assessment procedure	**1.** List every material concept in the decision path whose use depends on identifying a specific business instance. **2.** For each identity-bearing concept, identify the claimed Business Identity anchor or approved resolution method. **3.** Verify that the anchor or resolution method is approved for the stated semantic grain and decision scope.
Control-result determination	**Pass:** 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:** A concept requires identity for the decision scope and lacks an approved identity anchor.
Common failure modes	• A source key is assumed to be business identity without authority. • Multiple systems use incompatible identifiers with no crosswalk. • Approximate matching is used with no approved resolution rule. • Identity authority is unknown.

Remediation procedure	**Pattern references:** R-03 - Unstable identity or grain; R-04 - Missing authority; R-11 - Human adjudication **If a source-system key or local identifier is being treated as Business Identity without approval:** identify and approve the authoritative business identifier, durable identity rule, composite rule, or resolution method for the stated semantic grain and decision scope **If systems use incompatible identifiers:** create or approve the governed crosswalk or identity-resolution rule that connects the identifiers at the correct semantic grain **If approximate matching is used without an approved resolution rule:** govern the matching rule, threshold, tie-break logic, authority, and unresolved-case handling before relying on the result **If identity authority is unknown:** assign the accountable identity authority before the identity evidence is used for material stated use
Repeatable fix	Identity anchors are registered with scope, grain, authority, effective period, and resolution method.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference for identity-bearing evidence that still lacks an approved Business Identity anchor.
Example	Customer Account uses CRM Master Account ID, with a governed crosswalk for acquired systems.
Non-example	A display name is used to join customers across systems without an approved identity rule.
Authority and execution	**Authority:** The designated identity authority or steward approves identifiers and resolution rules; technical teams implement them.
Retest	Recheck every material identity-bearing concept. Confirm that each concept now has an approved Business Identity anchor or governed resolution method for the stated semantic grain and decision scope.

CORE-008: Semantic Grain Is Declared for Identity-Bearing Evidence

Prerequisites	Pass required: CORE-007.
Specification requirement	Each material Business Identity shall declare semantic grain for each identity-bearing evidence item at each point of consumption within the decision path. Where identity-bearing evidence is transformed, aggregated, split, or reconciled across grains, the source grain, transformation rule, and resulting grain shall be recorded.
Why this control exists	Identity failures often occur when different grains are treated as equivalent or when aggregation changes the business level at which identity is interpreted. DACS permits multi-grain decision paths only when each grain and material transition is explicit.
When this applies	When a material Business Identity is used, compared, counted, reconciled, resolved, or acted upon.
Evidence to inspect	Identity record, per-consumption semantic grain declaration, uniqueness exception where applicable, decision-scope mapping, and source-grain, transformation/aggregation-rule, and resulting-grain evidence for each material grain transition.
Evidence sufficiency	Each identity-bearing item has an explicit grain at every point of consumption. Each material transformation, aggregation, split, or reconciliation records the source grain, governing rule, and resulting grain. **Insufficient:** A single grain label on the source record does not establish the grain at later consumption points or explain a material change between grains.
Assessment procedure	1. Trace each identity-bearing evidence item through its points of consumption. 2. Verify the grain at each point and its link to the decision scope. 3. For each material grain transition, inspect source grain, transformation or aggregation rule, and resulting grain. 4. Verify any claimed cross-grain equivalence under its approved rule.
Control-result determination	**Pass:** Every identity-bearing evidence item records the business level at which it is unique and meaningful at its point of consumption, links that grain to the decision scope, and records each material grain transition from source grain to resulting grain with the governing transformation or aggregation rule. **Fail:** An identity-bearing evidence item is consumed without a declared grain, different grains are treated as equivalent without an approved transformation or equivalence rule, or a material grain transition is not recorded.

Common failure modes	• Account, person, household, contract, and transaction grains are mixed. • Uniqueness is asserted only technically. • Aggregate counts are compared as if they share the same business grain. • Grain is documented but not bound to the scope.
Remediation procedure	**Pattern references:** R-03, R-02 **If grain is missing at a consumption point:** declare the business level at that point and bind it to the scope. **If an aggregation, split, or reconciliation changes grain:** record the source grain, governing transformation, and resulting grain. **If different grains are treated as equivalent:** correct the use or establish the approved transformation or equivalence rule prospectively. **If a transformation changes meaning:** reassess the affected identity and downstream use.
Repeatable fix	Identity records require a semantic-grain field and a uniqueness expectation before approval.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when the semantic grain of a material Business Identity is missing, incompatible, or not approved for the scope.
Example	Account ID is unique at customer-account grain; household ID is recorded separately and is not treated as equivalent.
Non-example	A household key and an account key are treated as interchangeable because both are called Customer ID.
Authority and execution	**Authority:** Business identity owner or steward approves semantic grain and uniqueness expectations for the scope.
Retest	Trace the affected items through every relevant consumption point and material grain transition. Confirm the recorded grain, source-to-result transformation, scope mapping, and any approved equivalence rule.

CORE-009: Business Concept Is Not Assumed to Be Business Identity

Prerequisites	Pass required: CORE-007.
Specification requirement	A business concept shall not be treated as a Business Identity unless identity evidence is recorded.
Why this control exists	A concept defines meaning; identity distinguishes a specific instance.
When this applies	When a business concept, taxonomy node, glossary term, label, or classification might be used as evidence of a specific business instance.
Evidence to inspect	Business concept record, decision-scope mapping, and the distinct identity rule, identifier mapping, or approved resolution method used for each identity-bearing use.
Evidence sufficiency	The evidence must distinguish the governed meaning of a business concept from the evidence that identifies a specific business instance. Each identity-bearing use must have its own approved identifier, identity rule, or resolution method. ***Insufficient:*** A concept name, taxonomy node, glossary term, classification, category, or label is not sufficient evidence that two records represent the same business instance unless separate Business Identity evidence establishes that identity.
Assessment procedure	**1.** Inspect each identity-bearing use of a business concept. **2.** Verify the identity evidence is distinct from the concept definition, taxonomy node, glossary term, or classification label and includes an approved identifier or resolution method.
Control-result determination	**Pass:** Each identity-bearing use has a distinct identity rule, identifier, or approved resolution method beyond the existence of a concept label. **Fail:** A concept name, taxonomy node, glossary term, or classification is used as identity evidence without an approved identity anchor.
Common failure modes	• A taxonomy node, glossary term, label, or class is used as if it identifies a specific instance. • A concept-level code is confused with an instance identifier. • Identity evidence is omitted because the business concept is well defined.

Remediation procedure	**Pattern references:** R-03 - Unstable identity or grain; R-02 - Ambiguous meaning **If a concept, taxonomy node, glossary term, label, or class is being used as if it identifies a specific instance:** separate the concept definition from the evidence that identifies an individual business instance **If a concept-level code is being treated as an instance identifier:** record the actual business identifier or approved identity-resolution rule required for the instance **If identity evidence was omitted because the concept is well defined:** add the required Business Identity anchor for every use that depends on identifying a specific instance
Repeatable fix	Templates and reviews require distinct fields for business concept and Business Identity evidence.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a concept, label, classification, or taxonomy node is being used as identity evidence without a separate approved identity anchor.
Example	Customer is the concept; CRM Master Account ID plus its grain and resolution rule identifies the customer account instance.
Non-example	The taxonomy term “Customer” is used as proof that two records refer to the same customer.
Authority and execution	**Authority:** Semantic authority owns concept meaning; identity authority owns instance-identification evidence. Neither substitutes for the other.
Retest	Reinspect each identity-bearing use of a business concept. Confirm that the evidence now separates concept meaning from the approved identifier, identity rule, or resolution method used to identify a specific instance.

CORE-010: Identity Resolution Produces Determinate Results

Prerequisites	Pass required: CORE-002. Recorded result required: CORE-007, CORE-008.
Specification requirement	Each identity-resolution method used for stated use shall return the same identity result, or the same unresolved or exception result, when the inputs, rule set, threshold, method version, and decision scope are unchanged.
Why this control exists	Material decisions require repeatable identity outcomes.
When this applies	When identity resolution, matching, mastering, or adjudication determines identity in a decision path relied on for stated use.
Evidence to inspect	Identity-resolution method and version, tested inputs, rule set, threshold, scope reference, repeat-test results, and exception record where applicable.
Evidence sufficiency	Repeat-test records preserve unchanged inputs, rules, thresholds, method version, and scope. The tests return the same identity result or the same governed unresolved or exception result. **Insufficient:** An explanation for different outcomes under unchanged conditions does not establish Pass. Repeatable unresolved outcomes establish repeatability only, not identity readiness.
Assessment procedure	1. Record the tested inputs, rule set, threshold, method version, and scope. 2. Repeat the identity test without changing those conditions. 3. Compare outcomes, including unresolved or exception results. Any different outcome under unchanged conditions is Fail. 4. Record a changed configuration as a different test case and preserve the original result.
Control-result determination	**Pass:** Repeat tests using the same recorded inputs, rules, thresholds, method version, and scope return the same identity result or the same unresolved or exception result. A repeatable unresolved result does not establish that identity is ready for material use. **Fail:** Any different identity outcome under the same inputs, rule set, threshold, version, and decision scope is Fail. A recorded explanation does not convert that failed determinism test into Pass; a changed rule, threshold, version, or scope is a different test case.

Common failure modes	• Probabilistic or approximate resolution returns different identities for the same case. • Tie-breakers are undocumented. • Model or threshold version is not captured. • A steward resolves repeated cases differently because the adjudication was not converted into a governed rule or mapping.
Remediation procedure	**Pattern references:** R-03 - Unstable identity or grain; R-06 - Threshold or rule failure; R-11 - Human adjudication **If the same identity case produces different outcomes under the same governed conditions:** identify the source of the variation and establish a deterministic rule or governed unresolved outcome **If tie-break logic is undocumented:** define and approve the tie-break rule used when more than one candidate satisfies the primary rule **If the model, method, rule, or threshold version is not captured:** version the identity-resolution method and record the version and threshold used for the assessed case **If human adjudication produces inconsistent repeated outcomes:** convert the adjudication into a governed mapping, rule, tie-break decision, or recorded exception that can be applied consistently
Repeatable fix	The same inputs, rule version, thresholds, and scope produce the same identity or the same unresolved/exception result. Human adjudications become governed mappings or rules with effective dates.
Controlled disposition	***Disposition reference:*** **D-06, Determinacy or repeatability.** Use this reference while identity resolution does not reproduce the same result, or the same governed unresolved or exception result, under the same governed conditions.
Example	Two duplicate account candidates resolve to the same mastered account after the steward approves a tie-break rule and the replay test repeats the result.
Non-example	A reviewer manually chooses a different account each time without recording why or converting the choice into a governed rule.
Authority and execution	**Authority:** Identity authority owns the resolution rule; steward adjudication must be converted into governed rule, mapping, or exception evidence when repeatability is required. **Execution:** The same identity case must be replayable under the same inputs, rule version, thresholds, and scope so the result can be compared.
Retest	Repeat the identity test under the same recorded conditions and compare results. If remediation changed a rule or configuration, assess a new version and retain the original failure. A repeatable unresolved result does not permit material identity use.

CORE-011: Discovered Evidence Is Quarantined Until Governed

Prerequisites	Recorded result required: CORE-002, CORE-003.
Specification requirement	Candidate evidence shall be held under a recorded disposition that prevents material reliance unless the applicable Gate explicitly permits the stated use.
Why this control exists	Quarantined allows candidate evidence to remain available for exploration while preventing untested evidence from being relied on for material decisions by default.
When this applies	When evidence enters the decision path through discovery, inference, generation, retrieval, import, or another candidate-evidence process.
Evidence to inspect	Candidate evidence log, recorded disposition and holding or use evidence, Gate Record when evaluated, exception record where applicable, owner or review authority, and next action.
Evidence sufficiency	Recorded handling shows candidate evidence held as Quarantined or used only as the applicable Gate permits. Any constrained use has a valid authorizing exception and stays within its bounds. **Insufficient:** Review or exception paperwork alone is insufficient if actual material use violates Stop, Quarantined, scope, validity, or exception limits.
Assessment procedure	1. Identify candidate evidence and retrieve its holding or use records. 2. For held evidence, verify Quarantined handling prevents material reliance. 3. For used evidence, compare actual use with the recorded Gate state, scope, authority, validity, and constraints. 4. Where Caution permits use, verify the valid authorizing exception and its limits.
Control-result determination	**Pass:** Candidate evidence is held as Quarantined, or its actual use follows the recorded Gate disposition. Any constrained use has a valid authorizing exception and remains within its recorded bounds. **Fail:** Candidate evidence is relied on as evidence for stated use without applicable Gate evaluation, a recorded readiness state, or approved exception handling.
Common failure modes	• Candidate evidence enters a dashboard or model before Gate review. • AI-generated evidence is treated as ready for stated use because a human viewed it. • Discovered relationships have no candidate status. • Constrained use occurs with no exception record.

Remediation procedure	**Pattern references:** R-07 - Unsupported discovery; R-10 - Prohibited or out-of-scope use **If candidate evidence entered a dashboard, model, or decision path before Gate review:** remove it from stated use and assign the evidence to Quarantined until the applicable controls are completed **If AI-generated evidence is being treated as ready for stated use because a human viewed it:** treat the generated item as candidate evidence and route it through the same applicable controls as other evidence **If a discovered relationship has no candidate status:** record the relationship as candidate or Quarantined evidence and route material relationships to Extended Ontology review **If constrained use is occurring without an exception record:** record an authorized bounded exception with its limits and review condition or Stop the use
Repeatable fix	Discovery workflows label candidate evidence separately from evidence that is ready for stated use and route it through a defined review path.
Controlled disposition	***Disposition reference:*** **D-03, Ungoverned candidate evidence.** Use this reference for candidate evidence that has not yet passed the applicable controls or received an approved constrained-use exception.
Example	An AI-discovered customer relationship is retained for investigation but remains Quarantined until ontology controls pass.
Non-example	A newly inferred relationship is added directly to an executive risk score without completing the required ontology review.
Authority and execution	**Authority:** Discovery owner may capture candidate evidence; the applicable governance, semantic, identity, relationship, or AI authority controls promotion toward stated use.
Retest	Compare the affected evidence's actual holding or use with its Gate disposition. Verify prevention of prohibited reliance and compliance with any authorized constrained-use bounds. Containment Pass does not change another control's Fail.

CORE-012: DACS Normative Version Is Pinned

Prerequisites	Pass required: CORE-001.
Specification requirement	Each control evaluation, Gate Record, and Conformance Record shall identify the exact normative DACS Specification version and applicable control-set version used for the evaluation.
Why this control exists	A historical Pass, Fail, Gate state, or conformance claim is not reconstructable unless the exact normative control definitions used at that time are known.
When this applies	Whenever any normative DACS evaluation, Gate Record, or Conformance Record is created or relied upon.
Evidence to inspect	DACS Specification version reference, applicable profile/control-set version reference, evaluation record, Gate Record where present, and Conformance Record where present.
Evidence sufficiency	DACS version/control-set references must be explicit and retrievable.
Assessment procedure	1. Inspect each evaluation and each Gate or Conformance Record where present. 2. Retrieve the exact Specification and applicable control-set/profile definitions referenced. 3. Confirm the definitions are those used by that evaluation; a later completed record is not a prerequisite for inspecting earlier independent evaluation evidence.
Control-result determination	**Pass:** The evaluation evidence, Gate Record, and Conformance Record where present identify the exact DACS Specification version and applicable profile/control-set version in force for the evaluation, and those references are retrievable. **Fail:** The normative DACS version cannot be determined, a later version is substituted retroactively for the version actually used, or the record cannot establish which control definitions governed the result.
Common failure modes	• Version omitted. • “Current DACS” used instead of exact version. • Later control wording substituted retroactively.
Remediation procedure	Add exact normative version references and preserve the referenced definitions; if the historical version cannot be established, the affected historical claim fails.
Repeatable fix	All DACS record schemas require normative-version fields.

Controlled disposition	Disposition reference: D-01, Missing prerequisite.
Example	Gate G-22 records DACS Specification v1.13 and the exact applicable profile/control-set version. Historical records retain the earlier version actually used.
Non-example	A historical Gate says only “DACS compliant” with no version.
Authority and execution	Authority: DACS record owner preserves version references; evaluator confirms the normative version used.
Retest	Reinspect the record and verify the exact normative definitions can be retrieved.

CORE-013: Context, Version, and Causal Order Are Preserved

Prerequisites	Pass required: CORE-012. Recorded result required: CORE-004, CORE-005, CORE-006, CORE-007, CORE-008.
Specification requirement	Each decision path relied on for stated use shall preserve the minimum context, artifact versions, and causal ordering required to reconstruct the state of information and control at the time of use. Distributed paths may use logical causal-order markers together with declared wall-clock uncertainty rather than requiring a universal DACS clock tolerance.
Why this control exists	Accountability depends on the state and causal order that existed at the time, not on current definitions, current artifacts, or assumptions that unavailable historical AI models can be recreated.
When this applies	When a decision path relied on for stated use must later be reconstructed using the context that was in force at the time of use.
Evidence to inspect	Context record, time-source reference, timestamps/effective periods, declared clock uncertainty where applicable, correlation/logical-order markers, source record, Semantic Contract/taxonomy/ontology/identity/data/data-model/process/AI-model version references where material, DACS Specification version, and historical-model reproducibility limitation where applicable.
Evidence sufficiency	Preserved evidence establishes the context and artifact versions effective at use. Distributed paths include the recorded ordering rule, authoritative time source, declared clock uncertainty, and correlation or logical-sequence evidence. Historical AI evidence distinguishes reconstruction from rerunning the original model. **Insufficient:** Current artifacts, timestamps without adequate ordering evidence, or a newer AI model run cannot establish the historical state.
Assessment procedure	1. Retrieve context, source assertions, scope and contract references, and all required effective versions. 2. Inspect time-source evidence and, for distributed paths, clock uncertainty and correlation or logical-sequence markers under the recorded ordering rule. 3. For unavailable historical AI models, inspect contemporaneous provider/model/version, inputs/context, output, available material parameters, tool/API use, and trace. 4. Confirm reproduction limitations are recorded and no current artifact is substituted for historical evidence.

Control-result determination	**Pass:** Preserved context establishes the timestamp or effective period, authoritative time source, source assertion, decision-scope identifier, Semantic Contract version, and applicable taxonomy, ontology, identity-rule, and DACS Specification versions. Record material data, data-model, AI-model, or process versions where available. Distributed paths also preserve declared clock uncertainty and correlation or logical-sequence evidence sufficient to establish causal order under the recorded ordering rule. When the historical AI model is unavailable, preserve contemporaneous provider/model/version identity, inputs and context, output, material parameters where available, tool/API use, and execution trace. Record that the original execution cannot be rerun. Complete contemporaneous evidence may support reconstruction even when reproduction is unavailable. **Fail:** Causal order cannot be established under the declared ordering rule, required historical artifact versions cannot be identified, a current artifact is substituted for a historical version, or an unavailable historical model is treated as reproducible without the original model. Unavailability of the historical model does not by itself fail reconstructability when contemporaneous evidence is otherwise complete, but the reproducibility limitation must be recorded.
Common failure modes	• Current definitions explain a historical decision. • Causal order cannot be established across distributed traces. • Model/provider/version is missing. • A newer AI model is treated as reproduction of the original.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-09 - Missing execution record **If current definitions are being used to explain a historical decision:** restore or reference the semantic versions that were effective at the time of use **If a required taxonomy, ontology, identity, or context version is missing:** add the missing historical version reference or reassess the evidence if the original state cannot be established If the Gate Record or readiness state was not preserved: restore the contemporaneous Gate evidence when it exists; otherwise rerun the applicable Gate before relying on the evidence for stated use **If source assertions were overwritten:** restore the historical source assertion from verifiable evidence when possible; if the original assertion cannot be established, reassess the affected evidence and do not claim historical reconstructability **If required context exists only in memory, email, or informal notes:** convert verifiable context into a governed historical context record; if the required historical state cannot be proven, do not treat the decision path as reconstructable
Repeatable fix	Context is recorded as part of the evidence package at execution or Gate time, not reconstructed from memory later.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when required historical context cannot yet be retrieved for the decision path relied on for stated use.
Example	The record preserves source assertion time, Semantic Contract v4, taxonomy v7, identity rule v2, Gate G-12, and readiness state.
Non-example	Only the current glossary and current mapping are available, so the meaning used three months earlier cannot be established.
Authority and execution	**Authority:** Decision-scope owner defines required context; evidence custodians preserve the historical versions and Gate records.
Retest	Reconstruct the state and event order from the required context and effective versions. Verify distributed-ordering evidence and any historical-model reproduction limitation. Do not use a newer model as proof of the original execution.

CORE-014: Gate Record Is Created

Prerequisites	Pass required: CORE-012. Recorded result required: CORE-002, CORE-003, CORE-013.
Specification requirement	Each controlled transition toward stated use shall capture the Gate determination and required record fields before or at that transition, using the exact DACS version applied. A completed Gate Record shall exist before the transition unless the path uses the bounded Buffered Gate Capture procedure in Section 9.1. That procedure permits delayed durable persistence, not delayed authorization.
Why this control exists	Gates convert governance from policy into operational control.
When this applies	At each material transition from candidate or governed evidence toward stated use.
Evidence to inspect	Gate Record with complete minimum payload including DACS Specification/control-set version references.
Evidence sufficiency	A completed Gate Record has the full Section 9.1 payload and the exact normative versions. A permitted buffered path captures the complete determination before action and durably persists it within the declared interval measured from capture time. **Insufficient:** A later approval, partial capture, promised future record, or missed persistence deadline does not satisfy the record requirement.
Assessment procedure	1. Retrieve the Gate Record and check every Section 9.1 field against its scope and effective versions. 2. Compare the determination and capture time with the transition or action time. 3. If buffering is used, verify complete pre-action capture, stable Gate ID, trace link, and declared maximum persistence interval. 4. Verify durable completion within that interval. Assess completion when the evidence exists or the deadline expires; do not pre-record Pass. 5. Verify required follow-up evaluations are separate from controls actually evaluated before action and later events preserve the original determination.

Control-result determination	**Pass:** The completed Gate Record contains Gate ID, scope identifier/version, DACS Specification version, applicable profile/control-set version, evaluated control IDs and results, evidence references, timestamp/effective period, authority or approved automated rule reference, readiness state, applicable constraint/exception reference, validity condition for Proceed or Caution, and review condition. Where buffering is used, the complete pre-action capture and subsequent durable record also satisfy Section 9.1. **Fail:** A required field or valid normative-version reference is missing, the transition occurs without the required completed record or authorized complete pre-action capture, or buffered persistence violates Section 9.1.
Common failure modes	**• Approval occurred in a meeting or chat but no Gate record exists.** **• Gate record omits evaluated controls or readiness state.** **• Responsible authority or approved rule reference is unclear.** **• A Gate is recorded after the transition it was supposed to control.**
Remediation procedure	**Pattern references:** R-09, R-14, R-18 **If fields or version references are missing:** recover only verifiable evidence and record a linked finding; do not invent historical authorization. **If action preceded authorization or complete capture:** record the failure and correct the future execution barrier. **If buffering lacks a bound or misses its deadline:** record a linked failure, apply CORE-017 failure handling, and reassess affected further reliance. **If later completion overwrote the original event:** restore verifiable history and create linked completion or replacement records.
Repeatable fix	The Gate captures a complete versioned determination before the transition. Permitted buffering has a measured persistence interval and creates linked completion or failure events.
Controlled disposition	***Disposition reference:*** *D-01, Missing prerequisite.* *Use this reference when the required Gate Record does not exist or is incomplete for the transition.*
Example	Gate G-12 captures the scope, versions, controls actually evaluated, evidence, authority, Caution bounds, validity, and trace link before action. Required execution follow-up evaluations are listed separately. Durable persistence completes within the declared interval.
Non-example	An action runs first; a later approval is backdated and the record marks execution-completion controls Pass before their evidence exists.

Authority and execution	**Authority:** The recorded decision-scope authority or approved rule governs the Gate determination. **Execution:** Authorization and complete capture precede the controlled transition. Only durable persistence may be delayed under Section 9.1; later completion does not authorize an earlier action.
Retest	Inspect a controlled transition and the complete Section 9.1 payload. For buffering, verify capture precedes action, persistence meets its declared interval, completion checks are evidence-backed, and all later events link to the unchanged original capture.

CORE-015: Gate Record Is Structured

Prerequisites	Recorded result required: CORE-014.
Specification requirement	Each Gate Record shall be structured so its required fields are machine-readable or exportable as a data object.
Why this control exists	A Gate Record must be inspectable and exchangeable evidence, not merely a human-readable statement.
When this applies	Whenever a completed Gate Record is created, queried, exported, exchanged, or assessed, including completion of a permitted buffered record.
Evidence to inspect	Completed structured Gate Record, exportable Gate object or equivalent, field-level evidence for Section 9.1, and authorized retrieval or export evidence. Where buffering is used, include the pre-action capture, declared persistence interval, and durable-persistence result.
Evidence sufficiency	An authorized query or export exposes every Section 9.1 field as structured data. If buffering is used, the record includes complete pre-action capture and evidence of durable persistence within its declared interval. **Insufficient:** A readable narrative, screenshot, approval email, or partial structured object does not establish that every required Gate field can be retrieved as structured data.
Assessment procedure	1. Retrieve the completed Gate Record through an authorized query or export. 2. Compare its structured fields with the Section 9.1 payload and applicable control requirements. 3. Verify stable scope, control, evidence, authority, timing, readiness, validity, review, and reconstruction references. 4. For a buffered path, inspect complete capture, declared interval, and durable-persistence result. Do not claim Pass before required completion evidence exists.
Control-result determination	**Pass:** The Gate Record can be consumed, queried, exported, or exchanged as structured data. It contains every required field under Section 9.1. **Fail:** The Gate outcome exists only as unstructured narrative, slide content, email approval, log text without the required fields, or undocumented assertion.
Common failure modes	• Gate outcome exists only in narrative or email. • Structured export omits required payload fields. • Evidence or control references are flattened into untraceable prose. • Buffered capture is incomplete or persistence misses its deadline.

Remediation procedure	**Pattern references:** R-01, R-09, R-14, R-18 **If the outcome is narrative only:** represent every required Gate field in a structured record. **If fields or stable references are omitted:** correct the schema and preserve traceable references. **If authorized consumers cannot retrieve the fields:** provide a queryable or exportable representation. **If buffering is incomplete or late:** record the failure and correct capture/persistence handling without rewriting the original Gate event.
Repeatable fix	A versioned Gate schema or equivalent structured record exposes the complete required payload to authorized consumers and retains linked capture and persistence evidence.
Controlled disposition	***Disposition reference:*** *D-01, Missing prerequisite.* *Use this reference when the completed Gate Record or its required structured fields cannot be established. Apply the actual Gate logic; a structure check does not grant permission for material use.*
Example	An authorized JSON export exposes Gate ID, scope/version, control results, evidence, authority, timing, readiness, validity, constraints, review, and reconstruction references.
Non-example	Approval is available only as an email paragraph, and required Gate fields cannot be retrieved as structured data.
Authority and execution	**Authority:** The Gate record owner is accountable for its required fields; the platform or evidence custodian maintains authorized structured retrieval. **Execution:** Test the completed record's structure and any applicable buffered-completion evidence separately from the original authorization.
Retest	Query or export the remediated completed Gate Record. Confirm every required field is structured and retrievable. Verify buffering completion where used; preserve any earlier creation or timing failure as a separate result.

CORE-016: Readiness Validity Is Declared and Enforced

Prerequisites	Recorded result required: CORE-014.
Specification requirement	Each Proceed or Caution Gate readiness state shall declare and enforce a Readiness Validity Condition for new material reliance. Historical Gate Records remain immutable evidence of the state determined at their original evaluation time.
Why this control exists	Readiness is scope-bound and time-bound. A prior permitted state shall not remain valid silently after its declared validity condition ends.
When this applies	Whenever a Proceed or Caution Gate state is relied on for new material use, and when its recorded expiration or reassessment trigger occurs.
Evidence to inspect	Gate Record, Readiness Validity Condition, expiration/trigger evidence, reassessment record where triggered, new Gate Record where reassessed, and immutable prior Gate Record.
Evidence sufficiency	Each Proceed or Caution state has a recorded validity condition. Evidence shows that expiration or a declared trigger blocks new material reliance or invokes the required reassessment. Original Gate Records remain unchanged. **Insufficient:** A review date alone does not establish enforcement when use continues after expiry or triggering change without reassessment.
Assessment procedure	1. Inspect validity conditions for each Proceed or Caution state under review. 2. Verify an expiration, effective-period end, event trigger, or authorized no-fixed-expiration rule with defined triggers. 3. Inspect or test expired and triggered conditions; confirm new reliance is blocked or reassessed. 4. Trace any new evaluation to the preserved original Gate Record.
Control-result determination	**Pass:** Each Proceed or Caution state has an expiration timestamp, effective-period end, event-triggered reassessment rule, or explicitly authorized no-fixed-expiration rule with defined reassessment triggers; new material reliance is blocked or reassessed when the condition expires or triggers; and historical records are not retroactively rewritten. **Fail:** New material reliance continues after expiration/trigger without reassessment, or historical Gate Records are retroactively changed rather than linked to a new evaluation.
Common failure modes	• Proceed or Caution has no declared validity condition. • New use continues after expiration or a declared trigger. • No-fixed-expiration is assumed without authority or triggers. • A new state overwrites the historical Gate Record.

Remediation procedure	**Pattern references:** R-08, R-18 **If validity is missing:** record an authorized expiration or reassessment rule. **If use continues after expiry or a trigger:** block affected new reliance and reassess it. **If no-fixed-expiration is assumed:** obtain explicit authority and define reassessment triggers, or set a bounded validity period. **If history was overwritten:** restore verifiable prior records and link the new evaluation.
Repeatable fix	Recorded Gate validity is checked before new reliance. Expiration and material-change triggers invoke reassessment and preserve the earlier determination.
Controlled disposition	***Disposition reference:*** *D-04, Change or reassessment.* *Use this reference when readiness has expired or a declared trigger requires reassessment before new reliance.*
Example	A Proceed state expires Friday. On Monday, the workflow blocks new use until a linked Gate evaluation establishes a current readiness state; Friday's record remains unchanged.
Non-example	A prior Proceed state is reused indefinitely after its validity period ends.
Authority and execution	**Authority:** The decision-scope authority approves the validity condition and any no-fixed-expiration rule. The responsible workflow or process owner enforces it. **Execution:** Check validity for new reliance and preserve linked reassessment evidence when the condition expires or triggers.
Retest	Test an expiration and an applicable reassessment trigger. Verify affected new reliance is blocked or reassessed and the historical Gate Record remains unchanged.

CORE-017: Runtime Enforcement Failure Is Governed

Prerequisites	Recorded result required: CORE-014, CORE-015, CORE-016.
Specification requirement	Each material automated or hybrid path that depends on a Gate or Context Enforcement Point shall declare and enforce behavior for enforcement-service failure, loss of authoritative state, stale cached policy, or unavailable prerequisite evidence.
Why this control exists	Control infrastructure failure must not silently become permission to act.
When this applies	When a material automated or hybrid path depends on Gate or Context Enforcement Point availability.
Evidence to inspect	Runtime failure policy, fail-closed rule, degraded-mode authorization where applicable, action-class boundary, authority reference, constraints, expiration, invalidation triggers, execution evidence, and Gate/trace records.
Evidence sufficiency	A fail-closed rule or pre-authorized bounded degraded mode must exist before failure.
Assessment procedure	1. Simulate or inspect enforcement-service failure. 2. Confirm material actions stop by default. 3. If degraded mode exists, verify pre-authorization, action class, constraints, expiry, invalidation, and evidence capture.
Control-result determination	**Pass:** The path fails closed by default for material action, or uses a previously authorized bounded degraded mode whose action class, authority, constraints, evidence requirements, expiration, and invalidation triggers were recorded before the failure; no action outside that degraded-mode authorization is permitted. **Fail:** A material action proceeds because the enforcement mechanism is unavailable, a degraded mode is improvised after failure, the authorization is expired or broader than the action, or required evidence cannot be preserved.
Common failure modes	• “Fail open” on service outage. • Degraded mode improvised during outage. • Cached state expired but still used.

Remediation procedure	**Pattern reference:** R-16 Implement fail-closed behavior for material action. If continuity requires a degraded mode, obtain prospective authorization for its exact bounded action class, authority, constraints, evidence requirements, expiration, and invalidation triggers. Do not improvise permission during an outage or infer that reversibility alone authorizes action.
Repeatable fix	Runtime design includes tested fail-closed behavior and governed degraded-mode policy.
Controlled disposition	Disposition reference: D-05, Threshold, constraint, or conflict.
Example	A payment recommendation service blocks external release when Gate service is unavailable; a pre-approved read-only advisory mode may continue for 15 minutes under Caution.
Non-example	Transactions continue because the policy service timed out.
Authority and execution	Authority: Business/risk owner authorizes any degraded mode before an outage; engineering enforces it.
Retest	Test outage behavior and confirm unauthorized material action cannot occur.

CORE-018: Conformance Record Exists

Prerequisites	Pass required: CORE-012. Recorded result required: CORE-003, CORE-014, CORE-016.
Specification requirement	Each claim of decision-scope conformance, or recorded DACS determination of readiness for stated use, shall be supported by a completed Conformance Record bound to the exact DACS version used. A readiness determination may preserve failed controls and authorized constraints; the record does not make those results conformant.
Why this control exists	A claim of stated use without an evidence record is an assertion, not a DACS conformance outcome.
When this applies	Whenever decision-scope conformance is claimed or a DACS determination of readiness for stated use is recorded.
Evidence to inspect	Conformance Record, DACS Specification/control-set version references, profile-applicability determination, control results, evidence links, Gate/readiness references, authority, timestamp/effective period, review condition, and recorded limitations.
Evidence sufficiency	The completed Conformance Record supports the exact scope-bound readiness or conformance determination and includes every Section 9 field and applicable control requirement. It preserves failed results and constraints where present. **Insufficient:** The existence of a record, badge, or readiness claim does not prove the other controls passed. A complete record of Caution with failed controls does not establish full scope conformance.
Assessment procedure	1. Identify the readiness or conformance determination being assessed. 2. Retrieve its completed Conformance Record and exact scope and normative-version references. 3. Verify every Section 9 field and CORE-018 criterion, including independently established profile applicability, all applicable results, evidence, Gate, authority, timing, review, and limitations. 4. Check that any full-conformance claim is supported by all applicable mandatory results, rather than by the record's existence.

Control-result determination	**Pass:** The record includes decision scope/version, DACS Specification version, applicable profiles/control-set versions, the independently established profile-applicability determination, applicable controls and Pass/Fail/Not Applicable results, evidence links, Gate Record/readiness state, responsible authority or approved rule reference, timestamp/effective period, review condition, and any recorded limitations including unavailable historical-model reproducibility where relevant. **Fail:** A required readiness or conformance determination lacks a complete Conformance Record, required fields are missing, or the normative version used cannot be established.
Common failure modes	**• A readiness-for-stated-use claim appears in a report or presentation with no Conformance Record.** **• The record exists but omits failed controls or exceptions.** **• Evidence links are out of date.** **• The review condition or responsible authority or approved rule reference is missing.**
Remediation procedure	**Pattern references: R-01 - Missing evidence; R-09 - Missing execution record** **If DACS conformance is claimed without a Conformance Record: create the required Conformance Record before making the claim or remove the claim** **If the Conformance Record omits failed controls, exceptions, or other required results: complete the record so the full control outcome is visible** **If evidence links are outdated or broken: repair the links to the evidence used for the stated determination** **If the review condition or responsible authority or approved rule reference is missing: record the required authority or approved rule reference and review condition before relying on the claim**
Repeatable fix	A Conformance Record is produced from a standard record structure after Gate evaluation, with required control, evidence, authority, timestamp, and review fields.
Controlled disposition	***Disposition reference:*** **D-01, Missing prerequisite.** Use this reference when stated-use readiness is claimed but the required Conformance Record is missing.
Example	The decision scope has a Conformance Record listing all applicable controls and their results, evidence links, readiness state, responsible authority or approved rule reference, and review condition.
Non-example	A slide claims that evidence is ready for stated use under DACS, but no scope-bound Conformance Record exists.

Authority and execution	**Authority:** The responsible authority approves the Conformance Record within the stated scope. An approved rule may generate or populate the record under that authority.
Retest	Retrieve the completed record supporting each affected determination. Verify all required fields and links, and ensure failed controls, exceptions, and limitations remain visible. Check any full-conformance claim independently against the applicable results.

CORE-019: Conformance Record Is Structured

Prerequisites	Recorded result required: CORE-018.
Specification requirement	Each Conformance 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.
Why this control exists	A Conformance Record must be actionable evidence, not merely a presentation artifact.
When this applies	Whenever a Conformance Record is created, queried, exported, exchanged, or relied upon by an authorized downstream process or reviewer.
Evidence to inspect	Structured Conformance Record, exportable control result object, metadata record, API response, table record, graph record, JSON/XML/YAML document, or equivalent structured evidence.
Evidence sufficiency	Every required Conformance Record field under Section 9 is available as structured data to an authorized process or reviewer. **Insufficient:** A partial structured export or free-form explanation does not satisfy the requirement when any required scope, version, profile, result, evidence, Gate, authority, timing, rule, validity, constraint, review, or reconstruction field is missing.
Assessment procedure	1. Query or export the Conformance Record through an authorized mechanism. 2. Compare all fields with Section 9 and the applicable control requirements. 3. Verify required values and stable references remain structured and retrievable; do not treat a partial field list as the complete payload.
Control-result determination	**Pass:** The record contains every required Conformance Record field under Section 9. An authorized process or reviewer can consume, query, export, or exchange those fields as structured data. **Fail:** The DACS conformance determination exists only as unstructured narrative, slide content, email approval, or undocumented assertion.
Common failure modes	• The DACS conformance determination exists only as narrative, email, or slide content. • Structured record omits stable control IDs. • Exports flatten evidence links into prose. • Downstream systems cannot query result or readiness state.

Remediation procedure	**Pattern reference:** R-01 - Missing evidence **If the DACS conformance determination exists only as narrative, email, slide content, or another unstructured artifact:** create a structured Conformance Record with stable fields for the required DACS elements **If the structured record omits stable control identifiers:** add the applicable DACS control IDs and their results **If an export converts evidence references into prose that cannot be followed:** preserve structured evidence references or stable links in the exported record **If authorized downstream users or processes cannot query the result or readiness state:** make the required fields machine-readable or exportable without relying on narrative interpretation
Repeatable fix	A defined schema, table, record type, or export format is used consistently and can be queried or exchanged.
Controlled disposition	***Disposition reference:*** **D-01, Missing prerequisite.** Use this reference when the Conformance Record exists only as unstructured narrative and cannot support structured review or exchange.
Example	The Conformance Record is stored as structured records and exportable as JSON for authorized review.
Non-example	Approval exists only as an email paragraph and cannot be queried by control or decision scope.
Authority and execution	**Authority:** Evidence or platform owners maintain the structured record. The accountable record owner ensures that the required DACS fields remain available to authorized consumers. **Execution:** The Conformance Record must be queryable or exportable as structured data with stable control, result, evidence, readiness-state, timestamp, and responsible-authority or approved-rule fields.
Retest	Query or export every required Conformance Record field under Section 9. Confirm authorized consumers can retrieve structured values and references without interpreting free-form narrative.

CORE-020: Evidence and Record Integrity Is Verifiable

Prerequisites	Recorded result required: CORE-005, CORE-013, CORE-014, CORE-018, CORE-019.
Specification requirement	Material evidence, Gate Records, Conformance Records, execution traces, and control-result records shall preserve verifiable integrity appropriate to the stated decision scope.
Why this control exists	Reconstruction is not defensible when the organization cannot establish that the evidence and records being reviewed are the records that existed when the decision was made.
When this applies	When material evidence or DACS records are stored, transferred, reviewed, or relied upon.
Evidence to inspect	Integrity mechanism reference, hash/signature/immutable-log/WORM/ledger or equivalent evidence, record identifier and version, authority/custodian, effective period, and integrity-verification result.
Evidence sufficiency	An implementation-neutral integrity mechanism must detect unauthorized alteration/substitution.
Assessment procedure	1. Select material records. 2. Verify hash/signature/immutable log/WORM/ledger or equivalent evidence. 3. Attempt or inspect change detection. 4. Verify authority and effective period.
Control-result determination	**Pass:** Each required material record has a verifiable integrity mechanism that can detect unauthorized alteration or substitution and the integrity evidence is itself attributable and retrievable for the applicable effective period. **Fail:** A material record can be altered without detection, the integrity evidence is missing or unverifiable, or a substituted record cannot be distinguished from the record originally used.
Common failure modes	• Mutable spreadsheet with no revision integrity. • Hash exists but is stored with the file and can be changed silently. • Gate Record altered without audit evidence.

Remediation procedure	**Pattern references:** R-14, R-18 Add a verifiable integrity mechanism appropriate to the recorded scope and preserve its verification evidence. Recover original integrity only from verifiable contemporaneous support. If original integrity cannot be established, retain the historical failure or limitation; a new protected record and evaluation do not prove the old record was unchanged.
Repeatable fix	Material DACS records use a standard integrity-control pattern.
Controlled disposition	Disposition reference: D-01, Missing prerequisite.
Example	Gate Records are stored in an immutable audit log with signed record digests.
Non-example	A JSON export can be edited and replaced without any detectable change.
Authority and execution	Authority: Evidence custodian operates the integrity mechanism; decision-scope authority determines required protection.
Retest	Verify the integrity mechanism against representative records and confirm alteration is detectable.

© 2026 DataVaultAlliance Holdings LLC. All rights reserved.

CORE-021: Rule and Threshold Changes Are Prospective and Versioned

Prerequisites	Pass required: CORE-012. Recorded result required: CORE-002.
Specification requirement	Materiality Rules, Applicability Rules, Equivalence Rules, Multi-Value Rules, vector criteria, thresholds, authority rules, and other decision-scope predicates shall be versioned and effective before the dependent evaluation whose result they govern.
Why this control exists	DACS does not permit moving the decision boundary or threshold after observing evidence in order to manufacture a Pass.
When this applies	Whenever a materiality, applicability, threshold, equivalence, vector, or authority rule governs an evaluation.
Evidence to inspect	Versioned rule/threshold record, authority reference, effective period, change record, prior version reference, dependent evaluation timestamp, and replacement-evaluation reference where applicable.
Evidence sufficiency	Rule version/effective time must precede the dependent evaluation.
Assessment procedure	1. Compare rule effective time to evaluation time. 2. Inspect change history. 3. Confirm later rule changes created new evaluations and did not rewrite prior results.
Control-result determination	**Pass:** Each governing rule or threshold has a version, authority, effective period, and change record showing that it was established before the dependent evaluation; any later change creates a new evaluation version and does not retroactively alter the prior result. **Fail:** A rule or threshold is changed after observing the result and applied retroactively, an effective period cannot be established, or the prior rule version is overwritten.
Common failure modes	• Threshold lowered after a failure. • Prior rule version overwritten. • New applicability rule applied retroactively.
Remediation procedure	Restore prior rule history, create governed prospective versions, and retest under the valid rule. Do not re-label the prior result.
Repeatable fix	Rule-management process enforces effective dating and immutable version history.
Controlled disposition	Disposition reference: D-06, Determinacy or repeatability.

Example	Confidence threshold v3 became effective Monday; Friday's failed v2 evaluation remains failed and a new v3 evaluation is linked.
Non-example	The reviewer changes the threshold in the same record after seeing the score.
Authority and execution	Authority: Rule owner approves prospective changes; evaluator verifies effective dating.
Retest	Replay the audit trail and confirm each result used the rule effective before that evaluation.

CORE-022: Evaluation and Remediation History Is Append-Only

Prerequisites	Recorded result required: CORE-014, CORE-018, CORE-020, CORE-021.
Specification requirement	Control evaluations, Gate Records, Conformance Records, failures, exceptions, remediation actions, and retests shall preserve append-only historical lineage; later results shall not overwrite prior results.
Why this control exists	A corrected state does not erase the historical state on which earlier decisions were made.
When this applies	Whenever a control is retested, remediated, replaced, or re-evaluated.
Evidence to inspect	Evaluation history, prior-result references, remediation/change records, retest records, version links, timestamps, authority, and retention/deletion evidence where applicable.
Evidence sufficiency	Each new evaluation must append and link rather than overwrite.
Assessment procedure	1. Select a remediated control. 2. Retrieve original result and all retests. 3. Verify version links, timestamps, remediation cause, and Gate/Conformance transitions.
Control-result determination	**Pass:** Each retest or replacement evaluation creates a new versioned event linked to the prior result, preserves the prior Pass/Fail/Not Applicable result and Gate state, and records the remediation or change that caused reassessment. **Fail:** A prior failure or Gate state is overwritten, deleted without lawful authority, or replaced without a traceable version link.
Common failure modes	• Failed result deleted after fix. • New Gate state overwrites old state. • Retest has no link to remediation.
Remediation procedure	Restore append-only history from verifiable evidence where possible and change the workflow so every retest creates a linked event.
Repeatable fix	Evaluation service/workflow uses immutable event history or versioned records.
Controlled disposition	Disposition reference: D-04, Change or reassessment.
Example	CORE-007 fails, remediation R-44 is recorded, then a new CORE-007 evaluation passes and links to the failed result.
Non-example	The same spreadsheet cell is changed from Fail to Pass with no history.
Authority and execution	Authority: Record owner preserves history; assessors create new evaluation events.
Retest	Trace a sample from initial result through remediation and retest without losing any prior state.

CORE-023: Material Semantic Binding Change Triggers Forward Reassessment

Prerequisites	Pass required: CORE-021, CORE-022.
Specification requirement	Each decision path relied on for stated use shall define change-detection rules for material physical, logical, conceptual, Semantic Contract, taxonomy, ontology, identity, context, model, policy, or authority changes that could affect future readiness or conformance. Historical Gate and Conformance Records shall remain immutable evidence of what was evaluated under the versions effective at that time.
Why this control exists	Change should govern active and prospective reliance without rewriting history or forcing unnecessary retroactive execution of completed historical decisions.
When this applies	When physical, logical, conceptual, semantic, taxonomy, ontology, identity, or context bindings can materially change after a prior readiness or conformance determination.
Evidence to inspect	Version/change event, impact rule, affected-scope record, readiness-cache invalidation or suspension evidence, reassessment/new Gate or Conformance Record where required, and immutable prior record references.
Evidence sufficiency	The change-control evidence must show which semantic-binding changes are considered material, how affected decision scopes are identified, and how those changes trigger impact review, Gate reassessment, readiness-state update, or conformance-status update. ***Insufficient:*** A change log is not sufficient when a material change can be recorded without identifying affected decision scopes previously allowed for stated use or triggering the required reassessment and status update.
Assessment procedure	1. Inspect detection rules for material physical, logical, conceptual, contract, taxonomy, ontology, identity, context, model, policy, and authority changes. 2. Inspect or test a qualifying change and trace affected active or prospective scopes. 3. Verify required readiness invalidation or suspension and reassessment before future reliance. 4. Confirm historical records remain unchanged and new determinations link to prior evidence.

Control-result determination	**Pass:** Qualifying changes identify affected active or prospective decision scopes, invalidate or suspend cached readiness for new reliance as defined, and trigger impact review, Gate reassessment, readiness-state update, or Conformance Record replacement before future material use; historical records remain unchanged and linked to the new assessment when reused. **Fail:** A material change can affect future reliance without detection/reassessment, historical results are retroactively rewritten, or historical evidence is reused for a new decision without evaluation under current applicable rules.
Common failure modes	• Mappings change without impact detection. • Version changes are logged but do not trigger Gate reassessment. • Changes in identity or context are outside the monitoring rule. • Readiness for new reliance is not reassessed after a material binding change.
Remediation procedure	Version the changed artifact, identify only affected active/prospective scopes, invalidate readiness for new reliance where required, and reassess before future use. Do not retroactively rewrite historical Gate/Conformance Records.
Repeatable fix	Version/change events invoke a repeatable impact-assessment rule that identifies affected scopes and required reassessment.
Controlled disposition	***Disposition reference:*** **D-04, Change or reassessment.** Use this reference after a material semantic-binding change until affected decision scopes have been identified and reassessed.
Example	A taxonomy grain change automatically opens reassessment for all decision scopes previously allowed for stated use that reference that node.
Non-example	A source field is repurposed, but dashboards previously allowed for stated use continue with no review.
Authority and execution	**Authority:** Owners of affected semantic, identity, taxonomy, ontology, source, and context bindings participate in impact review under the decision-scope authority. **Execution:** Change detection must identify affected decision scopes and invoke the defined reassessment path when a material binding changes.
Retest	Inspect or trigger a representative qualifying change. Confirm affected active or prospective scopes are identified, cached readiness is invalidated or suspended as defined, required reassessment precedes new reliance, and historical records remain unchanged.

CORE-024: Lawful Evidence Preservation and Deletion Are Governed

Prerequisites	Recorded result required: CORE-013, CORE-020, CORE-022.
Specification requirement	When law, regulation, contract, privacy policy, or authorized retention rule requires evidence minimization or deletion, DACS evidence preservation shall comply while retaining the strongest lawful reconstruction anchor available.
Why this control exists	DACS must preserve accountability without requiring organizations to violate privacy, GDPR, retention, contractual, or other lawful deletion obligations.
When this applies	When material evidence is subject to lawful minimization, deletion, retention, or contractual destruction requirements.
Evidence to inspect	Retention/deletion rule, legal or policy authority, affected evidence identifier/version, deletion/minimization record, lawful reconstruction anchor where retention is permitted, integrity/provenance metadata where permitted, timestamp, and the resulting reconstruction limitation where applicable. If no lawful anchor may remain, record that limitation.
Evidence sufficiency	Evidence establishes the applicable deletion or minimization authority, action, affected evidence identity and time, and the strongest reconstruction anchor that may lawfully remain. If no anchor may remain, the limitation and constrained reconstruction claim are recorded. **Insufficient:** An anchor is not sufficient if retaining it violates the applicable rule. Unrecorded deletion or a claim of full reconstruction without lawful supporting evidence also fails the test.
Assessment procedure	1. Identify required deletion/minimization. 2. Verify authority and timing. 3. Inspect Lawful Reconstruction Anchor. 4. Verify reconstructability claims are constrained if the law forbids retaining enough evidence.

Control-result determination	**Pass:** Required deletion or minimization is authorized and recorded, the affected evidence is handled according to the applicable rule, and a lawful reconstruction anchor preserves the evidence identity, provenance, version/effective period, integrity reference where permitted, deletion authority, deletion time, and the metadata needed to establish what evidence existed and why it is no longer retained. If no lawful reconstruction anchor may be retained, that limitation shall be explicitly recorded and affected reconstructability claims shall be constrained accordingly. **Fail:** Unlawful retention, undocumented deletion, deletion without authority, substitution of current evidence for deleted historical evidence, or a claim of full historical reconstructability when required evidence and all lawful anchors are unavailable.
Common failure modes	• Raw personal data retained beyond lawful period “for DACS.” • Evidence deleted with no record of what existed. • Current evidence substituted for deleted historical evidence.
Remediation procedure	Follow the lawful retention/deletion rule, create the strongest permitted reconstruction anchor, record the resulting limitation, and revise any overstated reconstructability claim.
Repeatable fix	Retention workflows integrate DACS reconstruction metadata with privacy/legal deletion controls.
Controlled disposition	Disposition reference: D-04, Change or reassessment.
Example	A governed deletion removes raw customer data and retains only the provenance, evidence identity, version, integrity reference, authority, and timing permitted by the applicable rule. If no anchor may remain, that limitation constrains the reconstruction claim.
Non-example	Data is either retained unlawfully or deleted without any governed record.
Authority and execution	Authority: Privacy/legal/records authority governs deletion; DACS evidence owner preserves only what is lawful.
Retest	Verify deletion compliance and confirm the surviving anchor supports only the reconstructability claim actually made.

CORE-025: Decision Path Is Reconstructable

Prerequisites	Pass required: CORE-013, CORE-018, CORE-020, CORE-022. Recorded result required: CORE-010, CORE-024.
Specification requirement	Each analytic output, AI-assisted recommendation, automated action, human decision, or decision path relied on for stated use shall be linked to a reconstructable decision path using preserved governed evidence. Human-operated paths may satisfy this requirement through a Human Decision Record. Reconstructability does not require reproduction of an unavailable historical proprietary AI model.
Why this control exists	Defensibility requires evidence of what actually supported the decision at the time. Reproduction is desirable when possible, but unavailable proprietary historical models must not be falsely recreated with newer models.
When this applies	Whenever a material analytic, AI-assisted, automated, or human decision path is relied on for stated use or later challenged/reviewed.
Evidence to inspect	Decision-path record, Human Decision Record where applicable, identity/taxonomy/ontology/context/version references, causal-order evidence where applicable, Gate Records, output/action/decision record, authority, exception record where applicable, AI execution evidence/model identity where applicable, and explicit reproducibility limitation where the original model is unavailable.
Evidence sufficiency	The path must be explainable from recorded evidence, not undocumented memory. Human steps may use a Human Decision Record. If an original proprietary AI model is unavailable, contemporaneous execution evidence may establish reconstruction but the record must explicitly distinguish non-reproducibility.
Assessment procedure	1. Select a material decision. 2. Traverse identities, meanings, relationships, artifact versions, context, causal order, Gates, authority, evidence, exceptions, and output/action. 3. For human steps inspect Human Decision Records. 4. For AI steps verify model/provider/version and contemporaneous trace; if the model is unavailable, verify the non-reproducibility limitation is explicit. 5. Confirm no newer model is being used as proof of the historical result.

Control-result determination	**Pass:** An authorized reviewer can retrieve the material identities, classifications, applicable relationships, context and artifact versions, applicable causal order, Gate Records and readiness states, evidence references, output/action/decision state, exceptions, and authority that existed at the time of use. Reconstruction shall use preserved evidence rather than undocumented memory. For a material human step, the Human Decision Record preserves the actor or role, authority, material inputs and evidence, applicable rule or criterion, decision or action, timestamp/effective period, material override or exception, and Gate reference. If the historical AI model is unavailable, contemporaneous model/provider/version identity, inputs and context, material parameters where available, tool/API use, output, and execution trace shall establish what occurred. Record the reproduction limitation. A result from a newer model is comparison evidence and shall not be represented as reproduction of the historical execution. **Fail:** Reconstruction depends on undocumented human memory, required contemporaneous AI execution evidence is unavailable, a newer model is substituted as proof of the historical model result, or causal/artifact-version evidence cannot establish the state used at the time.
Common failure modes	• Reconstruction depends on analyst memory. • Historical taxonomy/model/version is unknown. • A newer AI model is rerun and presented as reproduction. • Human approval has no recorded basis or authority.
Remediation procedure	Preserve or restore verifiable historical references, create Human Decision Records for future manual steps, strengthen execution traces, and record non-reproducibility when the original model is unavailable. If the historical basis cannot be established, do not claim reconstructability.
Repeatable fix	Decision outputs retain stable links to versioned evidence, Gates, Human Decision Records where applicable, execution traces, and explicit reproducibility status.
Controlled disposition	Disposition reference: D-01, Missing prerequisite. Do not claim the path is reconstructable while a required material element remains unprovable.
Example	An auditor can establish the exact evidence, taxonomy/ontology versions, authority, Gate state, human override, model/provider/version and output used at the time, even though the retired proprietary model itself cannot be rerun.

Non-example	The team reruns the same prompt against a newer model and treats a different output as proof of the original decision.
Authority and execution	Authority: Decision-scope owner is accountable; evidence/model/process owners preserve the records they control. Reconstruction and reproduction are explicitly distinguished.
Retest	Repeat the historical reconstruction from records only. Confirm required elements are retrievable and any unavailable-model limitation is accurately stated.

8. Extended Taxonomy Controls

These cards apply when governed meaning, classification, labels, identifiers, semantic grain, or physical semantic anchoring materially affect the decision path.

Card boundary

The Specification requirement, Prerequisites, Evidence to inspect, and Pass/Fail text below reproduce DACS Specification v1.13. Sections 2 through 5 explain its global assessment and closure rules. Procedures, failure modes, remediation, and examples are informative guidance. Apply the exact Specification version governing the assessment; the catalog does not add criteria or override it.

ET-001: Taxonomy Scope and Purpose Are Declared

Prerequisites	Pass required: CORE-004.
Specification requirement	Each Extended Taxonomy evaluation shall declare the taxonomy scope and purpose for the stated decision scope.
Why this control exists	Classification cannot be tested if its scope and purpose are not declared.
When this applies	When an Extended Taxonomy is used for the decision scope and the boundary or purpose of that taxonomy must be explicit.
Evidence to inspect	Taxonomy scope record, purpose statement, owner, version, applicable decision-scope mapping, and excluded meanings.
Evidence sufficiency	The taxonomy-scope evidence must define what the Extended Taxonomy covers for this decision scope, why it is being used, who owns it, which version applies, and which meanings are explicitly outside the declared boundary. ***Insufficient:*** An enterprise-wide glossary or taxonomy reference is not sufficient when the decision-specific purpose, boundary, excluded meanings, owner, or applicable version cannot be determined.
Assessment procedure	**1.** Inspect the taxonomy scope record and verify purpose, owner, version, applicable decision scope, and excluded meanings are explicit. **2.** Confirm the declared taxonomy boundary is adequate for the material concepts in the scope.
Control-result determination	**Pass:** The record identifies the taxonomy scope, purpose, owner, version, applicable decision scope, and excluded meanings. **Fail:** Taxonomy scope or purpose is missing, ambiguous, or not linked to the decision scope.
Common failure modes	• Taxonomy scope is enterprise-wide but the decision use is unclear. • Excluded meanings are not stated. • Purpose is generic documentation rather than the decision scope. • Owner or version is missing.

Remediation procedure	**Pattern references:** R-02 - Ambiguous meaning; R-04 - Missing authority; R-01 - Missing evidence **If the taxonomy is enterprise-wide but its decision use is unclear:** define the taxonomy boundary that is relevant to the stated decision scope **If excluded meanings are not stated:** record the meanings, classifications, or domains that are outside the taxonomy scope for this use **If the stated purpose is generic documentation rather than the decision use:** state why the taxonomy is needed for this decision scope **If the owner or applicable version is missing:** record the accountable taxonomy owner and the version used by the decision scope
Repeatable fix	Taxonomy scope records use a standard scope-and-purpose template tied to the decision scope and version.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when the taxonomy scope or purpose is not yet sufficiently defined for the decision scope.
Example	The taxonomy covers subscription-customer status terms for internal operating review and explicitly excludes regulatory classifications.
Non-example	A company-wide glossary is cited without identifying which part or purpose governs the decision scope.
Authority and execution	**Authority:** Taxonomy owner defines scope and purpose for the decision use.
Retest	Reinspect the taxonomy-scope record. Confirm that scope, purpose, owner, version, decision-scope applicability, and excluded meanings are explicit and consistent.

ET-002: Ownership and Stewardship Are Recorded

Prerequisites	Pass required: ET-001.
Specification requirement	Each material taxonomy node shall record business ownership or stewardship authority.
Why this control exists	Accountability requires a recorded authority.
When this applies	When a material taxonomy node requires accountable business ownership, stewardship, approval, change authority, or dispute resolution.
Evidence to inspect	Owner or steward record, authority scope, approval responsibility, and review condition.
Evidence sufficiency	The ownership evidence must identify the accountable owner or steward for each material taxonomy node and define that role's authority for approval, change, dispute resolution, and review. ***Insufficient:*** A team name, technical custodian, system owner, or contact person is not sufficient when that party has not been given the business authority needed to approve or resolve the governed meaning.
Assessment procedure	**1.** Inspect each material taxonomy node for a named owner or steward, authority scope, approval responsibility, and review condition. **2.** Verify the named authority can resolve meaning, change, and dispute decisions.
Control-result determination	**Pass:** Owner or steward, authority scope, approval responsibility, and review condition are recorded. **Fail:** A material concept or classification lacks authority for approval, change, or dispute resolution.
Common failure modes	• Technical owner is assumed to have business authority. • Ownership is listed but authority scope is missing. • No one is empowered to resolve disputes. • Review condition is absent after organizational change.

Remediation procedure	**Pattern reference:** R-04 - Missing authority **If a technical owner is being treated as the business authority:** assign the business owner or steward who has authority over meaning and use **If an owner is named but the authority scope is missing:** record the decisions that the owner or steward is permitted to make **If no one is empowered to resolve disputes:** assign a dispute-resolution authority or escalation path **If organizational change made the ownership record outdated:** review and update the owner, authority scope, and review condition
Repeatable fix	Governed nodes require an accountable role and authority source before approval or change.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material taxonomy node lacks the business ownership or stewardship authority required to govern it.
Example	Finance owns Revenue Recognition Status; the steward may approve labels but not policy meaning.
Non-example	A taxonomy term is “owned by the data team” with no named business authority or dispute process.
Authority and execution	**Authority:** Business governance authority assigns ownership or stewardship and its decision rights.
Retest	Reinspect each affected taxonomy node. Confirm that a business owner or steward with the required authority scope, approval responsibility, dispute authority, and review condition is recorded.

ET-003: Taxonomy Node Type Is Declared

Prerequisites	Pass required: ET-002.
Specification requirement	Each material taxonomy node shall declare its node type.
Why this control exists	Node type controls how the node may be interpreted and used.
When this applies	When a material taxonomy node is used and its node type affects how the node may be interpreted, governed, or applied.
Evidence to inspect	Taxonomy node record, node type list, approval record.
Evidence sufficiency	The taxonomy-node evidence must assign every material node an approved node type and make the type explicit enough to govern how the node may be interpreted and used. ***Insufficient:*** A naming convention, folder location, visual shape, or reader assumption is not sufficient to establish whether a node is a concept, category, classification, alias, code set, identifier concept, deprecated term, or another approved type.
Assessment procedure	**1.** Inspect every material taxonomy node used by the scope, or an approved complete extract. **2.** Verify each has an approved node type and that the type governs how the node may be interpreted.
Control-result determination	**Pass:** Each node is identified as concept, category, domain, subdomain, classification, label, alias, deprecated term, code set, identifier concept, or other approved node type. **Fail:** A material node lacks a declared type or uses an unapproved type.
Common failure modes	• Node type is inferred from naming convention. • Aliases and concepts are stored as the same type. • Local custom types have no approval. • Node type changed without review of downstream use.

Remediation procedure	**Pattern references:** R-02 - Ambiguous meaning; R-01 - Missing evidence **If node type is inferred from naming convention:** assign an approved node type explicitly **If aliases, concepts, categories, or other node classes are stored as though they are the same type:** reclassify the affected nodes using the approved node-type model **If a locally invented node type has no approval:** map it to an approved type or obtain taxonomy-authority approval before governed use **If a node type changed without reviewing downstream use:** identify affected decision scopes and reassess the uses that depend on the prior type
Repeatable fix	The taxonomy service or stewardship process enforces an approved node-type list and records changes.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material taxonomy node lacks an approved node type.
Example	“Active Customer” is typed as a classification and “Customer” as a concept.
Non-example	Nodes are stored as unlabeled terms, so a category and an identifier concept are indistinguishable.
Authority and execution	**Authority:** Taxonomy steward or governing semantic authority approves node types.
Retest	Reinspect each affected material taxonomy node. Confirm that every node now has an approved node type that is explicit and governs interpretation and use.

ET-004: Business Meaning Is Recorded

Prerequisites	Pass required: ET-003.
Specification requirement	Each material taxonomy node shall have recorded business meaning.
Why this control exists	Labels alone do not establish governed business meaning or readiness for decision use.
When this applies	When a material taxonomy node contributes business meaning to the decision path.
Evidence to inspect	Definition record, semantic boundary, owner/steward approval, version, decision-scope mapping.
Evidence sufficiency	The business-meaning evidence must provide an approved definition, semantic boundary, accountable owner, applicable version, and decision-scope applicability for each material taxonomy node. ***Insufficient:*** A technical expression, circular definition, local shorthand, label alone, or undocumented team understanding is not sufficient when it does not establish the approved business meaning and boundary for the decision scope.
Assessment procedure	**1.** Inspect each material taxonomy node. **2.** Verify approved definition, semantic boundary, owner, version, and decision-scope applicability are recorded and that the definition is business-meaningful rather than only technical or local.
Control-result determination	**Pass:** The record includes approved definition, semantic boundary, owner, version, and decision-scope applicability. **Fail:** Meaning is missing, ambiguous, only technical, only local, or not approved for the decision scope.
Common failure modes	• Definition is technical or circular. • Business boundary is absent. • Local meaning is mistaken for enterprise-approved meaning. • Definition has no accountable owner or effective version.

Remediation procedure	**Pattern references:** R-02 - Ambiguous meaning; R-04 - Missing authority **If the definition is technical, circular, or otherwise fails to express business meaning:** replace it with an approved business definition that states what the concept means **If the business boundary is missing:** record the relevant inclusions, exclusions, or boundary conditions **If a local meaning is being treated as the approved business meaning:** resolve the meaning with the accountable semantic authority and record the approved version **If the definition has no accountable owner or effective version:** assign the owner and record the applicable version or effective period
Repeatable fix	Material nodes cannot reach ready-for-use status without governed meaning and versioned ownership.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when the approved business meaning or semantic boundary of a material taxonomy node is unresolved.
Example	Active Customer defines included and excluded account conditions and names Customer Operations as owner.
Non-example	The only definition is a SQL expression with no approved business meaning.
Authority and execution	**Authority:** Business concept owner or steward approves meaning and boundary.
Retest	Reinspect each affected material taxonomy node. Confirm that approved business meaning, semantic boundary, owner, version, and decision-scope applicability are now recorded.

ET-005: Controlled Label and Language Evidence Are Recorded

Prerequisites	Pass required: ET-004.
Specification requirement	Each material concept or classification shall record authoritative labels and non-authoritative variants.
Why this control exists	Controlled language reduces semantic ambiguity across systems and decision paths.
When this applies	When labels, aliases, synonyms, deprecated terms, local variants, or prohibited terms can affect interpretation of a material concept or classification.
Evidence to inspect	Preferred-label record; permitted synonyms, aliases, deprecated terms, and local variants, including explicit no-entry statements where appropriate; prohibited labels where applicable; and approval record.
Evidence sufficiency	The record distinguishes the preferred label from permitted synonyms, aliases, deprecated terms, and local variants. Empty required categories are recorded explicitly. Prohibited labels are recorded where applicable. **Insufficient:** A word list without authority, variant status, or an explanation for empty required categories does not establish governed language.
Assessment procedure	1. Inspect the controlled-language record for every material concept or classification. 2. Verify preferred label, permitted synonyms, aliases, deprecated terms, and local variants. Where a required category is empty, verify an explicit no-entry statement. 3. Verify prohibited labels where applicable and trace approval and concept mapping.
Control-result determination	**Pass:** The record identifies the preferred label and records permitted synonyms, aliases, deprecated terms, and local variants. Record prohibited labels where applicable. If a required category has no entries, record that fact rather than inventing a label or leaving an unexplained gap. **Fail:** The decision path depends on labels that are unapproved, ambiguous, deprecated, or not linked to an approved concept.
Common failure modes	• Synonyms are treated as exact equivalents without approval. • Deprecated labels remain active. • Local variants are undocumented. • Prohibited labels are known socially but not recorded.

Remediation procedure	**Pattern reference:** R-02 - Ambiguous meaning **If synonyms or aliases are treated as exact equivalents without approval:** classify the preferred label, permitted synonyms, aliases, and local variants under the approved concept **If deprecated labels remain active in material use:** mark them as deprecated and prevent them from being treated as current approved language **If local variants are undocumented:** record the local variants and their governed mapping to the approved concept **If prohibited labels are known only through informal practice:** record the prohibited labels and the rule that prevents their approved use
Repeatable fix	A controlled-label register is versioned and checked when terms enter a material decision path.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when material labels or language variants are not yet governed well enough for the decision scope.
Example	“Acct” is recorded as a permitted local alias for Account; an obsolete label is marked deprecated.
Non-example	Two teams use “active” for different meanings and both labels are accepted without distinction.
Authority and execution	**Authority:** Terminology or taxonomy authority approves preferred, permitted, deprecated, and prohibited labels.
Retest	Reinspect each required label category and its approval. Confirm authoritative and non-authoritative variants are distinguished, empty required categories are recorded, and prohibited labels are identified where applicable.

ET-006: Semantic Domain and Boundary Are Declared

Prerequisites	Pass required: ET-004.
Specification requirement	Each material concept or classification shall declare its semantic domain and boundary.
Why this control exists	The enterprise must know where one meaning ends and another begins.
When this applies	When a material concept or classification can be confused with adjacent, overlapping, broader, narrower, or excluded meanings.
Evidence to inspect	Semantic domain, included and excluded meanings, boundary rules, and material overlap/disjointness rules with decision-scope mapping.
Evidence sufficiency	The semantic-boundary evidence must state the domain of the concept or classification, what meanings are included, what meanings are excluded, and any material overlap or disjointness rules that affect decision use. ***Insufficient:*** A definition is not sufficient when a reviewer cannot determine where the concept stops, what nearby meanings are excluded, or how overlapping concepts are handled for the stated decision scope.
Assessment procedure	**1.** Inspect domain and boundary rules for each material concept or classification. **2.** Verify included meanings, excluded meanings, and overlap or disjointness rules are explicit where they affect decision use.
Control-result determination	**Pass:** The record states domain, boundary rules, included meanings, excluded meanings, and overlap/disjointness rules where material. **Fail:** Domain or boundary is missing where the distinction affects decision use.
Common failure modes	• Included and excluded meanings overlap. • Two concepts share a label but differ in domain. • Disjointness assumptions are undocumented. • Boundary rules exist but do not cover the decision use.

Remediation procedure	**Pattern references:** R-02 - Ambiguous meaning; R-05 - Conflicting evidence **If included and excluded meanings overlap without a rule:** define the boundary and the approved overlap or disjointness rule **If two concepts share a label but belong to different semantic domains:** separate or qualify the concepts so their domain-specific meanings cannot be confused **If disjointness or overlap is assumed but not recorded:** document the applicable relationship between the semantic domains **If existing boundary rules do not cover the stated decision use:** extend the boundary rule or narrow the decision use until the semantic boundary is explicit
Repeatable fix	Boundary criteria are recorded as reusable rules tied to the concept and decision scope.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material semantic domain or boundary is missing or unresolved.
Example	Customer Account excludes prospects and defines how reseller-held accounts are treated.
Non-example	A term is defined broadly enough that customer, prospect, and billing contact can all qualify depending on the user.
Authority and execution	**Authority:** Semantic domain owner or steward approves boundary, inclusion, exclusion, and overlap rules.
Retest	Reinspect the semantic-domain and boundary rules. Confirm that included meanings, excluded meanings, and material overlap or disjointness rules are now explicit for the decision scope.

ET-007: Semantic Grain Is Declared Where Material

Prerequisites	Pass required: ET-006.
Specification requirement	Each material concept, identifier, classification, count, integration point, aggregation, or transformation shall declare semantic grain at each point in the decision path where grain affects interpretation or use. Each material transition between grains shall declare the source grain, transformation or aggregation rule, and resulting grain.
Why this control exists	Same names do not guarantee the same grain or meaning. A decision path may legitimately use multiple grains, but every material grain and transition must be explicit and reconstructable.
When this applies	When grain affects how a material concept, identifier, classification, count, or integration point is compared, counted, joined, or interpreted.
Evidence to inspect	Semantic grain records by point of use, decision-scope mapping, source-grain and resulting-grain records, transformation or aggregation rule for each material grain transition, and Equivalence Rule where distinct grains are treated as comparable.
Evidence sufficiency	Grain is recorded wherever it affects interpretation or use. Every material transition identifies the source grain, governing transformation or aggregation rule, and resulting grain. An approved Equivalence Rule supports any treatment of distinct grains as comparable. **Insufficient:** Naming a source grain or recording equivalence alone does not explain an implicit material grain transition.
Assessment procedure	1. Trace each material concept, identifier, classification, count, integration point, aggregation, or transformation through its points of use. 2. Verify the grain at each relevant point. 3. Inspect source grain, governing transformation or aggregation rule, and resulting grain for every material transition. 4. Test any cross-grain comparability against the recorded Equivalence Rule.
Control-result determination	**Pass:** The record states the business level at which each material concept, identifier, classification, or count is unique, meaningful, counted, integrated, aggregated, or compared at its point of use, and every material grain transition is explicitly recorded with its governing transformation or aggregation rule. **Fail:** Different grains are treated as equivalent without a declared and approved transformation or equivalence rule, a material grain transition is implicit, or the grain at a point of consumption cannot be reconstructed.

Common failure modes	• Counts at different grains are compared directly. • Identifier grain is assumed from column name. • Aggregation changes the business meaning. • Equivalence between grains is used without an approved rule.
Remediation procedure	**Pattern references:** R-03 - Unstable identity or grain; R-02 - Ambiguous meaning **If counts, concepts, or identifiers at different grains are compared directly:** align them to a common governed grain or use an approved cross-grain rule **If identifier grain is inferred from a field or column name:** declare the business grain explicitly **If aggregation changes the business meaning:** record the aggregation grain and the rule that preserves or changes meaning **If equivalence between grains is used without approval:** establish the governed equivalence rule before relying on the cross-grain comparison
Repeatable fix	Material taxonomy mappings include semantic grain and approved equivalence rules where cross-grain use is necessary.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when semantic grain is missing, incompatible, or unsupported by an approved equivalence rule.
Example	Revenue is distinguished at contract, account, and consolidated-customer grain before comparison.
Non-example	Account counts from one source are compared to household counts from another as if the measures share grain.
Authority and execution	**Authority:** Concept owner and identity or measurement authority approve semantic grain where it affects use.
Retest	Trace every affected point of use and material grain transition. Confirm explicit grain, source-to-result rules, scope mapping, and any approved cross-grain equivalence.

ET-008: Provenance Is Recorded

Prerequisites	Pass required: ET-002.
Specification requirement	Each material taxonomy assertion shall record provenance.
Why this control exists	Decision readiness depends on knowing where meaning came from and when it was valid.
When this applies	When a material semantic assertion must be traced to its source, approval, version, and effective period.
Evidence to inspect	Provenance record, responsible authority or approved rule reference, version, effective date or timestamp.
Evidence sufficiency	The provenance evidence must identify the source of each material semantic assertion, the approving authority or rule, the applicable version, the timestamp or effective period, and the decision scope to which the assertion applies. ***Insufficient:*** A definition, label, classification, identifier rule, or boundary is not sufficient when its origin, approval, version, or effective period cannot be established.
Assessment procedure	**1.** Inspect provenance for each material taxonomy assertion. **2.** Verify assertion source, approving authority or rule, version, effective date or timestamp, and decision-scope applicability can be reconstructed.
Control-result determination	**Pass:** The record identifies the source of the assertion, approving authority or approved rule reference, version, timestamp or effective period, and decision-scope applicability. **Fail:** Material meaning, label, classification, identifier, or boundary evidence lacks provenance.
Common failure modes	• Meaning is approved but the source of the assertion is unknown. • Effective date is missing. • Imported reference data loses its authority source. • Provenance is retained for data values but not semantic assertions.

Remediation procedure	**Pattern reference:** R-01 - Missing evidence **If the origin of a material semantic assertion is unknown:** record the source from which the meaning, label, classification, identifier, or boundary assertion came **If the effective date or period is missing:** record when the assertion became valid and, where applicable, when it stopped being valid **If imported reference data has lost its authority source:** preserve the external or internal authority associated with the imported assertion **If provenance is kept for data values but not for semantic assertions:** add provenance records for the semantic evidence itself
Repeatable fix	Taxonomy changes and assertions are versioned with provenance automatically or through a controlled stewardship record.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when material semantic provenance is incomplete or cannot be reconstructed.
Example	A definition shows who approved it, the source policy, version, and effective date.
Non-example	A definition exists, but its origin and approval history are unknown.
Authority and execution	**Authority:** Semantic steward preserves provenance; the approving authority or rule must be identifiable from the record.
Retest	Reconstruct provenance for each affected semantic assertion. Confirm that source, approving authority or rule, version, effective time, and decision-scope applicability are now retrievable.

ET-009: Physical Semantic Anchors Are Recorded Where Required

Prerequisites	Pass required: CORE-005, ET-007, ET-008.
Specification requirement	Each material concept or classification shall record physical semantic anchors when physical representation affects the decision scope.
Why this control exists	The Extended Taxonomy closes the gap between governed meaning and real-world data.
When this applies	When a governed concept or classification must be tied to its physical representation in source data for the decision scope.
Evidence to inspect	Source-system reference, physical attribute/object reference, data asset reference, code-set or reference-data evidence where applicable.
Evidence sufficiency	The physical-semantic-anchor evidence must identify the source systems and physical representations needed to show how each material governed concept or classification appears in the data used by the decision scope. ***Insufficient:*** A governed definition is not sufficient when the reviewer cannot locate the tables, fields, files, messages, events, APIs, documents, code sets, or equivalent source representations that implement the concept for this scope.
Assessment procedure	**1.** Trace each material concept or classification to the physical representations needed by the decision scope. **2.** Verify source systems and relevant tables, fields, files, messages, events, APIs, documents, code sets, or equivalent anchors are recorded.
Control-result determination	**Pass:** 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:** A material concept is treated as ready for decision use without required physical representation evidence.
Common failure modes	• Governed concepts have definitions but no physical anchors. • Mappings stop at dataset level when fields or codes are material. • Source changes leave anchors out of date. • Physical representations are recorded without decision-scope relevance.

Remediation procedure	**Pattern reference:** R-01 - Missing evidence **If a governed concept has no physical semantic anchor:** record the source systems and physical representations that implement the concept for the decision scope **If the mapping stops at dataset level when fields, codes, or other details are material:** extend the anchor to the physical elements needed to test the concept **If source changes have made the recorded anchors outdated:** update the anchors, record the effective version, and reassess affected scopes **If physical representations are recorded without showing why they matter to the decision scope:** remove irrelevant anchors or bind the material representations explicitly to the stated decision use
Repeatable fix	Approved concepts maintain versioned physical anchors for the sources used by each decision scope.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a governed concept or classification lacks the physical semantic anchors required by the scope.
Example	Active Status maps to Billing.Status_Code and CRM.Account_State for the stated scope.
Non-example	A concept is approved in a glossary, but no one can identify which source fields implement it.
Authority and execution	**Authority:** Semantic steward owns the concept-to-physical binding; source owners confirm physical representation.
Retest	Trace the affected governed concepts or classifications to their physical source representations again. Confirm that all material physical anchors required by the scope are now recorded and locatable.

ET-010: Source-System Representation Is Recorded Where Required

Prerequisites	Pass required: ET-009.
Specification requirement	Each material concept shall identify source-system representations required for the decision scope.
Why this control exists	A single governed concept may be represented differently across source systems.
When this applies	When the same governed concept is represented in one or more source systems that contribute to the decision path.
Evidence to inspect	Source-system mapping, local term/attribute mapping, source representation notes, decision-scope mapping.
Evidence sufficiency	The source-representation evidence must identify how the governed concept is represented in every contributing source that matters to the decision scope, including material local terms, attributes, codes, and known representation differences. ***Insufficient:*** A standardized or enterprise representation is not sufficient when local source representations that affect interpretation, transformation, or testing are missing from the governed mapping.
Assessment procedure	**1.** For each material concept, inspect source-system mappings. **2.** Verify required local terms, attributes, codes, and representation differences are recorded for every source that contributes to the decision path.
Control-result determination	**Pass:** The record identifies source systems, local terms, local attributes, local codes, and representation differences required to test the decision scope. **Fail:** The concept is treated as ready for stated use without the source-system representation needed to support the decision path.
Common failure modes	• Only the standardized representation is recorded. • Local codes or terms that drive transformation are omitted. • Source-system differences are normalized without preserving evidence. • New source representations enter the path without mapping.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-08 - Material change or drift **If only the standardized representation is recorded:** add the source-system representations that materially contribute to the decision path **If local codes or terms that drive transformation are omitted:** record those local values and their mapping to the governed concept **If normalization removes evidence of source-system differences:** preserve the source mapping or provenance needed to reconstruct the original representation **If a new source representation entered the path without mapping:** map and govern the representation before stated use or keep it Quarantined
Repeatable fix	Source onboarding and change processes maintain concept-to-source mappings as versioned evidence.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material source-system representation is missing from the governed concept mapping.
Example	The concept record shows how Active Status is represented differently in CRM and Billing and which codes map to the governed meaning.
Non-example	A concept is assumed to be implemented identically in every source because the field names look similar.
Authority and execution	**Authority:** Semantic steward owns the governed mapping; source-system owner confirms local terms, codes, and representations.
Retest	Recheck every contributing source representation for the affected concept. Confirm that material local terms, attributes, codes, and representation differences are now recorded.

ET-011: Business Identifier or Key Evidence Is Recorded Where Applicable

Prerequisites	Pass required: ET-007, ET-008.
Specification 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.
Why this control exists	Business keys often differ by system even when they appear semantically similar.
When this applies	When identifiers or keys represent a material governed concept and equivalence, meaning, grain, or resolution matters to the decision path.
Evidence to inspect	Identifier record, source-key mapping, semantic grain record, material value-format exception where present, and authority or resolution rule.
Evidence sufficiency	The identifier evidence must establish the business meaning, semantic grain, source-system representation, material value-format expectations, and governing authority or resolution rule for each identifier or key used in the decision path. ***Insufficient:*** Similar column names, matching formats, or technically joinable values are not sufficient to prove that two identifiers represent the same business identity or grain.
Assessment procedure	**1.** Inspect material identifiers and keys used to represent governed concepts. **2.** Verify business meaning, semantic grain, source representation, material value-format expectations, and authority or resolution rule are recorded before equivalence is asserted.
Control-result determination	**Pass:** Each material identifier records business meaning, semantic grain, source-system representation, value-format expectation where material, and authority or resolution rule. **Fail:** Identifier fields or keys are treated as equivalent by name alone or without required evidence.
Common failure modes	• Identifiers with similar names are treated as equivalent. • Key meaning is undocumented. • Source keys represent different grains. • Format or authority changes are ignored. • No resolution rule exists for competing identifiers.

Remediation procedure	**Pattern references:** R-03 - Unstable identity or grain; R-05 - Conflicting evidence **If identifiers with similar names are being treated as equivalent:** prove equivalence through governed meaning, grain, source representation, and an approved crosswalk or resolution rule **If the business meaning of a key is undocumented:** record what business instance the identifier represents **If source keys operate at different semantic grains:** separate the identifiers by grain or establish an approved cross-grain resolution rule **If identifier format or authority changed without review:** version the change and reassess the affected identifier mapping **If competing identifiers have no resolution rule:** define the precedence, crosswalk, or identity-resolution rule and its accountable authority
Repeatable fix	Identifier mappings use governed records that distinguish local keys, business identifiers, crosswalks, and resolution authority.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when identifier meaning, grain, source representation, or resolution authority remains unresolved.
Example	Billing Customer Number and CRM Account ID are linked through an approved crosswalk at account grain.
Non-example	Two columns called customer_id are joined directly without proving they identify the same business instance.
Authority and execution	**Authority:** Identity or identifier authority approves key meaning and resolution; source owners confirm source representation.
Retest	Reinspect each affected identifier or key. Confirm that business meaning, semantic grain, source representation, material format expectations, and authority or resolution rule are now recorded before equivalence is asserted.

ET-012: Resolution or Mastering Rule Is Recorded Where Applicable

Prerequisites	Pass required: ET-011.
Specification requirement	Where multiple source representations or identifiers must be treated as the same concept or instance, the resolution or mastering rule shall be recorded.
Why this control exists	Integration requires tested equivalence, not assumed equivalence.
When this applies	When multiple source representations or identifiers are merged, mastered, counted, or treated as the same concept or business instance.
Evidence to inspect	The resolution or mastering rule used, authority record, threshold record where applicable, exception-handling rule, and exception record when an exception exists.
Evidence sufficiency	The resolution or mastering evidence must state the approved rule used to treat multiple source representations or identifiers as the same concept or instance, including authority, thresholds where applicable, scope, and exception handling. ***Insufficient:*** Similar values, analyst judgment, embedded code logic, or system precedence are not sufficient when no approved and reviewable rule explains why the representations may be merged, mastered, counted, or treated as equivalent.
Assessment procedure	**1.** Identify cases where multiple source representations or identifiers are merged, mastered, counted, or treated as equivalent. **2.** Verify an approved resolution or mastering rule, authority, threshold where applicable, exception handling, and scope applicability exist.
Control-result determination	**Pass:** The record includes approved rule, authority, threshold where applicable, exception handling, and decision-scope applicability. **Fail:** Source representations are merged, counted, mastered, or treated as equivalent without an approved rule.
Common failure modes	• Records are merged because values are similar. • Mastering precedence is embedded in code without governing authority. • Thresholds change without prospective versioning. • Unresolved cases are silently forced into a match.

Remediation procedure	**Pattern references:** R-03 - Unstable identity or grain; R-06 - Threshold or rule failure; R-11 - Human adjudication **If records are merged only because values appear similar:** define the approved resolution or mastering rule that establishes equivalence **If mastering precedence exists only inside implementation code:** record and govern the precedence rule outside the code as inspectable evidence **If thresholds change without versioning:** version the threshold and reassess uses affected by the change **If unresolved cases are forced into a match:** preserve a governed unresolved or exception outcome instead of manufacturing equivalence
Repeatable fix	A versioned mastering or resolution rule is invoked consistently, with exceptions captured as evidence.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when multiple representations are being merged, mastered, counted, or treated as equivalent without an approved resolution rule.
Example	Duplicate accounts are merged only when the approved identity rule and tie-break criteria are met.
Non-example	Analysts manually merge records case by case with no documented authority or reproducible rule.
Authority and execution	**Authority:** Mastering or identity authority approves resolution rules, thresholds, precedence, and exception handling.
Retest	Reapply the approved resolution or mastering rule to the affected cases. Confirm that the rule, authority, thresholds where applicable, exception handling, and scope applicability are recorded and produce the governed result.

ET-013: Governance Constraints, Jurisdiction, and Usage Boundaries Are Recorded

Prerequisites	Pass required: ET-004.
Specification requirement	Each governed taxonomy scope shall record applicable usage boundaries, policy constraints, and jurisdictional authorities. When two applicable authoritative constraints conflict, a recorded precedence or adjudication rule shall resolve the conflict before material use.
Why this control exists	Conflicting authority cannot be converted into permission by assessor judgment. An unresolved legal or policy conflict is a control failure and normally requires a Stop Gate state.
When this applies	When permitted, prohibited, constrained, policy, privacy, security, purpose, or other usage boundaries affect a material taxonomy node.
Evidence to inspect	Applicable constraint/policy records, jurisdiction and authority references, version/effective period, permitted/prohibited use, and any required precedence/adjudication rule. Include conflict and competent-authority resolution records when a conflict exists.
Evidence sufficiency	The governance-constraint evidence must state the permitted, prohibited, and constrained uses that matter to the decision scope and include applicable policy, privacy, security, purpose, or other governance limits. ***Insufficient:*** A correct definition is not sufficient when the evidence does not also show where, why, or under what constraints the concept or classification may be used.
Assessment procedure	1. Identify applicable constraints and jurisdictions for the governed taxonomy scope. 2. Verify each constraint's authority, scope, version/effective period, and permitted/prohibited use. 3. Identify actual conflicts and inspect the pre-recorded precedence/adjudication rule or competent-authority decision resolving each one. 4. If no valid resolution exists, record Fail and apply the Gate disposition before material use.
Control-result determination	**Pass:** Applicable constraints and jurisdictions are identified; each constraint has authority, scope, version/effective period, and permitted/prohibited use; and each conflict is resolved by a pre-recorded jurisdictional precedence/adjudication rule or explicit competent-authority decision. If no valid resolution exists, the control does not Pass. **Fail:** Constraints conflict without a valid precedence/adjudication rule, authority is unclear, or material use proceeds despite unresolved mutually exclusive requirements.

Common failure modes	• A valid concept is reused outside its approved purpose. • Privacy or policy constraints are documented elsewhere but not applied to the node. • Prohibited use is not machine- or process-visible. • Scope-specific restrictions are lost downstream.
Remediation procedure	**Pattern references:** R-10 - Prohibited or out-of-scope use; R-04 - Missing authority **If a valid concept is being reused outside its approved purpose:** constrain the use to the approved purpose or obtain the required authority for the new use **If privacy, policy, security, or other constraints exist elsewhere but are not applied to the node:** bind the applicable constraints to the taxonomy evidence used by the decision scope **If prohibited use is not visible to the process or system that evaluates the evidence:** record the prohibition in a form the Gate or governing process can inspect **If scope-specific restrictions are lost downstream:** preserve and enforce those restrictions wherever the taxonomy evidence is reused in the material decision path
Repeatable fix	Usage-boundary metadata is reusable and checked whenever the concept is proposed for a new decision scope.
Controlled disposition	Disposition reference: D-05, Threshold, constraint, or conflict. Unresolved mutually exclusive authoritative constraints cause Fail and normally require Stop. Caution is possible only after an explicit competent authority records a bounded resolution/exception that actually permits the stated use.
Example	A customer classification may be used for internal retention analysis but not for adverse eligibility decisions.
Non-example	A governed label is treated as universally usable because its definition is correct.
Authority and execution	**Authority:** Applicable business, governance, privacy, security, policy, or risk authority approves usage constraints.
Retest	Reinspect applicable constraints, jurisdictions, authority, scope, and effective versions. Confirm actual conflicts are resolved under recorded competent authority before use; containment or an unsupported exception alone does not establish Pass.

ET-014: Semantic Risk Is Recorded Where Present

Prerequisites	Recorded result required: ET-004, ET-013.
Specification requirement	Semantic risk shall be recorded when ambiguity, conflict, overlap, deprecated meaning, local variation, or known misuse may affect the decision scope.
Why this control exists	Unrecorded semantic risk can become hidden decision risk.
When this applies	When known ambiguity, conflict, overlap, deprecated meaning, local variation, or misuse may affect the decision scope.
Evidence to inspect	Semantic risk record, owner, readiness disposition, remediation or exception record.
Evidence sufficiency	The semantic-risk evidence must describe each known material semantic risk, identify the affected decision scope, assign an owner, state the readiness disposition, and link the remediation or approved exception. ***Insufficient:*** A known ambiguity, conflict, overlap, deprecated meaning, local variation, or misuse is not sufficiently governed when it exists only in discussion, meeting notes, or undocumented institutional knowledge and has no recorded owner or disposition.
Assessment procedure	**1.** Review known ambiguity, conflict, overlap, deprecated meaning, local variation, and known misuse for the material concepts. **2.** Verify each material semantic risk has an affected scope, owner, readiness disposition, and remediation or exception record.
Control-result determination	**Pass:** Each material semantic risk has a risk description, affected scope, readiness disposition, owner, and remediation or exception record. **Fail:** Known semantic risk affects the decision scope and is not recorded.
Common failure modes	• Known ambiguity is discussed but not recorded. • Risk has no owner. • Deprecated meaning continues without disposition. • Overlap or misuse is known but does not affect readiness state or remediation backlog.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-02 - Ambiguous meaning; R-04 - Missing authority **If known ambiguity, conflict, overlap, deprecated meaning, local variation, or misuse is only discussed informally:** create a semantic-risk record that describes the issue and affected decision scope **If the semantic risk has no owner:** assign the accountable owner for remediation, constraint, or escalation **If deprecated meaning continues without a disposition:** remove, constrain, replace, or explicitly disposition the deprecated meaning **If known overlap or misuse does not affect readiness or remediation tracking:** connect the risk to the appropriate readiness state and remediation or exception record
Repeatable fix	Known ambiguity, overlap, deprecated meaning, and misuse are captured in a repeatable semantic-risk record reviewed at Gates.
Controlled disposition	***Disposition reference:*** **D-05, Threshold, constraint, or conflict.** Use this reference when a known semantic risk has not yet been resolved, constrained, or given an approved disposition.
Example	“Active” has two legacy interpretations; the risk is recorded, the affected reports are identified, and remediation is assigned.
Non-example	Everyone knows the term is ambiguous, but the issue remains only in meeting notes and undocumented institutional knowledge.
Authority and execution	**Authority:** Concept owner or semantic risk owner accepts, remediates, constrains, or escalates recorded semantic risk.
Retest	Reinspect each affected semantic-risk record. Confirm that the risk description, affected scope, owner, readiness disposition, and remediation or exception evidence are now recorded.

ET-015: Relationship Seeds Are Not Treated as Decision-Ready Relationships

Prerequisites	Recorded result required: ET-004, ET-008, ET-013.
Specification requirement	Each relationship seed discovered during taxonomy work shall be preserved in a Relationship Candidate Record. Material use shall follow the applicable recorded Gate disposition and its authority and constraints.
Why this control exists	Taxonomy can expose possible relationships; ontology controls determine whether relationship use is defensible.
When this applies	When taxonomy work discovers, suggests, or exposes a relationship candidate that could become material to the decision path.
Evidence to inspect	Relationship Candidate Record, stable relationship-candidate identifier, source/provenance, discovery method, decision-scope reference, readiness state, Extended Ontology review reference when required, Gate Record, and exception record where applicable.
Evidence sufficiency	The Relationship Candidate Record preserves the stable identifier, source/provenance, discovery method, scope, and readiness state. Required ontology review preserves the same identifier. Actual use follows the recorded Gate authority and constraints. **Insufficient:** A plausible relationship or completed workshop does not establish ready-for-use status. Candidate containment, review, and authorized constrained use remain distinct from a full relationship-control Pass.
Assessment procedure	1. Retrieve each taxonomy-origin Relationship Candidate Record. 2. Verify stable identifier, source/provenance, discovery method, scope, and recorded readiness. 3. Where the Materiality Rule requires ontology review, trace the same candidate identifier into the review record. 4. Compare actual holding or use with the recorded Gate, authority, and any valid constrained-use exception.
Control-result determination	**Pass:** Each relationship seed has a stable relationship-candidate identifier, source and provenance, discovery method, decision-scope reference, current readiness state, and, when the Materiality Rule requires ontology review, an Extended Ontology review reference that preserves the same candidate identifier. **Fail:** A relationship seed is relied on as a ready relationship before required Extended Ontology evaluation, or a required seed-to-ontology evidence link cannot be traced by the same relationship-candidate identifier.

Common failure modes	• A likely relationship discovered during taxonomy work is published as approved. • Relationship seeds bypass ontology review. • Candidate status is lost when evidence is exported or reused.
Remediation procedure	**Pattern reference:** R-07 - Unsupported discovery **If a relationship discovered during taxonomy work was published as approved:** return it to candidate or Quarantined status until the applicable Extended Ontology controls are completed **If a relationship seed bypassed ontology review:** route the material relationship to the Extended Ontology assessment path **If candidate status is lost when evidence is exported or reused:** preserve the candidate or Quarantined state and its review requirement with the exported or reused evidence
Repeatable fix	Taxonomy workflows hand off relationship candidates through a defined ontology review queue with Quarantined state until resolved.
Controlled disposition	***Disposition reference:*** **D-03, Ungoverned candidate evidence.** Use this reference for relationship seeds discovered during taxonomy work until Extended Ontology review establishes their governed status.
Example	A taxonomy workshop identifies that Account “belongs to” Region; the relationship is logged as a candidate for ontology review.
Non-example	The relationship is added to an approved decision path because it appeared during taxonomy analysis.
Authority and execution	**Authority:** Taxonomy steward identifies the relationship seed; ontology authority determines whether it becomes an approved relationship.
Retest	Verify each required candidate field and identifier continuity into ontology review where required. Confirm actual handling follows the recorded Gate disposition and any authorized constrained-use bounds.

ET-016: Readiness State Is Declared

Prerequisites	Recorded result required: ET-013, ET-014, ET-015.
Specification requirement	Each material taxonomy node used in a decision path shall have a recorded readiness state for the decision scope.
Why this control exists	Governed meaning must have a decision-scope disposition.
When this applies	When a material taxonomy node is used in the decision path and therefore requires a scope-bound readiness disposition.
Evidence to inspect	Readiness state record, Gate Record, reason, responsible authority or approved rule reference, timestamp, review condition.
Evidence sufficiency	The readiness evidence must show the formal readiness state assigned to each material taxonomy node for the stated decision scope and the supporting reason, authority or rule, timestamp, and review condition where required. ***Insufficient:*** Catalog presence, publication status, prior approval, or use in another scope is not sufficient to establish Proceed, Caution, Stop, or Quarantined for the decision scope being assessed.
Assessment procedure	**1.** Inspect every material taxonomy node used in the decision path. **2.** Verify a formal readiness state is supported by Gate evidence, reason, authority or rule, timestamp, and review condition where required.
Control-result determination	**Pass:** The node is assigned Proceed, Caution, Stop, or Quarantined with reason, responsible authority or approved rule reference, timestamp, and review condition where required. **Fail:** A material node is used without a readiness state or the state is unsupported by evidence.
Common failure modes	• A readiness state is copied from another scope. • Proceed is inferred from catalog presence. • Reason or authority is absent. • Review date has expired. • Readiness is not updated after material change.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-08 - Material change or drift **If a readiness state was copied from another decision scope:** evaluate the taxonomy node for the current decision scope and assign a new scope-bound state **If Proceed is inferred merely because the node exists in a governed catalog:** run the applicable Gate evaluation and record the resulting readiness state **If the reason or authority supporting the state is missing:** record the basis and responsible authority or rule **If the review condition has expired:** reassess the node and issue a current readiness state **If material change occurred but the readiness state was not updated:** rerun the affected evaluation and record a new linked state before further stated use
Repeatable fix	Readiness is derived from Gate evaluation and stored with the taxonomy node for the decision scope.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material taxonomy node lacks a supported readiness state for the decision scope.
Example	A disputed classification is Caution with an approved internal-use constraint and review date.
Non-example	A node is marked Proceed because it is in the catalog, although required evidence was never evaluated.
Authority and execution	**Authority:** The responsible decision-scope authority approves the readiness state based on Gate evidence. An approved rule may execute or record the evaluation; the taxonomy owner or steward remains accountable for the underlying semantic condition.
Retest	Reinspect the readiness record for each affected material taxonomy node. Confirm that the formal readiness state is supported by reason, authority or rule, timestamp, Gate evidence, and review condition where required.

ET-017: Taxonomy Change Triggers Reassessment

Prerequisites	Pass required: CORE-023, ET-002. Recorded result required: ET-016.
Specification requirement	Each material Extended Taxonomy change shall trigger impact assessment for active or prospective decision scopes that rely on the changed artifact. Historical Gate and Conformance Records remain fixed to the taxonomy version that governed them.
Why this control exists	Meaning changes can invalidate evidence previously ready for stated use.
When this applies	When a material taxonomy definition, label, boundary, grain, identifier, source representation, ownership, constraint, or readiness state changes.
Evidence to inspect	Taxonomy change/version record, impact rule, affected-scope list, readiness invalidation/reassessment record, new Gate/Conformance Record where required, and immutable historical references.
Evidence sufficiency	The change evidence must show which taxonomy changes are material, which decision scopes are affected, and that those scopes receive the required impact review or Gate reassessment before prior readiness or conformance determination is relied upon. ***Insufficient:*** A taxonomy version or change log is not sufficient when a change to meaning, label, boundary, grain, identifier, representation, ownership, constraint, or readiness can occur without reassessing affected decision scopes previously allowed for stated use.
Assessment procedure	**1.** Inspect taxonomy change rules and a recent or test change to meaning, label, boundary, grain, identifier, representation, ownership, constraint, or readiness state. **2.** Verify affected decision scopes are identified and reassessed.
Control-result determination	**Pass:** A material taxonomy change is versioned, affected active/prospective scopes are identified, prior readiness for new reliance is invalidated or reassessed as defined, and any new Gate/Conformance Record is linked to the prior record without rewriting it. **Fail:** Future reliance continues under a materially changed taxonomy without reassessment, or historical records are retroactively recalculated or overwritten merely because the taxonomy changed.
Common failure modes	• Taxonomy version changes but affected scopes are not identified. • Label changes are treated as harmless despite semantic impact. • Source representation changes bypass reassessment. • Readiness remains out of date after material taxonomy change.

Remediation procedure	Apply forward-only impact assessment: identify active/prospective scopes, invalidate readiness for new reliance as defined, reassess, and preserve historical records unchanged.
Repeatable fix	Change management connects taxonomy version events to a scope-impact register and reassessment workflow.
Controlled disposition	***Disposition reference:*** **D-04, Change or reassessment.** Use this reference after a material taxonomy change until affected decision scopes have been identified and reassessed.
Example	Changing the boundary of Active Customer triggers reassessment of every metric previously allowed for stated use using that concept.
Non-example	A definition changes but prior readiness or conformance determinations continue indefinitely with no impact review.
Authority and execution	**Authority:** Taxonomy owner governs the change; affected decision-scope owners authorize reassessment and resulting disposition. **Execution:** A material taxonomy change must identify affected decision scopes and route them to impact review or Gate reassessment.
Retest	Apply or inspect a representative material taxonomy change. Confirm that affected decision scopes are identified and the required impact review, Gate reassessment, and linked replacement Conformance Records are created.

9. Extended Ontology Controls

These cards apply when material relationships or relationship paths affect the decision path. Discovery remains permitted; relationship use for the stated decision scope requires the applicable controls to pass.

Card boundary

The Specification requirement, Prerequisites, Evidence to inspect, and Pass/Fail text below reproduce DACS Specification v1.13. Sections 2 through 5 explain its global assessment and closure rules. Procedures, failure modes, remediation, and examples are informative guidance. Apply the exact Specification version governing the assessment; the catalog does not add criteria or override it.

EO-001: Relationship Candidate Is Not Treated as Decision-Ready

Prerequisites	Recorded result required: ET-015 (when the candidate originated in taxonomy work).
Specification requirement	A relationship candidate shall remain excluded from material reliance unless the applicable recorded Gate disposition explicitly permits its stated use.
Why this control exists	Discovery is valuable, but discovery does not establish readiness for stated use.
When this applies	When a relationship is declared, discovered, inferred, imported, derived, or otherwise introduced as candidate evidence.
Evidence to inspect	Relationship Candidate Record, stable relationship-candidate identifier, source/provenance, readiness state, Extended Ontology review evidence, Gate Record, and exception record where applicable.
Evidence sufficiency	The relationship-candidate evidence must preserve candidate status and show that each material declared, discovered, inferred, imported, or derived relationship is reviewed, constrained, rejected, Quarantined, or approved through the applicable Gate process before stated use. ***Insufficient:*** A relationship is not sufficient to establish readiness for stated use merely because it exists in a graph, was imported from an approved or governed system, was inferred with high confidence, or was accepted by an analyst.
Assessment procedure	1. Retrieve the Relationship Candidate Record, readiness state, and applicable review or Gate evidence. 2. Verify no material reliance occurs without a Gate that permits the stated use. 3. For taxonomy-origin candidates, trace the same candidate identifier and source/provenance through ontology review. 4. Verify any constrained use has an authorizing exception and remains within its bounds.
Control-result determination	**Pass:** The relationship candidate is recorded in a Relationship Candidate Record and has a recorded readiness state and Gate evidence before material use. If it originated in taxonomy work, the same relationship-candidate identifier and source/provenance are preserved through Extended Ontology review. **Fail:** A candidate relationship is relied on for stated use without the applicable Gate evaluation and readiness state, or a taxonomy-origin candidate loses its identifier or provenance during ontology review.

Common failure modes	• Inferred or discovered relationships are promoted directly into analytics. • Imported graph edges are assumed ready for stated use. • Candidate status is lost. • Constrained use is not recorded before material use.
Remediation procedure	**Pattern reference:** R-07 - Unsupported discovery **If an inferred, discovered, or derived relationship was promoted directly into analytics:** return it to candidate or Quarantined status until the applicable Extended Ontology controls pass **If an imported graph edge is assumed ready for stated use because it already exists in another system:** treat the imported relationship as candidate evidence and evaluate it for the stated decision scope **If candidate status was lost:** restore the candidate or Quarantined designation and the required review path **If constrained use occurs without a recorded exception:** record the authorized exception before material use or Stop the use
Repeatable fix	Relationship discovery pipelines separate candidate assertions from governed relationships and route them to review.
Controlled disposition	***Disposition reference:*** **D-03, Ungoverned candidate evidence.** Use this reference for relationship candidates that have not yet passed the applicable Extended Ontology controls or received an approved constrained-use exception.
Example	A graph-discovered supplier dependency is retained for analysis but cannot drive a sourcing decision until reviewed.
Non-example	An inferred relationship is immediately treated as ready for stated use because the model confidence is high.
Authority and execution	**Authority:** Relationship discovery may be performed by people or systems. The responsible ontology or decision-scope authority controls promotion toward stated use.
Retest	Verify the candidate record, Gate evidence before material use, and actual handling. For taxonomy-origin candidates, confirm identifier and provenance continuity. Review alone does not establish permission to rely.

EO-002: Relationship Type Is Governed

Prerequisites	Recorded result required: EO-001.
Specification requirement	Each material relationship shall map to an approved relationship type for the decision scope.
Why this control exists	A relationship cannot be tested if its type is not governed.
When this applies	When a material relationship is used and the relationship type determines its governed meaning for the decision scope.
Evidence to inspect	Relationship type record, owner, version, approval record, decision-scope mapping.
Evidence sufficiency	The relationship-type evidence must map each material relationship to a defined, owned, versioned, and approved relationship type for the stated decision scope. ***Insufficient:*** A free-text label, local relationship name, graph edge type, or technically valid association is not sufficient when the governed relationship type and its approved business meaning cannot be established.
Assessment procedure	**1.** Inspect each material relationship used by the decision scope. **2.** Verify that each material relationship maps to a defined, owned, versioned, and approved relationship type for that decision scope.
Control-result determination	**Pass:** The relationship type is defined, owned, versioned, and approved for the stated scope. **Fail:** The relationship uses an undefined, ambiguous, prohibited, or unapproved type.
Common failure modes	• Relationship labels are locally invented. • One label hides multiple business meanings. • Type owner or version is missing. • Relationship type is technically present but not approved for the scope.

Remediation procedure	**Pattern references:** R-02 - Ambiguous meaning; R-04 - Missing authority **If relationship labels are locally invented:** map the relationship to an approved relationship type or govern a new type before use **If one relationship label hides more than one business meaning:** split the meanings into distinct governed relationship types or define explicit boundaries **If the relationship type has no owner or version:** assign ownership and record the applicable version **If the type exists technically but is not approved for the decision scope:** obtain scope approval or keep the relationship out of stated use
Repeatable fix	Relationship-type governance maintains an approved vocabulary and change process.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material relationship does not yet map to an approved relationship type.
Example	“Account is billed through Billing Customer” uses an approved relationship type for the scope.
Non-example	A relationship labeled “related to” is used without defining what the relationship means.
Authority and execution	**Authority:** Relationship or ontology authority approves type definition, ownership, and scope use.
Retest	Reinspect each affected material relationship. Confirm that it now maps to a defined, owned, versioned, and approved relationship type for the stated decision scope.

EO-003: Relationship Orientation Is Declared

Prerequisites	Pass required: EO-002.
Specification requirement	Each material relationship shall declare orientation.
Why this control exists	Many failures occur when association is mistaken for authority, sequence is mistaken for cause, or a one-way relationship is treated as symmetrical.
When this applies	When direction, authority, sequence, dependency, ownership, lineage, hierarchy, flow, support, inclusion, identification, reconciliation, constraint, or causality affects use of a material relationship.
Evidence to inspect	Orientation record, orientation type, approval record, decision-scope mapping.
Evidence sufficiency	The orientation evidence must explicitly state the applicable direction or other approved orientation for each material relationship and support the way the relationship is traversed or interpreted in the decision scope. ***Insufficient:*** A relationship name alone is not sufficient when the decision depends on direction, authority, sequence, dependency, ownership, lineage, hierarchy, flow, support, inclusion, identification, reconciliation, constraint, or causality.
Assessment procedure	**1.** Inspect each material relationship for orientation. **2.** Verify direction, authority, sequence, dependency, ownership, lineage, hierarchy, flow, support, inclusion, identification, reconciliation, constraint, causality where separately established, or another approved orientation is explicitly recorded.
Control-result determination	**Pass:** 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:** Orientation is missing or an oriented relationship is used as symmetrical without approval.
Common failure modes	• Direction is omitted. • A one-way relationship is treated as symmetrical. • Sequence is interpreted as causality. • Dependency is treated as ownership. • Authority direction is reversed.

Remediation procedure	**Pattern references:** R-02 - Ambiguous meaning; R-06 - Threshold or rule failure **If relationship direction is omitted:** record the approved orientation and allowed direction of use **If a one-way relationship is treated as symmetrical:** restrict traversal to the approved direction unless symmetrical use is separately approved **If sequence is being interpreted as causality:** record the relationship as sequence unless separate causal evidence establishes causality **If dependency is being treated as ownership:** correct the relationship meaning and orientation to the approved type **If authority direction is reversed:** correct the orientation and reassess any decision path that used the reversed relationship
Repeatable fix	Relationship records require orientation from an approved set and Gate checks validate traversal against it.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when the required orientation of a material relationship is missing, ambiguous, or being used incorrectly.
Example	Contract governs Account is directional and cannot be traversed as if Account governs Contract.
Non-example	A correlation discovered in time sequence is labeled causal without separate causal evidence.
Authority and execution	**Authority:** Relationship or ontology authority approves orientation and any directional semantics.
Retest	Reinspect each affected material relationship and any traversal that uses it. Confirm that the approved orientation is explicit and that the relationship is not used with an unapproved symmetry, direction, or causal interpretation.

EO-004: Relationship Assertion Provenance Is Recorded

Prerequisites	Recorded result required: EO-001, EO-002.
Specification requirement	Each material relationship assertion shall record provenance.
Why this control exists	Relationship accountability requires knowing how the relationship entered the evidence stream.
When this applies	When a material relationship assertion must be traced to how, when, and under what authority or method it was created.
Evidence to inspect	Assertion provenance record, source/method record, responsible authority or approved rule reference, timestamp/effective period, version.
Evidence sufficiency	The relationship-provenance evidence must show how each material assertion was created, its source and method, the responsible authority or rule, the applicable version, and the timestamp or effective period. ***Insufficient:*** A graph edge or relationship record is not sufficient when a reviewer cannot determine whether it was declared, inferred, discovered, imported, derived, or generated, or cannot identify the method and authority behind the assertion.
Assessment procedure	**1.** Inspect each material relationship assertion. **2.** Verify that the provenance record states whether the assertion was declared, inferred, discovered, imported, derived, or generated. **3.** Verify that the record also identifies the source, method, authority or rule, applicable version, and timestamp or effective period.
Control-result determination	**Pass:** 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:** Source, creation method, authority or rule reference, timestamp/effective period, or version is missing or cannot be retrieved.
Common failure modes	• The relationship is visible but how it was created is unknown. • AI-inferred and human-declared assertions are indistinguishable. • Method version or source is missing. • Effective period is not preserved.

Remediation procedure	**Pattern reference:** R-01 - Missing evidence **If a relationship exists but its origin cannot be determined:** add the provenance record or keep the assertion Quarantined until its origin can be established **If AI-inferred and human-declared assertions cannot be distinguished:** record how each assertion was created and the method or authority responsible for it **If the method version or source is missing:** record the applicable source and method, rule, or model version **If the effective period is missing:** record when the relationship assertion is valid for the stated decision scope
Repeatable fix	Every material assertion carries provenance metadata from creation or import.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when the provenance of a material relationship assertion is incomplete or cannot be reconstructed.
Example	A relationship records that it was imported from CRM rule set v5 on the effective date and approved by the data steward.
Non-example	A graph edge exists, but no one can tell whether it was declared, inferred, imported, or generated.
Authority and execution	**Authority:** Assertion authority or method owner must be identifiable; ontology stewardship preserves provenance.
Retest	Reconstruct the provenance of each affected material relationship assertion. Confirm the creation method, source, authority or rule, version, and effective time are now retrievable.

EO-005: Physical Relationship Representation or Boundary Evidence Anchor Is Recorded Where Required

Prerequisites	Pass required: CORE-005, EO-004.
Specification requirement	Each material relationship shall record the physical relationship representation required for the decision scope. Where an external, legacy, proprietary, or third-party system prevents direct inspection, a Boundary Evidence Anchor may represent the relationship boundary only when it identifies the exact external relationship evidence consumed and the inaccessible boundary.
Why this control exists	Extended Ontology closes the gap between governed relationship meaning and real relationship evidence.
When this applies	When a material governed relationship must be tied to the physical join, association, event, message, API, document, lineage, or other representation that substantiates it.
Evidence to inspect	Physical relationship locator or complete Boundary Evidence Anchor, provenance, relationship reference, inaccessible-boundary statement where applicable, and decision-scope mapping.
Evidence sufficiency	Direct physical evidence identifies the representation needed to test the relationship. Where direct inspection is legitimately unavailable, the complete Boundary Evidence Anchor identifies the exact external evidence and inaccessible boundary, required versions and time, relationship reference, and scope mapping. **Insufficient:** An ontology diagram or vendor attestation alone does not identify the consumed relationship evidence.
Assessment procedure	1. Trace the relationship to its required physical join, event, link, document, API, message, or equivalent evidence. 2. Where direct inspection is legitimately unavailable, verify every required Boundary Evidence Anchor field, including exact evidence identity, interface/version, time, inaccessible boundary, relationship reference, and scope. 3. Inspect fingerprints where possible and supporting contract or attestation references where available. Vendor attestation alone is not sufficient.

Control-result determination	**Pass:** The relationship can be traced to the required join/event/link/document/API/message or equivalent physical evidence; or a complete Boundary Evidence Anchor records source identity, interface/feed/contract and version, payload/event/message/document identifier, acquisition time/effective period, fingerprint where possible, supporting attestation/contract where available, inaccessible boundary, relationship-candidate or assertion reference, and decision-scope mapping. Vendor attestation alone is not sufficient. **Fail:** A material relationship is relied on without traceable physical evidence or a complete Boundary Evidence Anchor.
Common failure modes	• A conceptual relationship has no traceable physical evidence. • Joins are inferred from naming alone. • Association structures or relationship attributes are omitted. • Physical representation changes without updating the governed relationship.
Remediation procedure	**Pattern references:** R-01, R-13 **If physical representation is missing:** locate and record the evidence used to substantiate the relationship. **If a join is inferred only from names:** obtain governed relationship evidence. **If direct inspection is legitimately unavailable:** complete the Boundary Evidence Anchor, including exact evidence identity and inaccessible boundary. **If the representation changed:** version the new anchor and reassess affected future use. Preserve historical references.
Repeatable fix	Governed relationship records retain the physical representation used by the scope and update it through change control.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material governed relationship lacks the physical representation needed for testing.
Example	Account-to-Contract is evidenced by the source association table and key mapping.
Non-example	The ontology diagram shows a relationship, but the implementing data cannot be located or tested.
Authority and execution	**Authority:** Ontology steward owns relationship meaning; source owners confirm the physical relationship evidence.
Retest	Trace the affected relationship to physical evidence or inspect every required field of the permitted Boundary Evidence Anchor. Verify the exact consumed evidence, relationship reference, scope mapping, and conditional fingerprint and supporting-reference obligations.

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

Prerequisites	Pass required: ET-011, EO-003.
Specification requirement	Each material relationship shall test whether related identifiers and concepts are aligned at compatible semantic grain for the decision scope.
Why this control exists	A relationship path can fail because its endpoints identify different business things at different grains.
When this applies	When a material relationship connects identifiers or concepts whose business identity or semantic grain could differ.
Evidence to inspect	Endpoint identity records, business-meaning and semantic-grain records, equivalence/non-equivalence rule, endpoint-alignment test results, and decision-scope mapping.
Evidence sufficiency	Each material endpoint has identity, business-meaning, and grain evidence. A recorded equivalence or non-equivalence rule governs compatibility, and endpoint-alignment test results satisfy that rule for the intended use. **Insufficient:** Endpoint records, technically joinable keys, or a crosswalk alone do not establish that the intended alignment was tested and satisfied its governing rule.
Assessment procedure	1. Identify both material endpoints and retrieve their identity, meaning, grain, and governing alignment rule. 2. Execute or inspect the endpoint-alignment test for the intended relationship use. 3. Compare recorded test results with the equivalence or non-equivalence rule. 4. Verify intended joining, traversal, counting, or inference does not exceed the demonstrated compatibility.
Control-result determination	**Pass:** The record identifies each material endpoint, its identity evidence, business meaning, and semantic grain; the governing equivalence or non-equivalence rule is recorded; and endpoint-alignment test results satisfy that rule for the intended relationship use. **Fail:** Relationship endpoints are joined, traversed, counted, or inferred as compatible without required grain and identity evidence.
Common failure modes	• Endpoints represent different business things or grains. • Source keys are assumed equivalent. • Many-to-many conditions are treated as one-to-one. • Crosswalks exist but are not governed for the scope.

Remediation procedure	**Pattern references:** R-03 - Unstable identity or grain; R-05 - Conflicting evidence **If relationship endpoints represent different business things or incompatible grains:** separate the endpoints or establish the governed compatibility or crosswalk rule **If source keys are assumed equivalent:** prove endpoint identity through approved Business Identity evidence or a governed crosswalk **If a many-to-many condition is treated as one-to-one:** record the actual cardinality or grain and correct the relationship logic **If a crosswalk exists but is not governed for the decision scope:** approve, version, and bind the crosswalk to the stated scope before stated use
Repeatable fix	Relationship onboarding requires endpoint identity and grain checks before traversal is approved.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when relationship endpoints do not yet have demonstrated identity and grain compatibility.
Example	Account-to-Billing Customer uses a governed crosswalk proving both endpoints represent account-level business instances.
Non-example	A person-level identifier is joined to an account-level identifier and treated as a one-to-one relationship.
Authority and execution	**Authority:** Identity authority governs endpoint identity and grain; ontology authority governs relationship compatibility.
Retest	Repeat the endpoint-alignment test under the recorded rule and effective versions. Confirm identity, meaning, grain, and test results support the intended relationship use.

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

Prerequisites	Pass required: EO-004.
Specification requirement	Each material relationship shall record the method by which it was declared, discovered, inferred, imported, or derived.
Why this control exists	DACS permits relationship discovery. Stated use requires the method evidence declared by EO-007 to review or reproduce the assertion path where the control applies.
When this applies	When a material relationship was declared, discovered, inferred, imported, derived, or generated by a method that must be reviewable or reproducible.
Evidence to inspect	Method record, input evidence, authority, rule/model/version where applicable, repeatability evidence where applicable.
Evidence sufficiency	The method evidence must identify the process by which each material relationship was declared, discovered, inferred, imported, derived, or generated, including the method owner or authority, input evidence, applicable rule or model version, and repeatability condition where required. ***Insufficient:*** Describing the method only as AI, analysis, discovery, or manual review is not sufficient when the reviewer cannot identify the actual method, inputs, authority, or version that produced the relationship assertion.
Assessment procedure	**1.** Inspect the method record for each material relationship assertion. **2.** Verify method or process, owner or authority, input evidence, rule or model version where applicable, and repeatability condition where applicable are recorded.
Control-result determination	**Pass:** The record includes method name or process, method owner or authority, input evidence, rule/model/version where applicable, and repeatability condition where applicable. **Fail:** The method name/process, authority, input evidence, required rule/model/version, or required repeatability condition is missing or cannot be retrieved.
Common failure modes	• The assertion method is described only as “AI” or “analysis”. • Input evidence is not retained. • Model or rule version is missing. • Declared relationships have no named authority. • Repeatability condition is undefined.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-12 - Automated or AI-assisted control **If the assertion method is described only as AI, analysis, or another vague label:** record the specific method or process that produced the relationship assertion **If input evidence was not retained:** preserve the inputs required to review or reproduce the assertion path **If the model or rule version is missing:** record the applicable version used to create the assertion **If a declared relationship has no named authority:** identify the person, role, or approved rule that declared it **If the repeatability condition is undefined:** state what inputs, versions, rules, or conditions must be held constant when the assertion is replayed or reviewed
Repeatable fix	Each method has a controlled method record and produces traceable assertion evidence.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when the method that produced a material relationship cannot yet be reviewed or reproduced from recorded evidence.
Example	A relationship inferred by rules engine v8 records input evidence and the rule that produced it.
Non-example	The team knows AI found the relationship but cannot identify the model version, inputs, or method.
Authority and execution	**Authority:** Method owner or declaring authority owns the assertion method; ontology authority approves its use for the scope.
Retest	Reinspect the method record for each affected relationship assertion. Confirm the method, owner or authority, input evidence, rule or model version where applicable, and repeatability condition are now recorded.

EO-008: Minimum Relationship Vector Criteria Are Defined

Prerequisites	Pass required: CORE-002, EO-003.
Specification requirement	Before a material relationship vector is evaluated, the decision scope shall define the measurement scale and minimum criteria for Strength, Confidence, and Orientation that govern the stated use. DACS supplies no universal numeric floor.
Why this control exists	A vector only controls use when the decision scope defines what passes.
When this applies	Before a material relationship vector is evaluated for a decision scope that relies on that relationship type or path.
Evidence to inspect	Vector-criteria record, scale definitions, thresholds/rules, authority, version/effective period, decision-scope mapping, reassessment triggers, and creation/effective timestamp.
Evidence sufficiency	The vector-criteria evidence must define the required Strength, Confidence, and Orientation thresholds or approved qualitative rules before the relationship is evaluated at the Gate. ***Insufficient:*** Criteria are not sufficient when they are chosen or changed after the relationship result is known, are undocumented, or omit a required vector dimension for the material relationship type or path.
Assessment procedure	1. Inspect criteria for every required vector dimension: Strength, Confidence, and Orientation. 2. Verify scale definitions, threshold or qualitative rule, authority, effective version, scope mapping, and applicable reassessment triggers. 3. Compare criteria creation/effective time with the dependent vector evaluation. 4. If criteria were selected after seeing the result, preserve that finding and assess a new prospective version.
Control-result determination	**Pass:** The criteria record identifies each vector dimension, measurement or qualitative scale, threshold/rule, authority, version/effective period, decision-scope mapping, and reassessment trigger where applicable, and it was established before the dependent vector evaluation. **Fail:** Criteria are absent, created after seeing the vector result, borrowed from an unrelated scope, or depend on an unspecified DACS default threshold.

Common failure modes	• Thresholds are chosen after observing results. • Qualitative rules are undocumented. • Criteria exist for Confidence but not Strength or Orientation. • Criteria are not bound to relationship type or decision scope.
Remediation procedure	**Pattern references:** R-06 - Threshold or rule failure; R-04 - Missing authority **If thresholds were selected after reviewers saw the results:** define and approve the vector criteria before evaluating the relationship **If qualitative criteria are used but not documented:** record the qualitative decision rule so another assessor can apply it consistently **If criteria exist for only one or two vector dimensions:** define the required Strength, Confidence, and Orientation criteria **If the criteria are not bound to a relationship type or decision scope:** link the criteria to the relationship type or path and the stated decision scope
Repeatable fix	Decision-scope setup requires approved vector criteria by relationship type or path before Gate execution.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when minimum relationship-vector criteria were not defined before Gate evaluation.
Example	Before testing, the scope records its own Strength scale and minimum, Confidence threshold, and permitted Orientation, with authority and effective version. These are scope criteria, not DACS default thresholds.
Non-example	Reviewers accept the relationship after seeing the result even though no approved criteria were defined.
Authority and execution	**Authority:** Decision-scope authority approves the minimum vector criteria before evaluation.
Retest	Verify every required dimension, scale, criterion, authority, version/effective period, scope mapping, and applicable trigger was established before the dependent evaluation. Later corrections belong to a new evaluation.

EO-009: Relationship Vector Is Recorded for Material Relationships

Prerequisites	Pass required: EO-007, EO-008.
Specification requirement	Each material relationship shall carry a relationship vector containing Strength, Confidence, and Orientation.
Why this control exists	The vector makes relationship evaluation testable rather than assumed.
When this applies	When a material relationship is evaluated using the DACS relationship vector of Strength, Confidence, and Orientation.
Evidence to inspect	Relationship vector record, Strength evidence, Confidence evidence, Orientation evidence, decision-scope mapping.
Evidence sufficiency	The relationship-vector evidence must include all three required dimensions, Strength, Confidence, and Orientation, and must identify the measurement method or approval basis used for the decision scope. ***Insufficient:*** A single confidence score, generic trust score, or unqualified relationship rating is not sufficient when Strength, Confidence, and Orientation cannot each be inspected and understood.
Assessment procedure	**1.** Inspect each material relationship vector. **2.** Verify Strength, Confidence, and Orientation are all recorded with the measurement method or approval basis used for the decision scope.
Control-result determination	**Pass:** Strength, Confidence, and Orientation are recorded with measurement method or approval basis for the decision scope. **Fail:** Any vector component is missing for a material relationship.
Common failure modes	• Only a single confidence score is recorded. • Strength or Orientation is missing. • Vector values have no measurement or approval basis. • Vector is copied between scopes without evaluation.
Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-06 - Threshold or rule failure **If only a single confidence or trust score is recorded:** record Strength, Confidence, and Orientation separately **If Strength or Orientation is missing:** complete the relationship vector with all required dimensions **If vector values have no measurement or approval basis:** record how each value was measured, derived, or approved **If a vector from another decision scope was copied without evaluation:** evaluate the relationship vector for the current decision scope

Repeatable fix	Relationship evaluation uses a standard vector record with all three dimensions and their basis.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when one or more required relationship-vector dimensions, or their measurement basis, are missing.
Example	Strength 4/5, Confidence 0.92, Orientation dependency are recorded using approved criteria.
Non-example	A relationship has one “trust score” with no orientation and no way to distinguish signal strength from evidence confidence.
Authority and execution	**Authority:** Relationship authority approves vector method or values; automated scoring may implement approved criteria.
Retest	Reinspect each affected relationship vector. Confirm that Strength, Confidence, and Orientation are all present and that the measurement method or approval basis for each dimension is recorded.

EO-010: Relationship Vector Meets Decision-Scope Criteria

Prerequisites	Pass required: EO-009.
Specification requirement	Each material relationship used for decision evidence for stated use shall meet the decision-scope vector criteria. A constrained-use exception may permit Caution after a failed vector test, but it does not make this control Pass.
Why this control exists	Relationship use must be controlled by evidence, not plausibility.
When this applies	When a material relationship is proposed for stated use and must be compared with the decision-scope vector criteria.
Evidence to inspect	Relationship vector evaluation record, applicable vector criteria, threshold or qualitative-rule results, Gate Record, and exception record where constrained use is authorized after a Fail.
Evidence sufficiency	Evaluation records compare Strength, Confidence, and Orientation with every applicable criterion and preserve the actual control result. Exception evidence is separate and may authorize bounded Caution after a Fail. **Insufficient:** High confidence, plausibility, or an approved exception does not establish that every vector criterion was met.
Assessment procedure	1. Compare each required vector dimension with the effective decision-scope criterion. 2. Record Pass only when every applicable criterion is satisfied; otherwise record Fail. 3. Separately inspect any exception, its authority and bounds, and the resulting Gate state. The exception does not change this result.
Control-result determination	**Pass:** The recorded Strength, Confidence, and Orientation evidence satisfies every applicable decision-scope vector criterion. **Fail:** Any applicable vector criterion fails, is missing, or is not evaluated. An approved constrained-use exception may affect the Gate readiness state but the control remains Fail.
Common failure modes	• A relationship that does not meet the approved vector criteria is still relied on as evidence for stated use. • Exception is verbal. • Only one vector dimension is checked. • Out of date vector evidence is reused after material change.

Remediation procedure	**Pattern references:** R-06 - Threshold or rule failure; R-10 - Prohibited or out-of-scope use **If a relationship does not meet the approved vector criteria but is still relied on as evidence for stated use:** remove it from stated use, improve the evidence, or use an authorized bounded exception that produces the appropriate readiness state **If an exception exists only verbally:** record the exception, authority, limits, and review condition **If only one vector dimension was evaluated:** evaluate every vector dimension required by the decision-scope criteria **If outdated vector evidence is being reused after material change:** recalculate or reassess the vector under the current evidence and criteria
Repeatable fix	Vector evaluation is repeatable against versioned criteria and records exceptions separately from Pass.
Controlled disposition	***Disposition reference:*** *D-05, Threshold, constraint, or conflict.* *Use this reference when an applicable vector criterion fails or cannot be established. Any valid constrained-use exception affects Gate permission only; the failed vector result remains visible.*
Example	Recorded Strength, Confidence, and Orientation satisfy their respective scope-defined criteria. The vector evaluation records Pass; the applicable Gate separately determines permitted use.
Non-example	A relationship below threshold is marked Pass because a reviewer believes it is probably correct.
Authority and execution	**Authority:** The responsible relationship or decision-scope authority owns the approved vector criteria and any constrained-use exceptions. A governed manual or automated mechanism may apply the criteria under that authority.
Retest	Reevaluate every applicable vector criterion under its recorded version. Preserve the new Pass or Fail separately from any exception and Gate disposition. An exception alone does not close the failed vector test.

EO-011: Permitted and Prohibited Relationship Paths Are Declared

Prerequisites	Pass required: CORE-002, EO-003.
Specification requirement	Each decision scope shall declare permitted and prohibited relationship paths when relationship traversal affects the decision.
Why this control exists	Path control prevents unauthorized semantic traversal.
When this applies	When relationship traversal can change the meaning, evidence path, or outcome of the stated decision scope.
Evidence to inspect	Permitted/prohibited path record, traversal rule, constraint record, decision-scope mapping.
Evidence sufficiency	The path evidence must state which material relationship paths are permitted, which are prohibited, and any traversal limits or path constraints that govern how the decision path may use them. ***Insufficient:*** Technical ability to traverse a graph, join, lineage path, or association is not sufficient authorization to use that path when the decision scope has not approved the traversal.
Assessment procedure	**1.** Trace the material decision path and identify relationship traversals that can affect the result. **2.** Verify permitted paths, prohibited paths, path constraints, and traversal limits are recorded before use.
Control-result determination	**Pass:** Permitted paths, prohibited paths, path constraints, and traversal limits are recorded. **Fail:** A decision path uses relationship traversal without approved path rules.
Common failure modes	• Graph or join traversal follows any technically available path. • Prohibited paths are implicit. • Traversal depth or path constraints are absent. • An approved path in one scope is reused in another without review.

Remediation procedure	**Pattern references:** R-10 - Prohibited or out-of-scope use; R-02 - Ambiguous meaning **If traversal follows any technically available path:** declare the permitted relationship paths for the stated decision scope **If prohibited paths are only implicit:** record the prohibited paths explicitly **If traversal depth, direction, or other path limits are missing:** define the required path constraints before use **If a path approved in another decision scope is reused without review:** evaluate and approve the path for the current scope
Repeatable fix	Traversal rules are stored as governed path policies and checked manually or automatically before use.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when material relationship traversal lacks approved permitted, prohibited, or constrained path rules.
Example	Account -> Contract -> Status is permitted; Account -> Prospect -> Credit Action is prohibited for the scope.
Non-example	An analytics query traverses any available graph edge because the graph technically allows it.
Authority and execution	**Authority:** Decision-scope owner and ontology authority approve permitted and prohibited traversal paths.
Retest	Retrace the affected relationship path. Confirm that every material traversal follows an approved permitted path, avoids prohibited paths, and respects the recorded traversal limits and constraints.

EO-012: Relationship Conflict and Jurisdiction Resolution Rule Exists Where Applicable

Prerequisites	Pass required: EO-011. Recorded result required: ET-013.
Specification requirement	When competing relationship assertions, jurisdictions, policies, or authorities can produce mutually exclusive relationship use, a recorded conflict-resolution or jurisdictional precedence rule shall exist before material reliance.
Why this control exists	Conflicting relationship evidence cannot support Defensible Analytics without disposition.
When this applies	When two or more material relationship assertions conflict for the same decision scope.
Evidence to inspect	Precedence/adjudication rule, applicable jurisdictional authorities, scope, version/effective period, tie-break/escalation behavior, and permitted/prohibited path. Include conflict and resolution records when an actual conflict exists.
Evidence sufficiency	Each applicable conflict class has a recorded rule with authority, scope, effective version, tie-break or escalation behavior, and permitted/prohibited path. Every actual conflict affecting material reliance is resolved under the rule or by a recorded competent-authority decision before use. **Insufficient:** An unresolved conflict held under Stop or Quarantined is correctly contained but does not establish Pass for conflict resolution. Escalation, informal selection, or an exception without competent resolution is not proof of resolution.
Assessment procedure	1. Identify applicable conflict classes and retrieve their precedence or adjudication rules. 2. Verify authority, scope, effective version, tie-break/escalation behavior, and permitted/prohibited path. 3. Trace each actual conflict affecting reliance to a resolution under that rule or a recorded competent-authority decision. 4. Record Fail for an unresolved conflict; inspect containment and any separately authorized Gate state without treating them as resolution.

Control-result determination	**Pass:** Each applicable conflict class has a recorded precedence/adjudication rule with authority, scope, version/effective period, tie-break or escalation behavior, and permitted/prohibited path. Each actual conflict affecting material reliance is resolved under that rule before use. A recorded competent-authority decision may resolve the conflict for the bounded scope. **Fail:** A conflict is unresolved, precedence is invented during assessment, or a relationship proceeds despite mutually exclusive authoritative constraints.
Common failure modes	• Conflicting relationships are averaged, ignored, or selected case by case without an approved rule. • Source precedence is not governed. • Human resolution is not recorded. • Both conflicting assertions remain usable without disposition.
Remediation procedure	**Pattern references:** R-05 - Conflicting evidence; R-11 - Human adjudication **If conflicting relationships are averaged, ignored, or selected case by case:** apply an approved conflict-resolution or adjudication rule **If source precedence is not governed:** define and approve the source-precedence rule for the conflict class **If human resolution is not recorded:** convert the adjudication into a governed decision, mapping, rule, or exception record **If both conflicting assertions remain usable without disposition:** assign the appropriate disposition to the conflicting evidence until the conflict is resolved
Repeatable fix	Known conflict classes have versioned precedence, adjudication, or escalation rules and preserve the losing evidence for audit.
Controlled disposition	Disposition reference: D-05, Threshold, constraint, or conflict. Unresolved jurisdictional or authoritative conflict is Fail and normally Stop; do not invent precedence during assessment.
Example	CRM and Billing disagree on account ownership; the approved authority rule selects Billing for this scope and records the conflict.
Non-example	The pipeline silently chooses whichever source arrives last.
Authority and execution	**Authority:** Relationship or decision authority owns conflict-resolution precedence, adjudication, and exception decisions.
Retest	Reinspect the governing rule and the recorded resolution of every actual conflict affecting material reliance. Verify competent authority and bounded scope. Stop or Quarantined containment alone does not satisfy the resolution test.

EO-013: Relationship Constraints Are Applied

Prerequisites	Pass required: EO-011. Recorded result required: EO-012.
Specification requirement	Each material relationship path shall apply the recorded governance, usage, jurisdictional, and conflict-resolution constraints that govern the stated decision scope.
Why this control exists	A relationship may be valid in one context and invalid in another.
When this applies	When a material relationship is subject to domain, time, authority, source, privacy, policy, regulatory, contractual, risk, purpose, or similar constraints.
Evidence to inspect	Relationship path, applicable constraint/policy records, jurisdiction/precedence rule, evaluation evidence, exception/resolution record where applicable, and Gate Record.
Evidence sufficiency	The constraint evidence must identify every material domain, time, authority, source, privacy, policy, regulatory, contractual, risk, purpose, or similar constraint and show that the applicable constraints were evaluated for the relationship use. ***Insufficient:*** Documenting a constraint is not sufficient when the decision path does not actually apply it at the point where the relationship is used.
Assessment procedure	**1.** Inspect material relationships against required domain, time, authority, source, privacy, policy, regulatory, contractual, risk, and purpose constraints. **2.** Verify applicable constraints were actually evaluated, not merely documented.
Control-result determination	**Pass:** Every applicable constraint and resolved precedence rule is evaluated before reliance, prohibited paths are blocked, bounded exceptions are explicit, and unresolved authoritative conflict results in a failed control and a Stop Gate state unless competent authority has recorded a valid bounded resolution. **Fail:** A constraint is ignored, a prohibited path is used, or unresolved jurisdictional conflict is allowed to proceed.
Common failure modes	• Constraints are documented but not evaluated at use time. • Time validity is ignored. • Source or authority restrictions are lost during traversal. • Privacy, policy, contractual, or purpose constraints do not propagate with the relationship.

Remediation procedure	**Pattern references:** R-10 - Prohibited or out-of-scope use; R-06 - Threshold or rule failure **If relationship constraints are documented but not evaluated when the relationship is used:** apply the relevant constraints at the Gate or other controlled point of use **If time validity is ignored:** evaluate the relationship against its effective period before use **If source or authority restrictions are lost during traversal:** preserve and evaluate those restrictions throughout the relationship path **If privacy, policy, contractual, risk, or purpose constraints do not propagate with the relationship:** attach and enforce the applicable constraints wherever the material relationship is used
Repeatable fix	Constraints are attached to governed relationship types or paths and evaluated at the Gate.
Controlled disposition	***Disposition reference:*** **D-05, Threshold, constraint, or conflict.** Use this reference when a required relationship constraint has not been applied to the material use.
Example	A relationship may be used only for records effective during the contract period and from approved sources.
Non-example	A valid relationship is used outside its effective period because the join still works.
Authority and execution	**Authority:** Relationship steward applies constraints; relevant policy, privacy, risk, contractual, or domain authorities own their constraint rules.
Retest	Reevaluate the affected relationship against all applicable constraints. Confirm that required domain, time, authority, source, privacy, policy, regulatory, contractual, risk, and purpose constraints are actually applied at use time.

EO-014: Cross-Domain Semantic Compatibility Is Declared Where Applicable

Prerequisites	Pass required: EO-006.
Specification requirement	When a relationship crosses domains, functions, systems, or stewardship authorities, semantic compatibility shall be declared before stated use.
Why this control exists	Cross-domain use requires more than local application meaning.
When this applies	When a material relationship crosses business domains, functions, systems, or stewardship authorities.
Evidence to inspect	Semantic domain references, boundary rules, compatibility record, grain rule, authority/stewardship record, decision-scope mapping.
Evidence sufficiency	The cross-domain compatibility evidence must show the semantic domains and boundaries on both sides of the relationship, compatible grain, material overlap or disjointness rules, and the responsible cross-domain authority or stewardship process. ***Insufficient:*** Similar names, shared identifiers, or a technically valid connection are not sufficient when the two domains use different meanings or grains and no governed compatibility decision has been recorded.
Assessment procedure	**1.** Identify each material relationship that crosses business domains, functions, systems, or stewardship authorities. **2.** Verify the semantic domain and boundary on both sides of the relationship. **3.** Verify compatible grain, material overlap or disjointness rules, and the responsible cross-domain authority or stewardship process before stated use.
Control-result determination	**Pass:** Cross-domain relationships reference semantic domains, boundary rules, compatible grain, disjointness or overlap rules where material, and authority or stewardship process. **Fail:** Cross-domain relationships are relied on for stated use without compatibility evidence.
Common failure modes	• Cross-domain terms look similar but have different meanings or grain. • Stewardship boundaries are unclear. • Overlap or disjointness is assumed. • One domain imposes its local relationship semantics on another without agreement.

Remediation procedure	**Pattern references:** R-02 - Ambiguous meaning; R-05 - Conflicting evidence; R-04 - Missing authority **If cross-domain terms look similar but have different meanings or grains:** reconcile the meanings and grains before treating the relationship as compatible **If stewardship boundaries are unclear:** identify the accountable authorities in each domain and the joint decision process **If overlap or disjointness is assumed:** record the approved overlap, disjointness, or boundary rule **If one domain imposes its local relationship semantics on another without agreement:** obtain explicit cross-domain agreement on the relationship meaning and permitted use
Repeatable fix	Cross-domain relationships require a compatibility record and accountable cross-domain review.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when cross-domain semantic compatibility has not yet been established for the material relationship.
Example	Sales Account and Finance Customer are linked only after their different grains and boundary rules are reconciled for the scope.
Non-example	A relationship crosses domains because both sides use the word “customer,” with no compatibility evidence.
Authority and execution	**Authority:** Relevant domain stewards or authorities jointly establish compatibility; decision-scope owner approves use.
Retest	Reinspect each affected cross-domain relationship. Confirm that domain boundaries, compatible grain, material overlap or disjointness rules, and cross-domain authority or stewardship are now recorded and approved.

EO-015: Traversal Path Is Determinate Where Used

Prerequisites	Pass required: EO-011. Recorded result required: EO-006, EO-013, EO-014.
Specification requirement	A relationship traversal used as decision evidence shall return the same path result, or the same unresolved or exception result, when the inputs, rule set, threshold where used, version, and decision scope are unchanged.
Why this control exists	Decision-path reconstruction requires repeatable relationship traversal.
When this applies	When a relationship traversal path is relied on as decision evidence for stated use and repeated execution must yield a determinate path or governed unresolved outcome.
Evidence to inspect	Traversal rule and version, tested inputs, thresholds where used, path records, repeat-test results, scope reference, and exception record where applicable.
Evidence sufficiency	Repeat-test records hold inputs, rules, thresholds where used, versions, and scope unchanged and return the same path or the same governed unresolved or exception result. **Insufficient:** An explanation for different outcomes under unchanged conditions does not establish Pass. A consistently unresolved path does not establish permission for relationship use.
Assessment procedure	**1.** Replay the same material traversal with the same inputs, rule set, version, and decision scope. **2.** Verify repeated runs return the same path or the same unresolved or exception result, and investigate unexplained differences.
Control-result determination	**Pass:** Repeat tests using the same recorded inputs, rules, thresholds where used, versions, and scope return the same path result or the same unresolved or exception result. A repeatable unresolved result does not establish permission to use the relationship. **Fail:** Any different traversal outcome under the same inputs, rule set, threshold, version, and decision scope is Fail. A recorded explanation does not convert that failed determinism test into Pass; a changed rule, threshold, version, or scope is a different test case.
Common failure modes	• Traversal order is nondeterministic. • Eligible paths are selected differently under unchanged conditions. • Tie-breakers or required thresholds are unrecorded. • Graph or rule version is not captured. • An unresolved path is silently replaced with another path.

Remediation procedure	**Pattern references:** R-06 - Threshold or rule failure; R-11 - Human adjudication **If traversal order is nondeterministic:** define the ordering rule required to produce a repeatable path result **If equivalent eligible paths are selected differently across runs:** define the approved path-priority or tie-break rule **If tie-break logic is missing:** add and govern the tie-break condition **If the graph, rule, or traversal version is not captured:** record the version used for the assessed traversal **If an unresolved path is silently replaced with another path:** preserve a governed unresolved or exception outcome instead of substituting an unapproved path
Repeatable fix	Traversal execution records rule/version and uses deterministic selection or governed unresolved outcomes.
Controlled disposition	***Disposition reference:*** **D-06, Determinacy or repeatability.** Use this reference while traversal does not reproduce the same path, or the same governed unresolved or exception result, under the same governed conditions.
Example	Two equivalent paths are resolved by a documented priority rule, producing the same path on replay.
Non-example	A graph search returns different eligible paths while the recorded inputs, rules, thresholds, versions, and scope are unchanged. A later explanation does not make that test Pass.
Authority and execution	**Authority:** Traversal-rule owner governs deterministic path selection; ontology authority approves the rule for the scope. **Execution:** Traversal execution must preserve the input, rule or graph version, ordering or tie-break logic, and result needed for replay.
Retest	Repeat traversal with unchanged recorded inputs, rules, thresholds where used, versions, and scope. Compare outcomes, including unresolved or exception results. A changed configuration is a new test case; repeatability alone does not permit relationship use.

EO-016: Relationship Readiness State Is Declared

Prerequisites	Recorded result required: EO-010, EO-013, EO-015.
Specification requirement	Each material relationship shall have a readiness state for the stated decision scope.
Why this control exists	Relationship evidence requires a decision-scope disposition.
When this applies	When a material relationship is used in the decision path and therefore requires a scope-bound readiness disposition.
Evidence to inspect	Relationship readiness record, Gate Record, reason, responsible authority or approved rule reference, timestamp, review condition.
Evidence sufficiency	The relationship-readiness evidence must show the formal readiness state assigned to the material relationship for the stated decision scope and the supporting reason, authority or rule, timestamp, and review condition where required. ***Insufficient:*** Existence in an ontology, graph, catalog, or governed repository is not sufficient to establish that the relationship is in Proceed for the decision scope being assessed.
Assessment procedure	**1.** Inspect each material relationship used by the decision scope. **2.** Verify the readiness state is supported by Gate evidence, reason, authority or rule, timestamp, and review condition where required.
Control-result determination	**Pass:** The relationship is assigned Proceed, Caution, Stop, or Quarantined with reason, responsible authority or approved rule reference, timestamp, and review condition where required. **Fail:** A material relationship is used without a readiness state or the state is unsupported by evidence.
Common failure modes	• Relationship readiness is inferred from relationship existence. • State has no supporting Gate evidence. • Caution constraints are not recorded. • Readiness is out of date after relationship or scope change.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-08 - Material change or drift **If relationship readiness is inferred from the relationship merely existing:** evaluate the relationship through the applicable Gate and assign the resulting readiness state **If the readiness state has no supporting Gate evidence:** produce or link the Gate evidence that supports the state **If Caution is used without recording its constraints:** record the bounded-use conditions, authority, and review condition **If the readiness state is outdated after relationship or scope change:** reassess the affected relationship and issue a current state
Repeatable fix	Relationship readiness is a scope-bound governed record updated through Gate execution.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material relationship lacks a supported readiness state for the decision scope.
Example	A newly imported relationship remains Quarantined until provenance and vector controls are complete.
Non-example	A relationship is labeled Proceed simply because it exists in the ontology repository.
Authority and execution	**Authority:** The responsible decision-scope authority approves relationship readiness based on Gate evidence. An approved rule may execute or record the evaluation; the ontology steward remains accountable for the underlying relationship evidence.
Retest	Reinspect the readiness record for each affected material relationship. Confirm that the formal readiness state is supported by Gate evidence, reason, authority or rule, timestamp, and review condition where required.

EO-017: Ontology Change Triggers Forward Reassessment

Prerequisites	Pass required: CORE-023. Recorded result required: EO-016.
Specification requirement	Each material Extended Ontology change shall trigger impact assessment for active or prospective decision scopes that rely on the changed relationship artifact. Historical Gate and Conformance Records remain fixed to the ontology version that governed them.
Why this control exists	Relationship rules can invalidate decision paths previously allowed for stated use.
When this applies	When a material relationship type, orientation, path, vector criterion, constraint, provenance rule, or permitted/prohibited traversal rule changes.
Evidence to inspect	Ontology change/version record, impact rule, affected-scope list, readiness invalidation/reassessment record, replacement Gate/Conformance Record where required, and immutable historical references.
Evidence sufficiency	A material ontology change is versioned, affected active or prospective scopes are identified, and required invalidation or reassessment precedes new reliance. Replacement Gate or Conformance Records link to unchanged historical records. **Insufficient:** A version log alone does not establish impact handling when affected future use continues without required reassessment.
Assessment procedure	**1.** Inspect ontology change rules and a recent or test change to type, orientation, path, vector criteria, constraint, provenance, or path rules. **2.** Verify affected scopes receive impact analysis, Gate reassessment, and Conformance Record update.
Control-result determination	**Pass:** A material ontology change is versioned, affected active/prospective scopes are identified, prior readiness for new reliance is invalidated or reassessed as defined, and any replacement Gate/Conformance Record is linked to the prior record without rewriting it. **Fail:** Future reliance continues under a materially changed ontology without reassessment, or historical records are retroactively recalculated or overwritten merely because the ontology changed.
Common failure modes	• Relationship type or orientation changes without scope impact analysis. • Path-rule changes do not invalidate prior readiness or conformance determination. • Vector criteria change without reassessment. • Ontology version changes are recorded but not operationalized.

Remediation procedure	Apply forward-only impact assessment. Reassess affected active/prospective use; do not retroactively recalculate completed historical decisions solely because ontology changed.
Repeatable fix	Ontology version changes produce a repeatable affected-scope review and conformance-status update.
Controlled disposition	***Disposition reference:*** **D-04, Change or reassessment.** Use this reference after a material ontology change until affected decision scopes have been identified and reassessed.
Example	Changing a relationship from permitted to prohibited triggers reassessment of every path that traverses it.
Non-example	A relationship type is redefined but existing decisions previously allowed for stated use continue under the old meaning without review.
Authority and execution	**Authority:** Ontology owner governs the change; affected decision-scope owners authorize reassessment and Conformance Record updates. **Execution:** A material ontology change must identify affected decision scopes and route them to impact review and Gate reassessment.
Retest	Apply or inspect a representative material ontology change. Confirm that affected decision scopes are identified and the required impact analysis, Gate reassessment, and linked replacement Conformance Records are created.

10. AI Context Contract Controls

These cards apply when AI, machine inference, generated evidence, automation, or agents materially affect the decision path. The controls define how AI-assisted evidence and behavior are tested against governed context for the stated decision scope; they do not establish intrinsic model correctness.

Card boundary

The Specification requirement, Prerequisites, Evidence to inspect, and Pass/Fail text below reproduce DACS Specification v1.13. Sections 2 through 5 explain its global assessment and closure rules. Procedures, failure modes, remediation, and examples are informative guidance. Apply the exact Specification version governing the assessment; the catalog does not add criteria or override it.

AI-001: Binding AI Context Contract Exists

Prerequisites	Pass required: CORE-004.
Specification requirement	Each AI-assisted decision scope shall have a Binding AI Context Contract before AI outputs are relied on for material use.
Why this control exists	AI cannot be governed against vague intent. It requires a concrete context contract.
When this applies	Before AI-assisted evidence, recommendations, or actions are relied on for a material decision scope.
Evidence to inspect	Binding AI Context Contract with identifier, owner/authority, version, scope mapping, and references to the applicable taxonomy, ontology, identity, context, path, vector, Gate, drift, and evidence rules.
Evidence sufficiency	The Binding AI Context Contract must identify the governed semantic, identity, relationship, context, path, vector, Gate, drift, and evidence rules that apply to the AI-assisted decision scope, with the applicable references and version. ***Insufficient:*** A system prompt, retrieval configuration, tool list, model instruction, or architecture diagram is not sufficient by itself when the governed context contract does not bind the AI use to the required DACS evidence and control rules.
Assessment procedure	1. Retrieve the Binding AI Context Contract for the stated scope. 2. Verify identifier, owner/authority, version, and scope mapping. 3. Inspect references to every applicable taxonomy, ontology, identity, context, permitted/prohibited path, vector, Gate, drift, and evidence rule.
Control-result determination	**Pass:** The contract is identified, owned, versioned, and linked to the decision scope. It references applicable Extended Taxonomy, Extended Ontology, Business Identity rules, preserved context, permitted/prohibited paths, vector criteria, Gate criteria, drift rules, and evidence requirements. **Fail:** AI output is relied on for material use without a contract or the contract lacks required semantic, identity, relationship, context, Gate, or drift constraints.
Common failure modes	• AI use begins with prompts or retrieval but no Binding AI Context Contract. • Contract omits permitted or prohibited paths. • Taxonomy, ontology, identity, Gate, or drift references are out of date. • Contract owner or version is unclear.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-04 - Missing authority; R-12 - Automated or AI-assisted control **If AI use begins with prompts, retrieval, tools, or workflows but no Binding AI Context Contract exists:** create and version the Binding AI Context Contract before AI-assisted stated use **If the contract omits permitted or prohibited relationship or context paths:** add the required permitted and prohibited path rules **If taxonomy, ontology, identity, Gate, drift, or other referenced evidence is outdated:** update the contract references and reassess the affected AI-assisted scope **If the contract owner or version is unclear:** record the accountable owner and the applicable contract version
Repeatable fix	AI-enabled scopes invoke a standard contract record and change process before production or stated use.
Controlled disposition	***Disposition reference:*** **D-01, Missing prerequisite.** Use this reference when the AI-assisted decision scope lacks a complete Binding AI Context Contract.
Example	The contract for a claims assistant references approved concepts, identity rules, allowed relationship paths, prohibited paths, Gate criteria, and drift tests.
Non-example	A system prompt is treated as the entire context contract even though governed semantic, relationship, and evidence rules are absent.
Authority and execution	**Authority:** The AI decision-scope owner is accountable for the Binding AI Context Contract. Referenced semantic, identity, ontology, risk, and other component authorities remain accountable for their respective components.
Retest	Reinspect identifier, owner/authority, version, scope mapping, and every applicable component reference. Confirm the contract governs this AI-assisted use and its effective versions.

AI-002: AI Inputs Conform to the Semantic Contract

Prerequisites	Pass required: AI-001.
Specification 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.
Why this control exists	Material information supplied to AI must be governed and traceable to the applicable Semantic Contract for the stated decision scope.
When this applies	When a material AI input, retrieved field, prompt variable, tool return, document excerpt, feature, or context element influences the decision path.
Evidence to inspect	AI input record, retrieval/prompt/tool context record, taxonomy reference, identity reference where applicable, physical attribution where required, Gate Record, decision-scope mapping.
Evidence sufficiency	The AI-input evidence must show how every material input or context element maps to the applicable Semantic Contract, including approved taxonomy, Business Identity where applicable, physical attribution where required, context rule, and Gate status. ***Insufficient:*** Successful retrieval, an authorized API response, a prompt variable, or a document excerpt is not sufficient merely because it was available to the AI. The input must also be governed and eligible for this decision scope.
Assessment procedure	**1.** Enumerate material AI inputs, including retrieved fields, prompt-supplied variables, tool-returned values, document excerpts, and context elements. **2.** Verify that each material AI input or context element maps to approved Semantic Contract evidence, identity where applicable, physical attribution where required, context rules, and Gate status.
Control-result determination	**Pass:** Each material AI input maps to approved taxonomy, Business Identity where applicable, physical attribution where required, context rule, and Gate readiness state for the decision scope. **Fail:** Material use of input or context that is unmapped, ambiguous, prohibited, unreviewed, or lacks the required evidence and readiness for the stated use.
Common failure modes	• Retrieved context is assumed valid because retrieval succeeded. • Prompt variables use local meanings. • Tool-returned values lack physical attribution. • Unreviewed documents enter context. • Input Gate status is ignored.

Remediation procedure	**Pattern references:** R-01 - Missing evidence; R-02 - Ambiguous meaning; R-07 - Unsupported discovery **If retrieved context is assumed valid merely because retrieval succeeded:** validate the retrieved evidence against the applicable Semantic Contract, identity, attribution, context, and Gate rules **If prompt-supplied variables use local or ambiguous meanings:** map the material variables to approved governed concepts before use **If tool-returned values lack required physical attribution:** record the source-level evidence needed to identify and test those values **If unreviewed documents enter AI context:** keep the documents Quarantined or route them through the applicable controls before material use **If input Gate status is ignored:** enforce the recorded input readiness state before the AI-assisted decision uses the evidence
Repeatable fix	Retrieval, prompts, tools, and features emit input-evidence records that can be checked before stated use.
Controlled disposition	***Disposition reference:*** **D-02, Unresolved governed evidence.** Use this reference when a material AI input or context element is not yet governed and eligible under the applicable Semantic Contract.
Example	A retrieved customer-status field maps to the approved concept, Business Identity, source field, and Gate state.
Non-example	An agent uses an unlabeled tool response because it was returned by an authorized API.
Authority and execution	**Authority:** The AI application or workflow owner controls how inputs enter the process. Semantic, identity, and source authorities govern their respective evidence; the responsible decision-scope authority approves input eligibility for stated use.
Retest	Recheck each affected material AI input or context element. Confirm that it maps to approved Semantic Contract evidence, Business Identity where applicable, physical attribution where required, context rules, and Gate status for the decision scope.

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

Prerequisites	Recorded result required: ET-016, AI-001.
Specification 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.
Why this control exists	AI outputs must use governed business language when they support Defensible Analytics.
When this applies	When an AI-assisted output introduces or uses a material business term, classification, or concept.
Evidence to inspect	AI output record, term extraction or mapping record, taxonomy references for mapped terms, and Quarantined/review records identifying unmapped or unreviewed terms where applicable.
Evidence sufficiency	The output-term evidence must show that every material AI-generated or AI-used term, classification, or concept maps to an approved Extended Taxonomy node for the decision scope, or is explicitly routed to Quarantined review before material use. ***Insufficient:*** A generated label or classification is not sufficient because it sounds reasonable, resembles an approved term, or was reviewed informally. Its governed taxonomy mapping or Quarantined status must be recorded.
Assessment procedure	**1.** Inspect material terms, classifications, and concepts in AI-assisted outputs. **2.** Verify that each material term, classification, or concept maps to an approved Extended Taxonomy node for the decision scope or is assigned Quarantined before material use.
Control-result determination	**Pass:** All material AI output terms map to approved taxonomy nodes for the decision scope or are routed as Quarantined evidence for review. **Fail:** The output uses material terms, classifications, or concepts that are unmapped, ambiguous, prohibited, or unreviewed as if ready for stated use.
Common failure modes	• Generated labels are accepted without governed taxonomy evidence. • Synonyms are mapped without approved taxonomy evidence. • Novel concepts enter material outputs without Quarantined status. • Output review checks wording but not governed meaning.

Remediation procedure	**Pattern references:** R-02 - Ambiguous meaning; R-07 - Unsupported discovery **If generated labels or concepts are accepted without governed taxonomy evidence:** map them to approved Extended Taxonomy nodes or assign them Quarantined before material use **If synonyms are mapped without approved taxonomy evidence:** use the governed synonym or alias record rather than name similarity **If novel concepts enter material outputs without Quarantined status:** route them to taxonomy review as candidate evidence **If output review checks wording but not governed meaning:** evaluate the material term against the approved business meaning and decision-scope boundary
Repeatable fix	Output validation extracts material terms and checks them against the governed taxonomy or a stewardship queue.
Controlled disposition	***Disposition reference:*** **D-03, Ungoverned candidate evidence.** Use this reference for AI-generated or AI-used terms and classifications that lack an approved taxonomy mapping.
Example	The model generates “Dormant Customer,” which is not approved, so the classification remains Quarantined until reviewed.
Non-example	A new model-generated category is added to an executive report because it sounds reasonable.
Authority and execution	**Authority:** Taxonomy authority governs output terms and classifications. The AI workflow owner implements the required mapping or Quarantined routing.
Retest	Reinspect the affected AI output terms, classifications, and concepts. Confirm that each maps to an approved Extended Taxonomy node for the scope or remains Quarantined before material use.

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

Prerequisites	Recorded result required: EO-016, AI-001.
Specification 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.
Why this control exists	AI relationship assertions must be tested, not accepted because they are plausible.
When this applies	When an AI-assisted output asserts, infers, or relies on a material relationship.
Evidence to inspect	AI output record, relationship extraction or mapping record, applicable ontology, vector, orientation, and path-rule references for governed relationships, and Quarantined/review records for unsupported or unmapped relationships where applicable.
Evidence sufficiency	The output-relationship evidence must show that every material relationship asserted or used by AI maps to approved Extended Ontology evidence, including the required relationship type, orientation, vector criteria, and path rules, or is routed to Quarantined review. ***Insufficient:*** A model citation, high confidence score, plausible explanation, or retrieved supporting text is not sufficient to establish an AI-generated relationship as ready for stated use when the applicable ontology controls have not been satisfied.
Assessment procedure	**1.** Inspect material relationships asserted or used by AI-assisted outputs. **2.** Verify that each material relationship maps to approved Extended Ontology evidence, permitted orientation, vector criteria, and path rules, or is assigned Quarantined before material use.
Control-result determination	**Pass:** 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:** The AI output asserts or depends on an unmapped, prohibited, unsupported, or unreviewed relationship as if ready for stated use.
Common failure modes	• AI infers relationships not present in the approved ontology. • Orientation is wrong or absent. • Vector and path criteria are skipped. • A plausible association is treated as ready for stated use because the model is confident.

Remediation procedure	**Pattern references:** R-07 - Unsupported discovery; R-06 - Threshold or rule failure **If AI asserts a relationship that is not present in the approved ontology:** map it to governed relationship evidence or keep it Quarantined as a candidate relationship **If relationship orientation is wrong or missing:** correct and approve the orientation before material use **If vector criteria or path rules were skipped:** evaluate the applicable relationship vector and permitted-path controls **If model confidence is being used as a substitute for governed relationship evidence:** apply the Extended Ontology controls regardless of the model confidence score
Repeatable fix	Output validation identifies material relationship assertions and checks them against governed ontology evidence.
Controlled disposition	***Disposition reference:*** **D-03, Ungoverned candidate evidence.** Use this reference for AI-generated or AI-used relationships that lack approved Extended Ontology evidence.
Example	The model asserts Supplier depends on Component; the assertion is Quarantined because no approved relationship evidence exists.
Non-example	A generated relationship is accepted as ready for stated use because the model cites supporting text.
Authority and execution	**Authority:** Ontology authority governs output relationships. The AI workflow owner implements the required relationship validation or Quarantined routing.
Retest	Reinspect the affected AI output relationships. Confirm that each maps to approved Extended Ontology evidence, permitted orientation, vector criteria, and path rules, or remains Quarantined before material use.

AI-005: AI Inference and Output Drift Are Tested

Prerequisites	Pass required: AI-001. Recorded result required: AI-002, AI-003, AI-004.
Specification 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.
Why this control exists	AI behavior can deviate from governed meaning and relationship rules. Drift must be testable against the contract.
When this applies	When AI can generate or infer material terms, classifications, relationships, context use, recommendations, or actions whose behavior can drift from the Binding AI Context Contract.
Evidence to inspect	Drift test record, AI output sample or production record, contract reference, applicable taxonomy/ontology references, drift result, and recorded readiness disposition.
Evidence sufficiency	The drift evidence must show that the required tests compare material AI terms, classifications, relationships, context use, recommendations, or actions with the correct Binding AI Context Contract version and record the tested item, result, timestamp, and responsible rule or authority. ***Insufficient:*** Model-performance monitoring alone is not sufficient when it does not test whether AI behavior has drifted from the governed semantic, relationship, context, or action rules in the Binding AI Context Contract.
Assessment procedure	1. Retrieve the required drift-test rules and records. 2. Confirm tests compare material terms, classifications, relationships, orientations, context use, or actions with the effective Binding AI Context Contract. 3. Verify test ID, contract version, tested output/action, result, timestamp, and responsible authority or approved rule. 4. Trace detected violations to their separate recorded consequence; completing a test does not authorize violating evidence.
Control-result determination	**Pass:** 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:** AI output is relied on for material use without required drift testing where AI may generate or infer material terms, classifications, relationships, context, or actions.

Common failure modes	• Only model-performance drift is monitored. • Semantic or relationship drift is not tested. • Tests use the wrong contract version. • Drift samples are not tied to the decision scope. • Violations do not update readiness.
Remediation procedure	**Pattern references:** R-08 - Material change or drift; R-06 - Threshold or rule failure; R-12 - Automated or AI-assisted control **If only model-performance drift is monitored:** add tests for the semantic, identity, relationship, context, or other contract conditions that can affect the stated decision scope **If semantic or relationship drift is not tested:** define and execute the missing contract-alignment drift checks **If drift tests use the wrong Binding AI Context Contract version:** bind the test to the version effective for the outputs or actions being assessed **If drift samples are not tied to the decision scope:** select and record samples that represent the stated decision scope and material AI behavior **If a detected violation does not update readiness or trigger a governed consequence:** route the violation to the required disposition, remediation, exception, or contract-review path
Repeatable fix	A repeatable evaluation process samples or tests outputs at the required cadence and preserves test evidence.
Controlled disposition	***Disposition reference:*** **D-04, Change or reassessment.** Use this reference when required AI drift testing has not been performed against the applicable Binding AI Context Contract version.
Example	A scheduled contract-alignment test records a deprecated classification. A linked Gate holds the affected output under Quarantined or Stop, or permits bounded Caution only through a valid authorizing exception.
Non-example	Model quality metrics are monitored, but no test checks semantic or relationship drift against the governed contract.
Authority and execution	**Authority:** Binding AI Context Contract owner defines required drift tests; AI operations or workflow owners execute and preserve test evidence. **Execution:** Drift testing must compare the tested output or action with the correct Binding AI Context Contract version and preserve the test result.
Retest	Run the required drift test against the correct Binding AI Context Contract version. Confirm that the tested terms, relationships, context use, recommendations, or actions produce the recorded expected result or a governed violation disposition.

AI-006: AI Context Contract Violation Has Consequence

Prerequisites	Pass required: AI-001. Recorded result required: CORE-014, AI-005.
Specification requirement	Each material violation of the Binding AI Context Contract shall produce a Gate Record with a resulting readiness state before the affected output, context, relationship, or action is relied on for stated use. Remediation, exception handling, or contract review may be required in addition to the Gate state; they do not substitute for it.
Why this control exists	A binding contract is not binding unless violations have consequence.
When this applies	When a material Binding AI Context Contract violation is detected.
Evidence to inspect	Violation record, Gate Record, resulting readiness state, approved constrained-use exception where Caution permits use, remediation record where required, and contract-review record where required.
Evidence sufficiency	Every material violation has a recorded Gate consequence before affected reliance: Stop, Quarantined, or Caution with a valid exception explicitly authorizing bounded use. Required remediation or contract review is additional evidence. **Insufficient:** Logging, alerting, remediation, or contract review without the required Gate state does not establish the consequence.
Assessment procedure	1. Identify each material contract violation and its affected evidence or action. 2. Retrieve the violation record and linked Gate determination. 3. Verify Stop or Quarantined prevents material reliance, or Caution has an explicit valid authorizing exception and actual use stays within its bounds. 4. Verify required remediation or contract-review records without treating them as substitutes for the Gate state.
Control-result determination	**Pass:** Each material violation is recorded and results in Stop or Quarantined, or in Caution with an approved constrained-use exception that explicitly authorizes the bounded use; any required remediation or contract-review action is also recorded. **Fail:** A material violation has no Gate readiness state, affected evidence or action proceeds under Stop or Quarantined, or Caution is used without an explicit approved constrained-use exception.
Common failure modes	• Violations are logged but have no control consequence. • Repeated exceptions become normal operation. • Violation severity is not tied to Gate disposition. • Contract review occurs without preserving the original violation evidence.

Remediation procedure	**Pattern references:** R-06, R-10, R-12 **If a violation is only logged or alerted:** produce the required Gate determination before affected reliance. **If Caution lacks explicit use authority:** prevent the use or obtain a valid prospective bounded exception. **If repeated exceptions have become normal operation:** reassess the contract or design while preserving failed findings and exception history. **If contract review replaces consequence or erases history:** preserve the original violation and create linked Gate and review records.
Repeatable fix	Violation handling is encoded in workflow or operating procedure and produces a Gate/readiness update.
Controlled disposition	***Disposition reference:*** **D-05, Threshold, constraint, or conflict.** Use this reference when a material AI context-contract violation has occurred and requires a governed consequence or exception.
Example	Use of a prohibited relationship path causes Stop and creates a remediation case.
Non-example	A violation is logged for monitoring but the output remains marked ready for stated use with no consequence.
Authority and execution	**Authority:** The responsible decision-scope or risk authority defines consequences for material contract violations and approves any constrained-use exception. **Execution:** A material contract violation must automatically or procedurally invoke a recorded consequence rather than remain a monitoring-only event.
Retest	Trace each affected violation to its Gate state before reliance. Confirm containment under Stop or Quarantined, or authorized bounded use under Caution. Verify any additional required remediation or review records.

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

Prerequisites	Pass required: CORE-017, AI-001.
Specification requirement	Each AI-assisted decision scope shall identify the point, process, or mechanism that enforces context eligibility before stated use. A high-frequency path may use a Cached Gate Policy State only when that state was produced by a prior full evaluation and is explicitly bound to decision scope, permitted action class, authority, policy/control versions, constraints, expiration, and invalidation triggers.
Why this control exists	Delivered context can be stale, unauthorized, semantically ambiguous, or outside the stated scope. A declared control point is required to test eligibility before material use.
When this applies	When context is supplied to AI and eligibility must be enforced before the resulting output is treated as ready for stated use.
Evidence to inspect	Context Enforcement Point/equivalent-control record, Semantic Contract/Gate criteria, scope/action-class mapping, authority, policy/control versions, constraints, Cached Gate Policy State and expiration/invalidation triggers where used, Equivalence Rule where used, execution evidence, and Buffered Gate Capture policy/evidence where applicable.
Evidence sufficiency	The declared enforcement point has the required identity, authority, version, scope, contract/Gate references, context rules, and pre-use execution evidence. A claimed equivalent is supported by an Equivalence Rule. Cached policy and buffering are conditional evidence paths with their own required bounds. **Insufficient:** A named retrieval layer, stale cache, or promised later audit does not establish context eligibility enforcement before use.
Assessment procedure	1. Inspect enforcement-point identifier, owner/authority, version, scope, contract, Gate criteria, and permitted/prohibited context rules. 2. Test eligible, ineligible, and bypass attempts; inspect evidence that enforcement precedes use. 3. For a claimed equivalent, inspect the recorded Equivalence Rule. 4. If cached policy is used, trace its prior full evaluation and verify scope/action class, authority, versions, constraints, expiry, and invalidation at runtime. 5. If buffering is used, verify complete pre-action capture and bounded durable persistence under Section 9.1.

Control-result determination	**Pass:** The Context Enforcement Point or equivalent control has an identifier, owner/authority, version, scope mapping, Semantic Contract reference, Gate criteria, permitted/prohibited context rules, and evidence of enforcement before use. Any claimed equivalent has a recorded Equivalence Rule. If Cached Gate Policy State is used, it must be current, bound to the scope and action class, versioned, authorized, constrained, unexpired, and invalidated on declared triggers. If buffering is used, its pre-action capture and durable persistence must satisfy Section 9.1. **Fail:** Use occurs before enforcement, a cached state is stale, expired, broader than the action, lacks an invalidation trigger, or is created after observing the action result.
Common failure modes	• Context is delivered through retrieval, connected tools, APIs, or other context-delivery mechanisms but no point enforces eligibility. • Enforcement occurs after output generation. • The control is not linked to the current contract or scope. • Prohibited context can bypass the enforcement path.
Remediation procedure	**Pattern references:** R-12 - Automated or AI-assisted control; R-10 - Prohibited or out-of-scope use; R-09 - Missing execution record **If context can enter through retrieval, tools, APIs, or other mechanisms without an eligibility check:** declare the Context Enforcement Point or equivalent control that evaluates context before stated use **If enforcement occurs only after output generation or action:** move the eligibility check to the point before the material output or action can rely on the context **If the enforcement control is not linked to the current contract or decision scope:** bind it to the applicable Semantic Contract or Binding AI Context Contract, Gate criteria, and decision-scope rules **If prohibited context can bypass the declared enforcement path:** close the bypass and ensure every material context-delivery path is subject to the declared control
Repeatable fix	The enforcement point is named, versioned, testable, and produces evidence of the rule applied.
Controlled disposition	***Disposition reference:*** **D-01, Missing prerequisite.** Use this reference when no declared control enforces context eligibility before stated AI use.
Example	A retrieval gateway checks context eligibility and records the contract and Gate rule before context reaches the decision step.

Non-example	The architecture diagram shows a retrieval layer, but no control determines whether retrieved context is permitted for the decision scope.
Authority and execution	**Authority:** AI workflow owner implements the Context Enforcement Point; Binding AI Context Contract owner defines the eligibility rules it must enforce. **Execution:** The declared Context Enforcement Point or equivalent control must operate before stated use and preserve which eligibility rule was applied.
Retest	Test pre-use enforcement and bypass prevention against the recorded scope and rules. Verify equivalent-control evidence, cached-policy bounds and invalidation, and buffered completion where those paths are used.

AI-008: Agentic Action Authority Is Declared Where AI Acts

Prerequisites	Pass required: AI-001.
Specification requirement	When AI or automation performs an Agentic Action, the decision scope shall declare the authority under which that action is permitted. An Agentic Action is an automated operation that changes or commits state outside the isolated reasoning workspace, or releases/publishes a material recommendation, instruction, message, approval, decision, or output for downstream reliance. Internal reasoning steps that neither change external state nor expose a material output for reliance are not Agentic Actions.
Why this control exists	An agent that acts requires scoped authority and accountability.
When this applies	When automation changes external state or releases a material recommendation/message/output for downstream reliance. Internal reasoning that remains isolated and is not released for reliance is not an Agentic Action.
Evidence to inspect	Agent identity, authority record, permitted action/action-class record, tool/API/channel permissions, downstream-reliance boundary, escalation rule, and Gate-before-action requirement.
Evidence sufficiency	The authority evidence must identify the agent or automation, the delegated business authority, allowed action class, allowed tools or APIs, escalation rule, and Gate-before-action requirement where applicable, and those limits must align with the permissions actually available to the agent. ***Insufficient:*** Technical permission to call an API, access a tool, or execute a workflow is not sufficient evidence that the agent has business authority to recommend or perform the material action.
Assessment procedure	1. Identify material external state changes and releases for downstream reliance, including recommendations and messages. 2. Inspect agent identity, delegated business authority, permitted action class, tools/APIs/channels, reliance boundary, escalation, and Gate-before-action requirements. 3. Compare declared limits with actual permissions. Internal reasoning is excluded only when it neither changes external state nor releases material output for reliance.

Control-result determination	**Pass:** Agent identity, delegated authority, permitted action class, allowed tools/APIs/channels, downstream-reliance boundary, escalation rule, and Gate-before-action requirement are recorded for every material Agentic Action. **Fail:** A state-changing or externally released material output occurs without declared authority, or a material recommendation is misclassified as an internal reasoning step to avoid Gate control.
Common failure modes	• Technical API permission is treated as business authority. • Agent identity is shared or ambiguous. • Allowed action class is too broad. • Escalation rule is missing. • Recommendation authority and execution authority are conflated.
Remediation procedure	**Pattern references:** R-04 - Missing authority; R-10 - Prohibited or out-of-scope use; R-12 - Automated or AI-assisted control **If technical API permission is being treated as business authority:** record the delegated business authority that permits the agent to perform the material action **If agent identity is shared or ambiguous:** assign a stable agent identity that can be linked to the delegated authority and execution trace **If the allowed action class is too broad:** narrow the authorized action class to the specific material actions the agent may perform **If the escalation rule is missing:** define when and to whom the agent must escalate instead of acting **If recommendation authority and execution authority are conflated:** separate the authority to recommend from the authority to execute a material action
Repeatable fix	Agent authorization is expressed as a governed, versioned authority record enforced by workflow or access policy.
Controlled disposition	***Disposition reference:*** **D-01, Missing prerequisite.** Use this reference when an agent or automation lacks recorded business authority and action boundaries for a material action.
Example	An invoice agent may recommend holds up to a defined class but must escalate payment release decisions.
Non-example	An agent can call any connected business API because the API credentials permit it.

Authority and execution	**Authority:** Business or operational authority delegates agent actions; technical permission alone is not business authority. **Execution:** Technical permission must be constrained to the recorded delegated action authority and escalation rules.
Retest	Inspect the affected material action classes, including externally released recommendations or messages. Verify declared business authority, action/tool/channel limits, downstream-reliance boundary, escalation, and Gate requirements against actual permissions.

AI-009: Material Agentic Action Requires Gate-Before-Action

Prerequisites	Pass required: CORE-016, AI-007, AI-008.
Specification requirement	Each material Agentic Action shall be evaluated by the applicable pre-action Gate synchronously before execution or release for downstream reliance. A valid Cached Gate Policy State may supply the pre-authorized policy decision when the runtime Gate synchronously verifies that the action is within the cached scope, action class, authority, constraints, versions, expiration, and invalidation state. Proceed permits the action. Caution permits only the explicitly authorized constrained action. Stop and Quarantined prohibit action. Compensating action may supplement, but shall not replace, pre-action authorization for irreversible actions.
Why this control exists	Low-latency execution may use precompiled policy state, but the action itself still requires synchronous verification against current authorized policy before it occurs.
When this applies	When an AI agent or automated workflow can execute a material action whose authority depends on a pre-action Gate.
Evidence to inspect	Pre-action Gate Record or Buffered Gate Capture, Cached Gate Policy State where used, decision scope/action class, authority, policy/control versions, constraints, expiration/invalidation status, readiness validity, execution trace link, persistence evidence, reversibility/compensating-action authorization where applicable, and action result.
Evidence sufficiency	Evidence establishes synchronous Gate determination and complete capture before each material action or release. Proceed or a valid explicitly authorizing Caution governs the exact action. Where permitted, delayed durable persistence has a declared interval and linked completion evidence. **Insufficient:** An exception without a pre-action Gate, later approval, partial capture, stale cache, or post-action rollback does not establish Gate-before-action.

Assessment procedure	1. Compare Gate determination/capture time with the material action or release; inspect causal-order evidence where needed. 2. Verify Proceed or explicitly authorizing Caution, current authority, scope/action class, constraints, and validity. 3. If cached policy is used, verify the runtime checked its effective versions, expiry, invalidation, and bounds synchronously. 4. If buffering is used, verify complete pre-action capture and durable completion within the declared interval. Assess completion when evidence exists or the deadline expires, not in advance. 5. Verify rollback or compensation applies only to a predeclared reversible or compensable class and never replaces pre-action authority for irreversible action.
Control-result determination	**Pass:** Gate logic completes before action or release; a current full evaluation or valid Cached Gate Policy State governs the exact action; the state is Proceed or an explicitly authorizing Caution; authority is valid; readiness and cached policy remain valid; and the complete pre-action determination is captured. Where buffering is used, the capture shall be durably persisted within the declared interval. This completion criterion is assessed under Section 9.1 and shall not be claimed as Pass before persistence completes. Any rollback or compensating mechanism is used only for an action class predeclared as reversible or compensable. **Fail:** Action before Gate evaluation, stale/invalid cached policy, Stop/Quarantined execution, unauthorized Caution, invalid authority, expired readiness, missing pre-action capture, missed persistence deadline, or reliance on post-action rollback as authorization for an irreversible action.
Common failure modes	• Action executes before pre-action Gate. • Cached policy is stale, expired, or broader than the action. • Stop/Quarantined action proceeds. • Caution lacks explicit action authorization. • Rollback is used as a substitute for pre-authorization of an irreversible action.

Remediation procedure	**Pattern references:** R-09 - Missing execution record; R-10 - Prohibited or out-of-scope use; R-12 - Automated or AI-assisted control **If the agent acts before the Gate and is reviewed afterward:** block the material action until the required Gate result exists **If the Gate evidence or authorization is outdated or belongs to another scope:** validate that the Gate evidence is current and bound to the same decision scope and action **If an exception is created only after execution:** require the authorized constrained-use exception before the action occurs **If an asynchronous workflow can proceed before control evaluation is complete:** add an execution barrier so the action cannot proceed until the Gate has completed
Repeatable fix	The workflow enforces synchronous Gate authorization and complete capture before material action. Permitted buffering has bounded persistence and separate completion checks; exceptions do not bypass the Gate.
Controlled disposition	***Disposition reference:*** *D-01, Missing prerequisite.* *Use this reference when pre-action Gate authority, valid policy, complete capture, or required persistence completion cannot be established. Record the actual failure and apply the Gate and runtime-failure rules.*
Example	A payment hold is executed only after the scope-bound Gate records the required control results.
Non-example	The agent executes first and relies on audit logs to review whether it should have acted.
Authority and execution	**Authority:** The responsible action authority authorizes the exact material use before it occurs. Caution requires a valid bounded exception. **Execution:** Synchronously determine and capture Gate readiness before action or release. An exception does not replace the Gate. Verify permitted durable persistence later within its declared interval.
Retest	Inspect controlled action tests for permitted and blocked states, invalid authority, expired or invalidated cache, and buffering where used. Verify authorization and complete capture before action, durable persistence within the bound, and no premature Pass for completion criteria.

AI-010: Decision Execution Trace Is Recorded Where AI or Automation Is Material

Prerequisites	Pass required: CORE-012. Recorded result required: CORE-013, AI-009.
Specification requirement	Each material AI-assisted or automated decision path shall record a Decision Execution Trace sufficient to establish what actually executed, including historical model limitations where the original provider/model version may later become unavailable.
Why this control exists	Technical execution logs may supply useful evidence, but defensibility requires the decision-scope evidence defined by applicable DACS controls.
When this applies	When AI or automation materially affects a recommendation, decision, routing step, or action that must later be reconstructed.
Evidence to inspect	Decision Execution Trace, request/actor/input/context, Gate reference, tools/APIs, model/provider/process/version and available material configuration, output/action, time/causal-order evidence, DACS version, conformance/exception state, buffered persistence evidence where applicable, and historical-model availability/reproducibility status.
Evidence sufficiency	Trace must identify provider/model/process version and available material configuration. If the original proprietary model later becomes unavailable, preserve contemporaneous execution evidence and state that original-model execution is not reproducible; a newer model is comparison only.
Assessment procedure	1. Select executions within a defined assessment population and retrieve their contemporaneous Decision Execution Traces. 2. Verify request, actor/agent, inputs/context, concepts, applicable relationship paths, Gate/readiness, tools/APIs, model/provider/process identity and versions, and available material configuration. 3. Verify output/action, timestamp/causal sequence, DACS version, and conformance/exception state. 4. Where the original model is unavailable, verify contemporaneous support and explicit non-reproducibility; a newer run is comparison only. 5. Inspect buffered-persistence evidence where applicable.

Control-result determination	**Pass:** The trace includes request, actor/agent, input/context, material concepts, relationship paths where applicable, Gate Records/readiness states, tools/APIs, model/provider/process identifier and version where applicable, material parameters/configuration where available, output/action, timestamp/causal sequence evidence, DACS normative version, and conformance/exception state. If the exact historical model later becomes unavailable, the trace must retain contemporaneous evidence sufficient to establish the execution and explicitly mark original-model execution as not reproducible; a newer model result is comparison evidence only. **Fail:** Material AI/automation execution cannot be reconstructed from contemporaneous trace evidence, model/provider/version identity is missing where material, or a newer model is represented as reproduction of an unavailable historical model.
Common failure modes	• Only prompts and responses are logged. • Retrieved context or tool calls are missing. • Model, process, or rule version is absent. • Agent identity is unknown. • Gate results and exception state cannot be reconstructed.
Remediation procedure	**Pattern references:** R-09 - Missing execution record; R-12 - Automated or AI-assisted control **If only prompts and responses are logged:** extend the Decision Execution Trace to the other material execution evidence required by the decision path **If retrieved context or tool calls are missing:** capture the material context sources, tool calls, APIs, and returned values needed for reconstruction **If the model, process, rule, or contract version is absent:** record the versions that governed the execution **If the actor or agent identity is unknown:** record a stable identity for the person, process, or agent that initiated or executed the material step **If Gate results, readiness, or exception state cannot be reconstructed:** link the trace to the relevant Gate, disposition, and conformance or exception evidence
Repeatable fix	Execution logging uses a structured trace schema linked to the decision scope and evidence records.
Controlled disposition	***Disposition reference:*** **D-01, Missing prerequisite.** Use this reference when a material AI-assisted or automated execution cannot be reconstructed from a Decision Execution Trace.

Example	An agent action can be reconstructed from request through tool calls, governed context, Gate result, model version, and final action.
Non-example	Only the final AI response is saved; the inputs, context, tools, and Gate results are unavailable.
Authority and execution	**Authority:** AI or automation owner ensures execution traces exist; evidence custodians preserve them for reconstruction and review. **Execution:** The Decision Execution Trace must capture the material inputs, context, tools, versions, Gates, output or action, and state needed for reconstruction.
Retest	Reconstruct the affected execution from contemporaneous trace evidence. Verify every required field, effective version, causal sequence, historical-model limitation, and applicable persistence evidence. If historical evidence is unprovable, a new run does not repair the old claim.

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

Prerequisites	Recorded result required: AI-002, AI-003, AI-004, AI-005, AI-006, AI-009, AI-010.
Specification requirement	AI-generated evidence shall be governed before material reliance. The applicable Gate shall either permit use within recorded authority and conditions or prevent use. Authorized constrained use under Caution does not establish full decision-scope conformance or change another control result from Fail to Pass.
Why this control exists	AI may produce useful candidates. This control verifies that their use follows the recorded Gate decision. A Pass for correct containment or constrained use does not mean the candidate evidence satisfies every other requirement or that the decision scope is conformant.
When this applies	When AI-generated evidence is held, released, or proposed for material reliance within the stated decision scope.
Evidence to inspect	AI-generated evidence record, applicable control results, Gate Record and readiness validity, recorded use or containment evidence, authority and enforced constraints, and exception/remediation records where applicable.
Evidence sufficiency	Evidence compares actual use or containment with the recorded Gate state, scope, authority, validity, and enforced constraints. Proceed use stays within its permitted scope. Caution use has a valid authorizing exception. Stop, Quarantined, or unauthorized Caution prevents reliance. **Insufficient:** A recorded disposition without matching actual handling, informal human review, production use, or plausible output does not establish this control's Pass. Correct containment does not make other failed controls Pass.
Assessment procedure	1. Identify the generated items within the stated assessment population and retrieve their applicable results, Gate, authority, and holding/use records. 2. Under Proceed, compare actual use with permitted scope and validity. 3. Under Caution, verify an authorizing exception and actual compliance with its bounds; without use authority, verify reliance is prevented. 4. Under Stop or Quarantined, verify material reliance is prevented. 5. Preserve failed prerequisite results and distinguish handling Pass from full scope conformance.

Control-result determination	**Pass:** Actual handling follows the recorded Gate decision. Under Proceed, use remains within the permitted scope and validity conditions. Under Caution, use occurs only within a valid authorizing exception and its bounds. Under Stop or Quarantined, material reliance is prevented. Caution without authority for the proposed use also prevents that use. **Fail:** Required control results, Gate evidence, authority, or use constraints cannot be established; material reliance occurs under Stop or Quarantined; Caution use lacks a valid authorizing exception or exceeds its bounds; or permitted use exceeds the recorded scope or validity conditions. A failed prerequisite remains Fail.
Common failure modes	• Actual use exceeds the Gate's scope, validity, or constraints. • Stop or Quarantined evidence enters material reliance. • Caution is treated as permission without a valid authorizing exception. • A handling Pass is presented as proof that every control passed. • Generated evidence loses provenance or enforced bounds during reuse.
Remediation procedure	**Pattern references:** R-07, R-10, R-12, R-09 **If use violates Stop or Quarantined:** prevent reliance and preserve the finding. **If Caution lacks authority or exceeds bounds:** prevent that use or obtain a valid prospective bounded exception and new Gate determination. **If Proceed use exceeds scope or validity:** block affected use and reassess the proposed scope. **If disposition records do not match actual handling:** correct enforcement and preserve linked use or containment evidence. **If provenance or constraints are lost in reuse:** restore verifiable links and enforce the bounds through the receiving path. **If handling Pass is presented as full conformance:** correct the claim while retaining every other control's actual result.
Repeatable fix	Generated evidence retains provenance, recorded Gate bounds, and inspectable use or containment evidence through transformation and reuse.
Controlled disposition	***Disposition reference:*** *D-03, Ungoverned candidate evidence.* *Apply the actual Gate state to the generated item. This card tests compliance with that state; it does not promote candidate evidence or erase other failures.*
Example	AI-003 records an unmapped term held as Quarantined. Use records show no material reliance. AI-011 may Pass its handling test when its prerequisites and all local criteria are satisfied; the term remains held and full scope conformance is assessed separately.

Non-example	A Gate records Quarantined, but the generated mapping is used in a material decision. An informal human review does not authorize that reliance.
Authority and execution	**Authority:** The applicable decision-scope authority governs permitted use or containment. Component authorities remain accountable for their controls. **Execution:** Enforce the recorded Gate state, validity, authority, and constraints at the point of material use and preserve actual handling evidence.
Retest	Compare each affected item's actual handling with its Gate state and valid authority. Verify scope and validity under Proceed, exception bounds under Caution, and prevention of reliance under Stop, Quarantined, or unauthorized Caution. Retain every other control's result.

11. Remediation record template

Use this record when a failed control requires correction, exception handling, or controlled disposition. The record may be implemented in a document, workflow, ticket, table, governance platform, API, or other structured mechanism.

Decision-scope identifier and version	
DACS Specification and profile/control-set versions	
Original evaluation ID, version, and time	
Original Gate ID and readiness state	
Control ID	
Original control result	Pass / Fail / Not Applicable with reason
Failed condition or evidence gap	
Affected evidence references and effective versions	
Prerequisite results and supporting references	
Affected controls, if any	
Failure classification	Missing evidence / ambiguity / identity or grain / authority / conflict / threshold or rule / drift or change / unsupported discovery / prohibition / missing execution record / other
Remediation pattern references	
Remediation action and owner	
Approving authority or rule and effective period	
Prospective rule, mapping, source, contract, or version change	
Exception authority, scope, constraints, expiration or review	
Permitted or blocked use while unresolved	
Retest ID, version, and time	

Retest inputs, rules, and effective versions	
Retest scope and Gate reassessment required	Control only / affected controls / full Gate, with reason
Retest evidence reference	
Retest control result	Pass / Fail / Not Applicable with reason
Required follow-up evaluations and persistence deadline, if applicable	
Resulting Gate readiness state and validity condition	Proceed / Caution / Stop / Quarantined
Review condition or date	
Linked replacement Gate or Conformance Record reference	
Prior event link, integrity reference, and lawful-retention limitation	

12. Closing guidance

Remediation makes a failed condition explicit, assigns accountable corrective work, and produces evidence for retest. When the condition cannot yet be corrected, the recorded Gate determines whether use is blocked or explicitly constrained.

A control that fails should create useful information. It should identify what is missing, who has authority to resolve it, what evidence must change, what use is permitted while the condition remains unresolved, and what must be retested before the result changes.

DACS defines control and evidence requirements for a stated decision scope. Accountable authorities own the obligation. Human, procedural, automated, or hybrid mechanisms execute the controls. Preserved evidence makes their results inspectable and supports decision-path reconstruction; rerunning an unavailable historical model is not required when the required contemporaneous evidence is complete.

Final operating rule

Actual handling follows the recorded Gate disposition. Keep every control’s evidence-backed result separate from permission for use. Later correction creates a linked new result; it does not overwrite the original failure. A handling or containment Pass does not establish full decision-scope conformance.