The Defensible Analytics Control Specification Manifesto

DACS: Doctrine for Accountable Information and Defensible Decision Paths

Available at: https://dacs.datavaultalliance.com/documents/dacs-manifesto/

Doctrine statement: Defensible Analytics requires an organization to be able to show why a material decision was permitted to rely on the evidence it used, for the stated use, under the conditions that existed at the time.

Status: v1.18 Release Candidate. This manifesto explains the doctrine behind DACS. It is an informative companion doctrine and is not the formal conformance specification.

Founding Authors and Committee Leads:

Daniel Linstedt – CEO, DataVaultAlliance Holdings, LLC

Cindi Meyersohn – COO, DataVaultAlliance Holdings, LLC

When a material decision is challenged, the organization should be able to reconstruct the evidence, meaning, identity, relationships, context, authority, controls, and permitted use that supported it.

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 Redistributed copies may become outdated.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.

1. Executive Statement

Enterprises do not lack data or AI. They lack accountable decision paths.

Modern organizations can usually show where data came from, how it moved, what a model returned, which API was called, or what an automated workflow executed. They are often less prepared to show why a material decision was permitted to rely on the identities, meanings, relationships, context, authority, and evidence embedded in that execution.

That distinction matters because a technically successful decision path can still be based on ambiguous business meaning, unstable identity, an invalid or misoriented relationship, stale context, missing authority, or evidence that was available but not eligible for the stated use.

The problem is not that catalogs, lineage, semantic layers, governance programs, data-quality controls, observability tools, AI platforms, or guardrails are ineffective. The control gap appears when their presence or output is treated as sufficient proof that a material decision path had the evidence, authority, controls, and conditions required for permitted use.

DACS stands for Defensible Analytics Control Specification.

DACS is a vendor-neutral, implementation-neutral control specification for decision-evidence readiness within a stated decision scope. It is not a product category, software platform, consulting slogan, replacement architecture, data model, governance program, or AI tool.

DACS defines testable controls for determining whether the material evidence behind a decision may be relied upon for a stated use and whether the basis of that decision can later be reconstructed, inspected, challenged, and defended.

Defensible Analytics is the intended outcome: a decision path whose material evidence, meaning, identity, relationships, context, authority, control results, constraints, and permitted use can be reconstructed for the scope in which the decision was made.

2. The Control Gap

The control gap appears when availability, connectivity, governance artifacts, or technical execution are treated as sufficient evidence of decision accountability yet no tangible evidence exists for such treatment.

DACS addresses the control gap that can remain when:

- **A data platform** connects information but does not by itself prove what the connection means.
- **A data catalog** documents assets but does not by itself determine whether identity, meaning, classification, or relationship use is ready for a stated decision scope.
- **A semantic layer** standardizes metrics but does not by itself govern enterprise meaning across systems, time, and decision paths.
- **A data fabric** exposes distributed data but does not by itself determine whether the relationship path is appropriate for the decision.
- **A data mesh** assigns domain ownership but does not by itself establish cross-domain semantic compatibility for a decision path.
- **A lakehouse** scales storage and processing but does not by itself enforce accountable interpretation.
- **An AI platform** discovers patterns but does not by itself establish that those patterns are ready for material decision use.

These technologies and methods are valuable. They solve real problems and remain essential parts of the modern enterprise stack. DACS does not replace them.

The control gap appears when connected, cataloged, modeled, governed, or AI-generated information is used in a material decision path before the enterprise can answer one question with evidence:

Can the organization show why this material decision was permitted to rely on these identities, meanings, classifications, relationships, context, authority, and evidence for this stated use?

If the enterprise cannot answer that question, it has a control gap.

DACS focuses on that gap.

3. The Doctrine of Defensible Analytics

DACS is built on a set of direct declarations about how material decision evidence should be treated. These declarations do not replace the normative controls. They explain why those controls exist and what problem they are intended to solve.

3.1 Availability Does Not Establish Permission to Rely on Evidence

Technical access answers whether information can be reached. DACS asks a different question: whether that information is eligible to be relied upon for this decision, for this purpose, under this authority, and at this point in time.

A governed repository, approved system, connected API, retrieved document, or authorized tool may supply valuable evidence. Its location, availability, or accessibility does not by itself establish decision readiness. The evidence still has to satisfy the controls that apply to the stated use.

3.2 Discovery Produces Candidate Evidence

Discovery is valuable. Analytics can reveal patterns. AI can infer associations. Models can identify signals. Agents can recommend actions. Human expertise and source-system behavior can expose relationships the enterprise has not previously governed.

DACS preserves that discovery without converting it into automatic reliance. A discovered, inferred, generated, imported, retrieved, or declared result remains candidate evidence until the applicable controls establish how it may be used. It may be explored, reviewed, remediated, constrained, or kept Quarantined.

3.3 Meaning and Identity Are Part of the Evidence

A decision cannot be reconstructed if the organization cannot show what the material concepts meant and which specific business instances were involved. A source-system key may be technically valid while still failing to establish the Business Identity required for a cross-system decision. A familiar label may be widely used while still hiding conflicting definitions or semantic grain/atomicity.

DACS therefore treats governed meaning, identity rules, semantic grain, source attribution, and authority as part of the evidence behind a material decision. They are not documentation added after the fact of the material decision.

3.4 Relationships Require Governed Meaning

A technically valid join, graph edge, lineage path, or inferred association can show that two things are connected. It does not establish that the relationship carries the meaning required for the stated decision, that its direction is valid, or that it may be relied upon for the stated use.

Material relationships must be testable for meaning, source, orientation, evidence, constraints, and permitted use. Where a relationship materially influences a decision, the organization must be able to show why that relationship path was valid for that scope.

3.5 Context and Authority Are Scope-Bound and Time-Bound

Evidence that was appropriate in one decision scope may be inappropriate in another. A prior approval may no longer apply after a policy change, semantic change, source change, new relationship, changed threshold, or different intended use.

DACS binds readiness to a stated decision scope and preserves the context and authority that applied when evidence was evaluated. Reuse is possible when the scope and conditions remain valid and aligned. An assumption is not a substitute for evidence.

Changes in rules, thresholds, governed meaning, or authority apply to new evaluations from their effective point forward. Historical records remain evidence of the conditions that existed when the decision was made.

3.6 Execution Does Not Create Authority

A workflow, agent, model, rule engine, or Gate may execute a control mechanism. Execution does not make the mechanism the accountable authority. Business authority, technical permission, control execution, evidence, and recorded outcome are distinct responsibilities.

This distinction matters most as automated systems become capable of recommending, routing, approving, or executing material actions. A machine can apply an approved rule without becoming or being the source of the authority behind that rule.

3.7 Defensibility Depends on Reconstruction

Logs and technical lineage can show what happened and how data moved. Defensible Analytics requires enough additional evidence to reconstruct why the material decision path was allowed to rely on the evidence it used.

A reconstructable path preserves the governed decision evidence, control results, Gate Record and resulting readiness state, constraints or exceptions, and the state of relevant evidence at the time. The purpose is not to guarantee that the decision was correct. The purpose is to make the basis of the decision inspectable, challengeable, and defensible.

3.8 What This Means in Practice

- **Identity**: A source-system key may be valid as a technical key in its own application and still fail as the Business Identity for a cross-system decision scope when grain, authority, or resolution rules are missing.
- **Relationships**: A technically valid join, graph edge, or inferred association remains candidate evidence until the required relationship type, orientation, provenance, vector, path, and constraint controls are satisfied.
- **Discovery**: An AI-generated classification may be useful immediately for exploration while remaining Quarantined until it maps to approved governed meaning or receives the required review.
- **AI context:** A retrieved document, authorized API response, or connected tool output is not eligible merely because the AI can access it. The evidence must be governed and eligible for the stated decision scope.
- **Gates**: Approval in another scope, another time period, or another workflow does not automatically establish current readiness. The applicable Gate applies the current criteria and records the resulting readiness state under the responsible authority or approved rule.

3.9 Stated Use Is the Boundary

DACS does not assign universal trust to data, relationships, models, or evidence. It evaluates readiness for a stated decision scope.

A decision scope defines the material business context, grain, intended use, excluded use, applicable authority, and evidence boundary being evaluated. This makes the question precise: not whether an item is good in general, but whether the evidence supports reliance for this particular use.

DACS conformance for a decision scope requires every applicable mandatory control to Pass or be recorded as Not Applicable with a recorded reason. An approved exception may support constrained use and a Caution readiness state, but it does not convert Fail into Pass or establish DACS conformance.

3.10 DACS Starts Narrow

> ***DACS starts narrow: one decision scope, one decision path, one bounded evidence test.***

It does not require a complete enterprise ontology, a new platform, or a full governance reorganization before use. The first pass can be manual and lightweight. The purpose is to identify the evidence that must pass, assign explicit control results and readiness states, quarantine what is not ready, and expose the remediation work that remains.

DACS readiness evaluation remains tied to defined controls for the stated decision scope.

A DACS Capability Level is an organizational adoption measure, not a decision-scope result. It describes how an organization applies DACS across a declared boundary in terms of scope breadth, operational repeatability, governance, and adaptive control. The framework uses Levels 0-5; the companion DACS Capability Levels and Organizational Adoption Guide defines the level criteria and evidence expectations.

Organizational capability can expand over time. The organization can repeat Gate evaluations, extend DACS to more decision scopes, improve governance and version control, automate appropriate control execution, strengthen evidence preservation, and scale operations.

A higher Capability Level does not change the meaning of Pass or Fail and does not confer conformance on a decision scope that has not been evaluated.

The first goal is not perfection. The first goal is to stop relying on untested evidence for material decision use.

4. DACS Inside the System of Information Management

DACS operates within SIM, the System of Information Management, as the control specification for decision-evidence readiness.

SIM is the enterprise system for managing information as a governed business asset. It is not limited to storage, modeling, access, reporting, governance documentation, or AI tooling. SIM manages the broader information lifecycle: its meaning, identity, classification, relationships, context, continuity, controls, readiness, delivery, and accountability.

SIM does not replace operational systems of record. It governs how information from those systems is interpreted, related, contextualized, tested, and made ready for decision use.

In this role, SIM establishes the enterprise record of governed meaning, identity evidence, relationship evidence, Gate Records and resulting readiness states, and decision context. It provides the management environment in which information can move from discovery to decision readiness.

DACS is the control specification inside SIM.

The relationship is simple:

- **SIM** provides the management system for governed information.
- **SIM-ZONEs** organize stages of readiness through which information may move.
- **Gates** apply approved control logic and create Gate Records that preserve readiness states under the responsible authority or approved rule.
- **DACS** defines what must be true before information can be used as decision-scope evidence.

SIM-ZONEs and Gates provide the operating path; DACS Capability Levels describe how systematically an organization applies that operating model across a declared organizational boundary. As capability increases, Gate execution across SIM-ZONE transitions may become more repeatable, integrated, governed, and automated where appropriate. These operating improvements do not change the DACS controls or conformance requirements for any decision scope.

DACS defines what must be true about identity, meaning, classification, relationships, context, AI context adherence, and decision paths before information can be treated as ready for the stated use within a stated decision scope.

The DACS control model is organized into profiles:

- **Core Decision-Scope Controls** are defined in the DACS Specification and apply to every decision scope.
- **Extended Taxonomy Controls** are defined in the DACS Specification and apply when governed meaning, labels, boundaries, ownership, provenance, readiness, risk, or usage must be tested.
- **Extended Ontology Controls** are defined in the DACS Specification and apply when material relationships affect the decision path.
- **AI Context Contract Controls** are defined in the DACS Specification and apply when AI, machine inference, generated classifications, generated relationships, agents, or AI-assisted recommendations affect the decision path.

Defensible Analytics is the intended outcome.

SIM governs information. SIM-ZONEs organize readiness. Gates apply approved control logic and record readiness states. DACS defines the controls for accountable identity, semantic meaning, relationships, context, AI adherence, and decision paths. Defensible Analytics makes the decision path reconstructable, testable, and defensible.

5. The Semantic Contract

DACS depends on a Semantic Contract.

A Semantic Contract is the governed agreement that defines how an enterprise interprets business concepts, identifies instances of those concepts, classifies them, relates them, constrains their use, and preserves their meaning over time.

It is more than a glossary, more than a BI semantic layer, and more than a collection of tags, descriptions, or documentation.

In DACS, the Semantic Contract is the governed agreement that allows information to be evaluated for decision readiness. It establishes how meaning, identity, classification, relationships, context, constraints, and use are governed for the stated decision scope.

Without a Semantic Contract, the enterprise may still have data, models, metrics, dashboards, and AI outputs. What it lacks is a governed basis for determining whether those outputs mean what the business thinks and agrees that they mean.

DACS defines three essential building blocks of the Semantic Contract before extending it to AI-assisted decision scopes. These three building blocks are: Extended Taxonomy, Extended Ontology, and Business Identity.

5.1 Extended Taxonomy

The Extended Taxonomy defines governed classification and physical semantic anchoring.

Extended Taxonomy extends controlled and approved business meaning into the physical data estate. It binds approved concepts to source systems, physical attributes, Business Identity, semantic grain, ownership, provenance, authority, and permitted use.

That binding matters because business meaning alone does not establish decision readiness, and physical data alone does not establish what the business thinks the data means. Two fields or identifiers are not equivalent merely because their names look similar; they must represent the same governed concept at the required grain for the stated decision scope.

At the doctrine level, the requirement is simple: governed meaning must be traceable to the physical evidence used by the decision, with enough authority and context to test whether that evidence is eligible for the stated use.

5.2 Extended Ontology

The Extended Ontology defines governed relationship meaning and physical relationship anchoring.

Extended Ontology extends governed relationship meaning into the physical data estate. It binds or anchors relationship type, source, orientation, semantic grain, provenance, constraints, and permitted use to the real structures and paths that represent the relationship.

While discovery remains valuable, a join, graph edge, lineage path, or inferred association may reveal a real connection, but it does not by itself establish that the relationship is valid for material use.

> ***But discovery is not automatic trust.***

Material relationships must be testable for meaning, direction, authority, evidence, constraints, and stated use. DACS uses Strength, Confidence, and Orientation to make the force, evidentiary support, and direction of a material relationship explicit.

The purpose is not to suppress discovery. It is to connect governed relationship meaning to real-world evidence so the organization can determine whether a relationship path is permitted, constrained, stopped, or Quarantined for the decision scope.

5.3 Business Identity

Business Identity anchors specific instances of governed concepts.

The Extended Taxonomy tells the enterprise what kind of thing something is. The Extended Ontology tells the enterprise how that kind of thing is allowed to relate to other things. Business Identity tells the enterprise which specific instance is involved.

DACS does not require one universal key. It requires enough evidence to show which specific business instance is involved, at what semantic grain, from which source or authority, which identity or resolution rule established it, and how material conflicts, if they arise, are resolved for the stated use.

Decision readiness cannot be established if the enterprise cannot demonstrate, through evidence, which business instance the decision path refers to. A classification may be correct, and a relationship may be permitted, but the decision can still fail if the wrong customer, account, contract, product, asset, or event is being counted, compared, joined, inferred, or acted upon.

Without Business Identity, the enterprise can classify concepts and define relationships, but it cannot reliably compare history, reconcile systems, resolve conflicts, reconstruct decisions, or defend analytics.

5.4 The Contract as a Whole

The Semantic Contract is formed when governed meaning, physical semantic anchoring, Business Identity, relationship rules, preserved context, Gate criteria, stewardship, versioning, usage boundaries, and audit expectations are brought together as decision evidence.

It is not a single artifact. It is the governed agreement that allows the enterprise to determine whether information means what it claims to mean, refers to the correct business instance, relates through an approved path, and is ready for the decision scope in which it is to be used.

Together, the components of the Semantic Contract answer:

- What does this concept mean, and which specific business instance is involved?
- How is it classified and physically represented across systems?
- How may it relate to other concepts or instances, and what orientation governs the relationship?
- What context, authority, usage boundaries, or constraints apply?
- What evidence and Gate criteria govern movement toward the stated use?
- What readiness state applies, and can the decision path be reconstructed?

Without the Semantic Contract, identities, meanings, classifications, and relationships can become informal assumptions.

With the Semantic Contract, they can be governed, tested, and recorded as accountable decision evidence.

5.5 The Binding AI Context Contract

For AI-assisted decision scopes, the Semantic Contract becomes a **Binding AI Context Contract**.

The Binding AI Context Contract defines the governed context against which AI behavior can be tested. It combines Extended Taxonomy, Extended Ontology, Business Identity, preserved context, relationship vectors, permitted paths, prohibited paths, governance constraints, Gate criteria, drift rules, and decision-scope evidence requirements.

Its purpose is not to prevent AI from discovering patterns, generating classifications, inferring relationships, or recommending actions. Those capabilities are valuable. Its purpose is to provide a governed basis for testing whether AI-assisted outputs remain aligned with governed meaning, approved identity, permitted relationships, valid context, and the stated decision scope.

Without a Binding AI Context Contract, AI governance remains dependent on general policy, model behavior, prompt design, or human interpretation after the fact. With the contract, AI inputs, outputs, inferred relationships, generated classifications, recommendations, and semantic or relationship drift can be tested against governed meaning and permitted relationship paths.

The result is not automatic trust. The result is a recorded Gate readiness state. A governed process routes AI-assisted evidence through the applicable controls, and the Gate records the resulting readiness state under the responsible authority or approved rule.

This is one reason DACS extends the taxonomy and ontology. The extension creates a governed context contract that is testable through Gates. It gives AI a decision-scope boundary, a semantic boundary, a relationship boundary, and an evidence boundary before AI-assisted outputs are treated as decision-ready.

6. The DACS Control Model

DACS defines the control model for determining whether information is ready for stated use within a stated decision scope.

It does not rely on general confidence, informal trust, tool presence, governance intent, or data availability. It requires evidence.

DACS controls apply to the things that make decision paths defensible:

- governed business meaning;
- physically anchored classification;
- verified and validated Business Identity;
- approved relationship paths;
- preserved context;
- source and provenance evidence;
- usage boundaries;
- Gate criteria;
- readiness states;
- exceptions and remediation;
- reconstructable decision evidence.

The manifesto describes these requirements at the doctrine level. The DACS specification expresses them as binary controls through conformance profiles.

This distinction matters.

For a stated decision scope, each applicable control evaluates to Pass, Fail, or Not Applicable. Not Applicable requires a recorded reason. An exception may support constrained use and a Caution readiness state, but it does not convert Fail into Pass. An enterprise may begin with one decision path, one Gate, one evidence packet, and one readiness determination.

DACS therefore separates two concepts:

- Decision-scope conformance is established only when every applicable mandatory control for that scope Passes, or is recorded as Not Applicable with a recorded reason, in accordance with the DACS Specification.
- A DACS Capability Level describes organizational adoption across a declared boundary. It does not change control semantics, cause a control to Pass, or confer conformance on an unevaluated decision scope.

The purpose of the DACS control model is not to create bureaucracy. Its purpose is to make decision evidence testable, accountable, and reconstructable before information is treated as reliable for a stated use.

6.1 Identity Anchor

Every material decision path must begin with stable Business Identity.

DACS does not require every system to share one physical key. It requires the enterprise to know which business instance a decision path refers to, which source asserted that instance, which identifier or resolution rule established it, and at what semantic grain the identity is unique and meaningful for the stated decision scope.

Source-system identifiers, operational keys, generated IDs, matched records, mastered records, reference records, and semantic identifiers may all contribute identity evidence. They do not automatically constitute enterprise identity. For material use, identity evidence must be governed, repeatable, and tied to approved meaning.

Probabilistic, approximate, or AI-assisted identity methods may be valuable for discovery and resolution. For material use, as determined by the applicable Materiality Rule for the stated decision scope, the identity method may remain probabilistic, but the DACS control evaluation does not: the applicable control result is Pass, Fail, or Not Applicable. The associated Gate readiness state is Proceed, Caution, Stop, or Quarantined, as appropriate. An exception may support constrained Caution but does not convert Fail to Pass.

Without stable Business Identity, there is no reliable history. Without reliable history, there is no accountability. Without accountability, analytics cannot be defended.

In an implementation-neutral DACS context, this anchor may be represented by a stable business identifier, durable identity rule, approved resolution method, identity registry, semantic identifier, governed master or reference record, data model structure, metadata object, knowledge-graph node, or equivalent evidence construct. The requirement is not a specific artifact. The requirement is stable Business Identity anchored to governed meaning and a stated decision scope, as evidenced by the applicable control results, Gate Record, and resulting readiness state.

6.2 Accountable Relationship Vector

Every material relationship used in a decision path must be evaluated through an accountable relationship vector.

A relationship is not ready for stated use merely because it appears in a source system, lineage view, model, graph, dashboard, analytic output, or AI response. It is ready only when the relationship meaning, source, direction, evidence, constraints, and decision-scope applicability satisfy the associated controls and Gate criteria.

The vector records three elements:

- ***Confidence***: How much evidence supports the relationship? Confidence measures evidence quality, support, repeatability, recency, and reliability.
- ***Strength***: How strong is the relationship or signal? Strength measures the practical force of the relationship and whether it meets the decision-scope threshold for influencing a decision.
- ***Orientation***: Which way does the relationship point? Orientation identifies direction, authority, sequence, dependency, ownership, lineage, hierarchy, flow, inclusion, identification, support, or causality when causality has been separately established.

These vector elements govern use, not merely describe risk. The decision scope must define the thresholds or qualitative criteria that determine whether a relationship is sufficient for the stated use. A detected association may show that two things are related, but it does not by itself establish the meaning or authority of that relationship. Temporal sequence establishes order, not causation. Dependency establishes reliance or connection, not ownership or accountability. And a relationship that is valid in one direction may not be valid in the reverse direction.

6.3 Preserved Context

Relationships, classifications, identities, and AI outputs do not exist in isolation. They exist at a point in time, under a set of conditions, from a source, within a process, under a definition, and inside a decision context.

DACS requires preserved decision context because meaning changes over time. A relationship may have been valid last quarter and invalid today. A policy may have changed. A hierarchy may have shifted. A customer may have moved segments. A product may have been reclassified. A regulatory interpretation may have evolved. A source system may have overwritten operational history.

If context is lost, the enterprise may still know what result was produced, but it cannot explain why that result was defensible at the time.

Preserved context allows the organization to compare what was true then with what is true now. It protects institutional memory, supports challenge and remediation, and makes reconstruction possible.

In an implementation-neutral DACS context, preserved context may be represented by temporal descriptive records, versioned assertions, provenance records, context logs, event history, semantic annotations, data model structures, or equivalent evidence objects. DACS requires the capability to preserve descriptive context over time, not a single physical implementation.

6.4 Reconstructable Decision Path

A defensible result must be reconstructable.

The enterprise must be able to show which identity was used, which classification applied, which relationships were followed, what context applied, which Gate Record and readiness state governed use, what evidence existed, what Conformance Record or other structured evidence record was produced, and what state of information was available at the time.

This is not limited to technical lineage. Technical lineage shows how data moved. DACS requires decision lineage: how identity, meaning, classification, relationship path, context, control results, Gate Records, readiness states, and evidence supported the result.

Reconstructability is not the same as reproducibility. A decision path can remain reconstructable even when the original model, service, or technology is no longer available, provided contemporaneous evidence preserves what was executed, the relevant versions, inputs and context, output, authority, control results, and Gate Record. A later run with a different model or version is comparison evidence; it is not reproduction of the original execution.

A result that cannot be reconstructed may still be useful. It may even be correct. But it is not defensible in the DACS sense.

6.5 Structured Evidence and Conformance Records

A Conformance Record preserves the scope-bound DACS determination in a structured form that supports review, exchange, audit, and reconstruction. Supporting evidence may remain in different systems or formats, but the record must preserve the required references. Narrative approval alone is not sufficient.

At minimum, the record identifies the decision scope, applicable DACS Specification and control-set versions, applicable Profiles and controls, control results, evidence references, Gate Records and resulting readiness states, the responsible authority or approved rule reference, timestamp or effective period, constraints or exceptions, and review conditions.

The Conformance Record preserves a scope-bound determination. It does not establish universal truth, guarantee decision correctness, or create organization-wide conformance.

Authorized downstream processes, auditors, governance workflows, and automation may use the recorded control results and readiness state to permit, constrain, block, review, or remediate use within the responsible authority.

DACS does not require all evidence to live in one tool. It requires sufficient records and evidence references to reconstruct and challenge the decision path.

Evidence preservation also requires integrity and lawful retention. DACS does not require indefinite retention of every raw artifact. When law, regulation, contract, privacy policy, or an authorized retention rule requires deletion or minimization, the organization preserves the most complete lawful reconstruction anchor available, the authority for the action, and any resulting limitation on reconstruction.

6.6 Controls Make Readiness Testable, Accountability Remains Assigned

DACS defines the criteria and evidence obligations. Accountable authorities own the obligation. Assessors, governed processes, or authorized automation execute controls. Evidence demonstrates what existed and whether the requirements were satisfied. Gates apply approved logic and record the resulting readiness state. Conformance Records preserve the scope-bound determination.

Execution does not create authority. An automated mechanism may execute a DACS control without becoming the accountable authority. A person may own an obligation without personally executing the control. Authority, execution, evidence, and recorded outcome must remain distinguishable.

This distinction allows organizations to formalize accountability without inventing a new bureaucracy. Existing business owners, stewards, risk functions, operational teams, technical teams, and executive decision routines can retain their responsibilities when authority, execution, and evidence are explicit.

Defensible Analytics is not created by documentation alone. It depends on controls being executed consistently, evidence being preserved, accountable authorities remaining visible, and decisions being reconstructable and challengeable when necessary.

6.7 Evidence-Based Readiness

DACS does not accept subjective confidence or general assertions of trust as conformance evidence.

Readiness is not established by saying information feels trustworthy, accountable enough, or appropriate enough. The assessment records what passed, what failed, what is Not Applicable, what remains constrained, what is Quarantined, what evidence exists, and what readiness state applies.

For DACS, readiness is evidenced through control results, required evidence, thresholds or approved rules, Gate Records and resulting readiness states, exceptions or constraints, and reconstructable decision paths. If a claim cannot be tested, it may be useful discussion language, but it is not sufficient to establish readiness for stated use.

Operational measurement may include relationship readiness, AI context readiness, Gate readiness, evidence readiness, and Quarantine visibility. Detailed indicator definitions belong in the DACS Specification and operational guidance; the Manifesto retains the doctrine that readiness must be observable and testable rather than asserted.

7. Gates Turn Governance Into Control

DACS controls are applied through Gates.

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

The evaluation at a Gate should establish answers to questions such as:

- Is the Business Identity resolved at the correct semantic grain?
- Is the classification governed by the Extended Taxonomy?
- Is the relationship governed by the Extended Ontology?
- Is the relationship explicit, permitted, and tested for this use?
- Does the relationship vector meet the decision-scope threshold or approved qualitative criteria?
- Is the context current, historically valid, and preserved?
- Is the information authorized for this decision scope?
- Can the decision path be reconstructed from the evidence?
- If AI is in scope, does the output adhere to the Binding AI Context Contract?

A Gate is not merely a meeting, policy statement, or documentation exercise. Its evaluation must have an operational consequence in the governed process, and the Gate Record must preserve the resulting readiness state. Depending on that state, the process permits use, constrains use, blocks use, or keeps candidate evidence Quarantined until the applicable controls pass or an approved constrained-use exception exists.

This is the practical control model behind Defensible Analytics. Skipping a Gate does not create speed. It transfers risk downstream.

8. Proceed, Caution, Stop, and Quarantined

DACS defines four Gate readiness states to keep decision-readiness language simple, visible, and actionable.

These readiness states are separate from control results. A control result is Pass, Fail, or Not Applicable. An exception may support constrained Caution, but it does not convert a failed control into Pass.

Proceed

Applicable controls have passed for the stated decision scope. Use is permitted only within the approved scope.

Caution

Caution permits only explicitly authorized constrained use. The constraints, monitoring or remediation requirements, responsible authority or approved rule reference, and review condition must be recorded and enforceable. An automated workflow may continue only within those recorded bounds. Caution does not establish DACS conformance for the decision scope and does not convert a failed control into Pass.

Stop

A control failure, prohibition, missing authority, invalid context, or contract violation prevents material use for the stated decision scope. Use is not permitted until the blocking condition is resolved or an authorized constrained-use path explicitly supports Caution where permitted.

Quarantined

Evidence is known, discovered, inferred, generated, imported, retrieved, or available but has not passed the required controls. It may be explored, reviewed, remediated, or routed through additional Gates, but it must not be relied on for material decisions until the required controls pass or an approved constrained-use exception exists.

Quarantined allows candidate evidence to be captured, reviewed, and remediated without relying on it for material decisions. Stop prevents failed, prohibited, or unauthorized evidence from being used for the stated decision scope.

The model is intentionally simple. It allows executives, architects, governance teams, analysts, AI teams, automation teams, and auditors to discuss decision readiness using the same language.

9. What DACS Makes Explicit

DACS focuses on decision-control points that are often implicit, fragmented, or left to interpretation. It explicitly demonstrates:

- How Business Identity becomes accountable for a stated decision scope;
- How semantic meaning becomes governed and physically anchored;
- How classification becomes testable through the Extended Taxonomy;
- How relationships become governed, oriented, evidenced, and constrained through the Extended Ontology;
- How discovery is separated from decision-ready use;
- How relationship-vector criteria govern use rather than merely describe risk;
- How context, usage boundaries, Gates, and readiness states become part of the decision path;
- How AI inputs, outputs, inferred relationships, generated classifications, recommendations, and drift are tested against the Binding AI Context Contract;
- How decision paths can be reconstructed beyond technical lineage; and
- How structured evidence records support Defensible Analytics.

This is not a claim that existing platforms, vendors, or consultancies lack value. Many are essential to the enterprise stack. DACS clarifies their boundary.

Tools can move, expose, document, model, govern, and automate information. But the enterprise still needs a control specification that defines what must be true before information is treated as ready for its stated use in a material decision scope.

That specification is DACS.

10. What DACS Does and Does Not Claim

10.1 What DACS Defines

- A vendor-neutral, implementation-neutral control specification for decision-evidence readiness within a stated decision scope.
- Profiles, control criteria, evidence obligations, control results, Gate readiness states, and claims boundaries.
- The distinction between discovery, governed review, constrained use, Quarantined evidence, and stated decision use.
- Requirements for reconstructable evidence paths, structured Conformance Records, and controlled exception handling.

10.2 What DACS Does Not Claim

- DACS does not guarantee that a decision is correct, optimal, lawful, risk-free, or immune from challenge.
- DACS conformance is specific to a stated decision scope. It does not establish organization-wide conformance, a DACS Capability Level, formal certification, or legal or regulatory compliance status. It also does not certify an enterprise, platform, vendor, model, repository, or product.
- DACS does not replace data governance, data quality, metadata management, taxonomy, ontology, lineage, AI governance, risk management, architecture, or stewardship.
- DACS does not require one data model, graph, catalog, semantic layer, warehouse, lakehouse, workflow platform, AI platform, or other implementation architecture.
- DACS does not make connectivity, availability, provenance alone, prior approval, or technical accessibility equivalent to decision readiness.
- Execution by an automated rule, Gate, workflow, or model does not make that mechanism the accountable authority.

10.3 What DACS Does Not Accept as Sufficient Evidence

DACS requires testable control evidence. The following conditions do not, by themselves, establish readiness for a stated use:

- unmanaged inference presented as enterprise truth;
- identity, classification, and relationship assumptions hidden inside reports, pipelines, dashboards, semantic layers, model features, or agent prompts;
- confidence without evidence;
- classification without governance;
- association without orientation;
- relationship vectors that describe risk but do not govern use;
- lineage that cannot explain decision logic;
- human approval without inspectable evidence;
- AI outputs that drift from governed meaning, approved classifications, permitted relationships, or decision-scope context without detection, review, or consequence; and
- governance that cannot be implemented, observed, tested, or evidenced.

DACS permits discovery, analytics, automation, and AI. It prohibits treating untested discovery as evidence ready for material decision use.

11. The Executive Commitment

Defensibility is not created by storage, dashboards, catalogs, automation, or AI. These capabilities matter, but they do not, by themselves, establish that a material decision path has the evidence, authority, controls, and conditions required for permitted use.

The executive commitment behind Defensible Analytics is to make the material basis of important decisions explicit before reliance, test it against applicable controls, and preserve enough evidence to reconstruct that basis if the decision is later challenged.

That means requiring enough governed decision evidence to show what was relied upon, which controls were evaluated, which Gate Record and readiness state governed use, and under what conditions the use was permitted.

DACS is narrow by design. It does not attempt to define every aspect of enterprise architecture, governance, analytics, or AI. It focuses on the decision-evidence control boundary where implicit assumptions become material risk.

This commitment is not to fund a new bureaucracy. It is to require enough governed evidence for decision paths to be tested, challenged, remediated, and reconstructed using responsibilities the organization already owns.

A DACS evaluation can be useful even when it exposes failure. Control results show what has Passed, Failed, or been determined Not Applicable. Gate readiness states make the permitted next step explicit: Proceed permits use within scope; Caution constrains use; Stop records a blocking condition; and Quarantined preserves candidate evidence without allowing it to become an unexamined basis for material action.

DACS does not guarantee that every analytic or AI-assisted result is correct. It defines the requirements used by governed assessment to determine whether the evidence path satisfied the applicable controls for the stated decision scope.

12. Closing Declaration

Defensible Analytics begins when the material basis of a decision is no longer implicit.

The organization can identify the governed evidence relied upon, the controls evaluated, the Gate Record and readiness state, and the conditions that permitted use.

DACS makes those conditions testable. The resulting records show what passed, what failed, what remains constrained or Quarantined, and what action, if any, is required before readiness can advance.

The test is whether responsible people can apply the controls consistently and preserve enough evidence to make material decision paths reconstructable, explainable, and defensible.

The DACS commitment is simple: make the material basis explicit, test it against applicable controls, record the permitted next step, and preserve enough evidence to reconstruct the decision later.

If required evidence cannot establish the conditions for the stated use, the decision path cannot be represented as DACS-conformant. DACS does not promise perfect decisions; it makes the basis for material decisions testable, reconstructable, challengeable, and defensible.