Companion A — Regulatory Cross-References

Status: v1.0 — Reading Edition (rev. 8) | Drafted: 2026-05-30

Source markdown: ./decision-provenance-standard-v1.0-companion-A-regulatory-cross-reference.md

---

Companion to the Decision Provenance Standard v1.0; tracks core revision rev. 8.

This Companion cross-references the Standard's core sections (§1–§7, §11) against named regulatory and control frameworks. Its cross-references to the core sections resolve against the core Reading Edition (rev. 8); its references to other Companions (B, C) and to Appendix G resolve against those documents.

Companion A — Regulatory Cross-References

> **Disclaimer pointer.** See the top of the core Standard for the load-bearing UPL firewall, jurisdiction-assumed declaration, and the rule that the Standard produces audit-ready decision provenance — input to compliance work performed by qualified personnel — and is not itself a regulatory substitute, certification, or attestation.
>
> **Jurisdiction Assumed**: U.S. federal + Delaware as primary; UK / EU AI Act / Israel as named secondaries.

> *Decision Provenance Standard records inform — without satisfying — regulatory frameworks. A Decision Provenance Standard record may be cited as supporting evidence under NIST AI RMF, ISO/IEC 42001, EU AI Act and equivalent frameworks. It does NOT itself satisfy any control, requirement, or audit obligation under those frameworks. Adopting organizations remain responsible for their own regulatory posture.*

A.0 Section Purpose and Discipline

This Companion maps the Decision Provenance Standard™'s structural primitives onto nine frameworks the Standard converses with around AI governance and traditional internal-control and oversight. Those primitives are the Charter mechanism (Section 3), the decision-record schema (Section 6), the Mode 1 / Mode 2 dispatch

architecture (Section 4), the Article 50 disclosure metadata (Section 4 §4.6), the record lifecycle states (Section 5), and the conformance levels (Section 7). The frameworks fall into two clusters.

The AI / ISO interlocking trio (§A.1–§A.5) addresses forward-looking AI governance: EU AI Act Articles 14, 17, and 50; the U.S. National Institute of Standards and Technology AI Risk Management Framework (with explicit attention to Manage 4.1); and ISO/IEC 42001:2023.

The traditional internal-control and oversight backbone (§A.6–§A.9, with cross-cutting notes at §A.10) addresses the existing internal-control and governance frameworks the Standard's primitives produce input substrate into: the Caremark / Marchand v. Barnhill line of Delaware oversight-duty case law; COSO 2013's Internal Control – Integrated Framework; Sarbanes-Oxley § 404 management assessment of internal control over financial reporting; and SOC 2 Type II under the AICPA Trust Services Criteria.

The Standard's records **inform** the regulatory work below **without satisfying** any framework's obligation; the obligation belongs to the obligated party, and the full non-claim set governing every cross-reference in this Companion is at core §1.4.2.

The cross-references in §A.1–§A.10 follow three discipline rules that govern every sentence below.

1. **The Standard is input, not satisfaction.** Per the locked lead paragraph above and the Standard's vocabulary discipline (§2.3), no cross-reference below claims that the Standard satisfies, ensures, certifies, or substitutes for any framework's requirements. Each framework's requirements are discharged by the deployer's qualified personnel, using the audit-ready decision provenance the Standard produces as one input among many. Those personnel include counsel, compliance officers, internal auditors, third-party assessors, and certification bodies. They also include the engaged service auditor in SOC 2 engagements, the external auditor in SOX § 404 engagements, and the board itself in Caremark / Marchand work. The cross-references show *where the Standard's primitives map onto framework requirements*; they do not show *that the Standard meets the requirements*.
2. **Citation forms are locked.** Citation forms in §A.1–§A.10 are coherent with Appendix G (References) §12.2.1, §12.2.2, and §12.2.3.
3. **Each cross-reference closes with an explicit non-claim.** Every framework sub-section ends with a paragraph naming what the Standard does not claim against that framework, in the framework's own register. The non-claim is structural scaffolding, not decoration. It is the sentence a regulator or plaintiff's counsel would otherwise read into the cross-reference if it were absent.

Section 4 carries verbatim normative Article 50 conformance language. §A.3 cites the cross-reference and points to Section 4; it does not reproduce the conformance language. Section 7 enumerates the conformance-level criteria the Standard's Charter and decision records satisfy. §A.1–§A.10 cite the conformance-level surface and point to Section 7; they do not redefine levels. Section 5 establishes the lifecycle states (`draft` → `reviewed` → `affirmed`). The cross-references below note where the lifecycle's properties — the affirmation event, the seal, the supersedes mechanism — produce structural inputs counsel and auditors find useful. They do not claim that any framework's requirements are met by the lifecycle alone. Where the Caremark /

Marchand line names doctrinal tests, §A.6 names the subject domain and explicitly reserves substantive holdings for counsel admitted in Delaware; it does not characterize what the cases hold.

The mapping is structural, not substantive. In each case below, the Standard's primitives are an input substrate: a structured record of how decisions were made, by whom, against which inputs, with what review, with what affirmation, and sealed at what moment. Counsel, auditors, internal-controls officers, and board fiduciaries can use that substrate when preparing their own work product. The conversion from structured record to legal evidence, audit attestation, regulatory filing, or board-oversight finding is performed by qualified personnel under their own professional standards. The Standard does not perform that conversion; it produces the substrate the conversion runs on.

A.1 EU AI Act — Article 14 (Human Oversight)

A.1.1 What Article 14 requires

Regulation (EU) 2024/1689, Article 14 imposes on providers of high-risk AI systems an obligation to design and develop those systems so that natural persons can exercise effective human oversight while the system is in use. The article enumerates the capabilities a high-risk AI system must support to make that oversight effective. The natural person carrying out oversight must be able to understand the relevant capacities and limitations of the system, monitor its operation, and recognise and address signs of system anomaly, dysfunction, or unexpected performance. They must also be able to decide not to use the system or override its output where appropriate, and to intervene in or interrupt the system's operation through a "stop" button or comparable procedure. Article 14 adds a further requirement for the high-risk AI systems referred to in Annex III point 1(a). For those systems, no action or decision may be taken by the deployer on the basis of identification resulting from the system unless that identification has been separately verified and confirmed by at least two natural persons.

Article 14's obligation is a **design-and-development obligation on the provider**, paired with corresponding **use-side obligations on the deployer** (the natural or legal person that uses the AI system under its authority). The deployer's obligations under Article 26 reinforce Article 14. The deployer must ensure that the natural persons assigned to human oversight have the necessary competence, training, authority, and support to carry out the oversight task that Article 14 made possible.

A.1.2 How the Standard's primitives map

The Decision Provenance Standard does not produce AI systems. It produces a Charter mechanism (Section 3) and a decision-record schema (Section 6). These bind deployers to a documented decision-making mechanism around the use of AI systems within governed decisions. The mapping onto Article 14 is therefore deployer-side, not provider-side, and runs through three primitives:

Mode 1 (Human-Led, AI-Enforced) as the structural shape of "strong human oversight." Mode 1 dispatch under a Charter places a named human as the author of record of the decision; the AI system functions as a Charter-conformance check on the human's work. The artifact reaching the reader is human-authored. The AI's contribution is internal to the production process: the AI is a discipline mechanism, not a content generator. In Mode 1, the named human exercises Article 14's oversight competencies by definition. Those competencies are to understand capacities and limitations, monitor operation, recognise signs of anomaly, decide not to use the output, intervene, and interrupt. The human is authoring, the AI is checking, and the human's authorship-of-record carries the authority Article 14 requires the natural person to be able to exercise.

Mode 2 (AI-Led, Human-Reviewed) as the structural shape of human review of an AI-authored output. Mode 2 dispatch places the AI system as the author of record of the decision artifact and a named human as the reviewer of record, per the Charter's dispatch state machine (Section 4 §4.4). Mode 2 does not eliminate human oversight; it relocates it from authorship to review. The named reviewer in Mode 2 exercises the Article 14 competencies on the AI-authored output before action. The reviewer must be in a position to decide not to use the output, override it, or interrupt the downstream process. The Charter's Mode 2 dispatch metadata (per Section 4) records who the reviewer of record is, what review was performed, and the reviewer's sign-off. This produces audit-ready provenance that the deployer's qualified personnel can use as input when validating that the Article 14 / Article 26 oversight obligations the deployer carries were actually exercised.

Charter mechanism as the structural shape of oversight competence and authority. Section 3 of the Standard requires a Charter to name an accountable owner (single named human), to enumerate the inside-decisions and outside-decisions the Charter governs, to declare the dispatch mode authorized for those decisions, to record the decision cadence, and to identify the escalation rule. These fields are not Article 26 training records. They are the **structural inputs** a deployer's qualified personnel use when assembling the documentation Article 26 requires the deployer to maintain about the natural persons assigned to oversight. The Charter records who has the authority to oversee what. The deployer's HR, training, and competence-management programs record whether those people have the necessary training and support. Together, the two sets of records support the deployer's qualified personnel in meeting the Article 14 / Article 26 obligation.

A.1.3 What the Charter mechanism + decision-record schema supplies as input

For a deployer's qualified personnel preparing Article 14 oversight documentation, the Standard's primitives supply five concrete inputs:

4. **Mode declaration** (per Section 3 Charter field `mode_declaration` and per Section 4 dispatch state machine) — declares whether oversight is exercised at authorship (Mode 1) or at review (Mode 2). Locks the structural shape of oversight for every decision dispatched under the Charter.
5. **Named accountable owner** (per Section 3 Charter field `accountable_owner`) — the single named human who carries Charter-level accountability for the decision class. Not a substitute for Article 26 training records, but the named human whose oversight authority the deployer's training records must substantiate.

6. **Decision-record schedule** (per Section 6) — the enumerated set of decision records the Charter commits to maintain. Each record carries the dispatch mode, the named author of record (Mode 1) or reviewer of record (Mode 2), the inputs to the decision, and the sign-off. The schedule is the substrate the deployer's qualified personnel use to demonstrate that oversight was exercised on every decision in the class, not selectively.
7. **Escalation rule** (per Section 3 Charter field `escalation_rule`) — the named pathway for moving a decision out of the Charter's normal dispatch when the named human determines that override or interruption is appropriate. Article 14's "decide not to use" and "intervene or interrupt" competencies require an authority pathway. The escalation rule is that pathway, structurally.
8. **Re-decision triggers** (per Section 3 Charter field `re_decision_triggers`) — the named outcome-evidence and market-evidence triggers that re-open a decision for review. Article 14's "monitor operation" competency requires that the natural person be in a position to recognise when the AI system's performance has shifted. Re-decision triggers are the structural commitment a Charter makes to re-open decisions when those signals fire.

A.1.4 Non-claim

The Decision Provenance Standard does not satisfy, ensure, or certify any obligation under Regulation (EU) 2024/1689 Article 14 or Article 26. The Standard does not opine on any of the following: whether a specific AI system is a high-risk AI system within the meaning of Article 6 and Annex III; whether a specific deployer has discharged its Article 26 obligations; whether the natural persons assigned to oversight under a Charter have the necessary competence and training Article 26 requires; or whether the oversight measures designed into a specific AI system meet the Article 14 design-and-development obligation. Those determinations are made by the deployer's qualified personnel — counsel admitted in the relevant jurisdiction, compliance officers, the deployer's AI governance function, and where applicable the provider of the AI system — using the audit-ready decision provenance the Standard's Charter and decision-record schema produce as one input among many. The Standard structures the inputs; the deployer's qualified personnel discharge the obligation.

A.2 EU AI Act — Article 17 (Quality Management System)

A.2.1 What Article 17 requires

Regulation (EU) 2024/1689, Article 17 imposes on providers of high-risk AI systems an obligation to put in place a quality management system that ensures compliance with the Regulation. The article enumerates the elements the quality management system must address. Those elements include a strategy for regulatory compliance; techniques and procedures for design, design control, development, quality control, and quality assurance of the high-risk AI system; examination, test, and validation procedures to be carried out before, during, and after development; technical specifications; and systems and procedures for data management. They also include the risk management system referred to in Article 9, the post-market monitoring system referred to in Article 72, and procedures related to the reporting of serious incidents in accordance with Article

73. The remaining elements are the handling of communication with national competent authorities and other relevant authorities, systems and procedures for record keeping of all relevant documentation and information, resource management, and an accountability framework setting out the responsibilities of management and other staff.

Article 17 is an obligation **on providers**. The deployer of an AI system inside its decision-making does not become a provider by virtue of using the system. The provider obligation runs to the entity that places the AI system on the market or puts it into service in the Union. The Decision Provenance Standard is consumed by deployers governing how their decisions are made; it is not consumed by providers building AI systems for the EU market.

A.2.2 How the Standard relates (provider vs deployer boundary)

The Standard's territory is the deployer side of the provider/deployer split. The Charter mechanism, the decision-record schema, the Mode 1 / Mode 2 dispatch architecture, and the conformance levels all govern decisions a deployer makes using AI systems. They do not govern the design, development, validation, or post-market monitoring of an AI system as a product. Article 17's quality management system requirements run upstream of the deployer's use, not at the deployer's use.

The cross-reference here is therefore **briefer and bounded**. Where a deployer of a Charter under this Standard is *also* a provider of high-risk AI systems within the meaning of Article 3(3) and Article 16, that deployer-and-provider must satisfy Article 17 separately, on the provider side, using the provider's own quality management system documentation. The Charter and decision records produced under this Standard do not constitute, replace, or contribute to the Article 17 quality management system documentation in any structurally load-bearing way. A provider may, in its discretion, reference the Charter and decision records as part of its broader governance environment. The Article 17 obligation is still discharged by the provider's quality management system, not by the Standard's primitives.

Two surfaces interact at the provider/deployer boundary. The first is the deployer's selection and configuration of the AI system used inside Mode 1 enforcement or Mode 2 authorship, which the Charter records via the `ai_system_identity` field on the Article 50 disclosure metadata schema (Section 4 §4.6). The second is the provider's documentation of the AI system itself, which lives outside the Standard's territory and is governed by the provider's Article 17 quality management system. The Charter's `ai_system_identity` field points at the AI system; the provider's quality management system documents what that system is.

A.2.3 Non-claim

The Decision Provenance Standard does not satisfy, ensure, or certify any obligation under Regulation (EU) 2024/1689 Article 17. The Standard does not opine on any of the following: whether a specific provider has put in place a quality management system that meets Article 17; the adequacy of any provider's design control, validation, post-market monitoring, or incident-reporting procedures; or the allocation of provider obligations between a primary provider and downstream economic operators (importers, distributors, authorised representatives) under the Regulation. A deployer that is also a provider must discharge its Article 17

obligations through its own provider-side documentation; the Standard's Charter and decision-record schema do not contribute structurally to that discharge. Determinations about Article 17 conformance are made by the provider's qualified personnel — counsel admitted in the relevant jurisdiction, conformity-assessment bodies where applicable under Article 43, and the provider's quality management function — independently of the Standard.

A.2.bis EU GDPR — Article 17 (Right to Erasure / Right to be Forgotten)

> ⚠ **Disambiguation — two unrelated Article 17s.** This sub-section §A.2.bis addresses **Regulation (EU) 2016/679 (the General Data Protection Regulation), Article 17** — the data subject's right to obtain erasure of personal data concerning them. The preceding sub-section §A.2 addresses **Regulation (EU) 2024/1689 (the EU AI Act), Article 17** — the provider's obligation to put in place a quality management system. The two Articles share a number; they cover entirely different subject matter, operate against different obligated parties, and are engaged by the Standard through entirely different primitives. A reader who treats them as the same article has misread §A.2 and §A.2.bis. Counsel and auditors consulting either cross-reference verify which Article 17 is in scope before proceeding.

A.2.bis.1 What GDPR Article 17 requires

GDPR Article 17 grants a data subject the right to obtain from the controller the erasure of personal data concerning them without undue delay, where one of the grounds in Article 17(1) applies. Those grounds are: the data are no longer necessary for the purposes for which they were collected; the data subject withdraws consent; the data subject objects under Article 21; the personal data have been unlawfully processed; erasure is required for compliance with a legal obligation; or the data have been collected in relation to the offer of information-society services to a child. The right is not absolute. Article 17(3) enumerates grounds on which the processing may continue notwithstanding the erasure request. These include (b) compliance with a legal obligation requiring processing under Union or Member State law, (e) the establishment, exercise, or defence of legal claims, and (d) archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes under Article 89(1).

A.2.bis.2 How the Standard's primitives map

The Standard's seal-hash tamper-evidence requirement at §5.1(3) is compatible with GDPR Article 17, because the two concepts operate at different layers of the data flow. (That seal is tamper-evident on a stored, access-controlled record per §2.2.18, not cryptographic immutability against all attack surfaces.) Article 17's "erasure" means that personal data are no longer processed for the original purpose; the data subject's data must be removed from the operational data store and from active processing. The Standard's seal preserves the historical record of *what decision was made, by whom, on what basis, with what review*. That record is retained for accountability purposes and is distinct from operational use.

The §5.5 redaction-event record pattern makes this distinction explicit. The named fields are erased from the operational data store, operationalizing the deployer's Article 17 erasure obligation as the deployer's counsel determines it applies. The archival record retains the original sealed content under one of the Article 17(3) grounds — typically (b) where the deployer's accountability framework constitutes a legal obligation, (e) where the record may be needed in a legal claim, or a combination. The redaction-event record itself documents the lawful basis on which the archival retention proceeds, via the `archival_record_retention_basis` field (§6.2.3). The seal-hash integrity property of the original record is what makes the archival retention defensible. A record that could be silently altered after a regulatory inquiry could not credibly serve any of the §17(3) grounds.

The redaction-event schema makes audit-trail integrity through erasure events structurally enforceable; substantive Article 17 analysis (whether a specific data subject's request applies, whether a specific Article 17(3) ground supports archival retention, whether the deployer's accountability framework substantively constitutes a §17(3)(b) legal obligation under the regulator's interpretation) is the deployer's counsel's territory.

A.2.bis.3 Non-claim

The Decision Provenance Standard does not satisfy, ensure, or certify any obligation under Regulation (EU) 2016/679 Article 17. The Standard does not opine on any of the following: whether any specific data-subject erasure request applies under GDPR or any other regime; whether any Article 17(3) exception applies to a deployer's archival retention; the position of the European Data Protection Board or any individual EU Member-State Data Protection Authority on the redaction-as-new-affirmed-record framing; whether the enumerated `deletion_method` values in §6.2.3 (`field_purge`, `record_purge_with_pointer_retention`, `field_cryptographic_shredding`, `tombstone_with_purge_window`, `other`) are substantively adequate under a specific jurisdiction's interpretation of erasure; the cross-border data-flow implications of an erasure event; or the interaction between Article 17 and Article 19 (notification to recipients) or Article 5(2) accountability. The redaction-event schema structures the input the deployer's counsel relies upon; the substantive determinations are made by the deployer's qualified personnel — counsel admitted in the relevant jurisdiction, the deployer's Data Protection Officer, the deployer's AI governance function, and where applicable the relevant supervisory authority.

A.3 EU AI Act — Article 50 (Transparency Obligations for Providers and Deployers)

A.3.1 What Article 50 requires

Regulation (EU) 2024/1689, Article 50 imposes transparency obligations on providers and deployers of certain AI systems whose output is delivered to natural persons. The article addresses four cases: providers of AI systems intended to interact directly with natural persons (Article 50(1)); providers of AI systems generating

synthetic audio, image, video, or text content (Article 50(2)); deployers of emotion-recognition or biometric-categorisation systems (Article 50(3)); and deployers of AI systems that generate or manipulate image, audio, or video content constituting a deep fake (Article 50(4)) or text published with the purpose of informing the public on matters of public interest (Article 50(4) second sub-paragraph). The transparency obligations are operationalised through disclosure. Natural persons interacting with the AI system or being exposed to its output are informed of the AI involvement in a clear and distinguishable manner, at the latest at the time of the first interaction or exposure.

Article 50's deployer-side transparency obligation is precisely the obligation Mode 2 dispatch under this Standard intersects with. A Mode 2 artifact is, by definition, a decision summary, recommendation, decision-aid, draft, classification, or other content where the AI system is the author of record. That artifact may reach a natural person, who is therefore entitled to disclosure under Article 50.

A.3.2 Cross-reference to Section 4 §4.6 (verbatim conformance language)

The substantive Article 50 conformance language for this Standard is carried by **Section 4 §4.6** (Authority and Authorship in AI-Mediated Decisions — Article 50 Conformance), into which the Article 50 conformance pre-draft flows verbatim. Section 4 §4.6 carries four things. First, the extraterritorial-reach scoping rule that binds deployers incorporated outside the EU whose Mode 2 outputs reach EU natural persons. Second, the five required transparency-disclosure metadata fields the Charter must attach to every Mode 2 artifact (`declaring-authority`, `ai-system-identity`, `jurisdictional-applicability-tag`, `content-type-tag`, `generation-timestamp`). Third, the Conformance Level 2 conformance test for transparency-disclosure metadata. Fourth, the Mode 1 edge case: embedded AI-generated content within an otherwise Mode 1 artifact carries Section 4 §4.6 transparency-disclosure metadata at the embed point, irrespective of the container's Mode 1 classification. **Section A.3 does not reproduce the Section 4 §4.6 conformance language.** Reproduction would create dual-source drift risk; the Section 4 surface is canonical and §A.3 cross-references it.

The Mode 1 edge case is referenced from Section 4 §4.7 (Mode-Drift Composed Mitigation). Section A.3 cites the cross-reference without reproducing the rule. Readers needing the operative Mode 1 edge-case rule consult Section 4 §4.7; readers needing the Article 50 conformance test consult Section 4 §4.6.

A.3.3 How the Standard's primitives map (summary; full mapping in Section 4)

The summary mapping, with full normative text in Section 4:

- **Mode 2 dispatch is the trigger.** Every Mode 2 artifact under a Charter governed by this Standard is within the scope of Section 4 §4.6 transparency-disclosure metadata. The disclosure metadata schema (Section 4 §4.6) is the **structural shape** of the inputs Article 50 requires the deployer to surface to the natural person. The schema does not generate, approve, or substitute for the disclosure text itself, which the named declaring authority approves per Section 4 §4.6 field `disclosure_text_pointer`.
- **Extraterritorial reach is binding by default.** Per Section 4 §4.6, deployers of Charters under this Standard whose Mode 2 outputs reach or are reasonably foreseeable to reach EU natural persons are within scope,

regardless of the deployer's jurisdiction of incorporation. Deployers verifiably outside the reach must declare the exclusion in their Charter. Absent declaration, the conformance requirement applies.

- **Mode 1 edge case is content-level, not container-level.** Embedded AI-generated content inside an otherwise Mode 1 artifact is Mode 2 content at the embed point; Section 4 §4.7 carries the operative rule.
- **Conformance Level 2 requires complete metadata.** A Charter producing Mode 2 artifacts without complete Section 4 §4.6 transparency-disclosure metadata cannot claim Conformance Level 2 (see Section 7 for the conformance-level criteria).

A.3.4 Non-claim

The Decision Provenance Standard does not satisfy, ensure, or certify any obligation under Regulation (EU) 2024/1689 Article 50. The Standard's transparency-disclosure metadata schema (Section 4 §4.6) **structures** the inputs the named declaring authority — a natural person — uses to discharge the Article 50 disclosure obligation; the schema does not discharge the obligation itself. The Standard does not opine on any of the following: whether a specific Mode 2 artifact is within Article 50's substantive scope (e.g., whether a particular text is "published with the purpose of informing the public on matters of public interest"); the form, language, accessibility, or timing of the disclosure text the declaring authority must produce; the interaction between Article 50 and Article 6 (high-risk classification), Article 22 GDPR (automated decision-making with legal effect on the natural person), or member-state-level transparency requirements that may apply additionally; phased-applicability questions for Mode 2 artifacts produced before the Article 50 phased-applicability date but circulated after it; or the allocation of liability between the Charter deployer (declaring authority) and the third-party AI-system vendor whose output the Charter governs. Those determinations are made by the deployer's qualified personnel — counsel admitted in the relevant jurisdiction (including counsel familiar with EU AI Act Article 50 and any applicable member-state transposition or implementing measures) and the deployer's AI governance function. The Standard structures the inputs; the named declaring authority and the deployer's qualified personnel discharge the obligation.

A.4 NIST AI Risk Management Framework — Manage 4.1

A.4.1 What the AI RMF and Manage 4.1 require

The U.S. National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (AI RMF 1.0, NIST AI 100-1, January 2023) is a U.S. **voluntary** framework. It structures how organizations identify, measure, and manage risks associated with the design, development, deployment, and use of AI systems. The framework is organized around four core functions — Govern, Map, Measure, Manage — each of which decomposes into categories and sub-categories of recommended outcomes. The Generative AI Profile companion (NIST AI 600-1, July 2024) is a companion document, not a successor version; AI RMF 1.0 remains the operative framework version this sub-section engages with.

The Manage function addresses how identified and measured AI risks are responded to, allocated, and tracked over time. **Manage 4.1**, in particular, addresses post-deployment AI system monitoring with continuous documentation. The sub-category articulates that organizations document how identified risks and impacts of AI systems are managed post-deployment, including responses to incidents and significant performance changes. Manage 4.1 frames continuous documentation as the substrate that enables an organization to demonstrate, over time, that its AI risk-management actions are responsive to actual deployment behavior rather than only to design-time assumptions.

A.4.2 How the Standard's primitives map

The Standard's decision-record schema (Section 6) and the Charter's schedule of records produce a structurally well-suited input substrate for Manage 4.1's continuous-documentation expectation. Specifically:

The schedule of records is a continuous-documentation commitment. A Charter under Section 3 commits, at `fields-completed` state, to maintain a `schedule_of_records` — the enumerated set of decision records the Charter will produce as decisions dispatch under it. The schedule is not a sample; it is the committed superset. Every decision dispatched under the Charter becomes a record; no decision in the class is silently undocumented. Manage 4.1 expects that AI risk management is documented continuously and not only at incidents. That expectation maps directly onto the schedule-of-records commitment: the Charter is the structural primitive that converts ad-hoc post-deployment documentation into committed continuous documentation.

The decision-record schema captures dispatch mode, inputs, reviewers, and sign-offs. Section 6 of the Standard defines the fields a decision record carries — including the dispatch mode (Mode 1 / Mode 2), the named author of record or reviewer of record, the inputs the decision drew on, the sign-off, and the closure timestamp. For a deployer operating a Charter that uses an AI system inside Mode 1 enforcement or Mode 2 authorship, each decision record is a structured documentation event. It captures how the AI system's contribution was used in the decision, who reviewed or authored, and what inputs the decision considered. Manage 4.1 expects that responses to incidents and significant performance changes are documented, and this maps onto the decision-record schema. Incidents and performance changes that surface inside re-decision triggers (Section 3 field `re_decision_triggers`) re-open a decision for review. The re-opened decision produces a new decision record under the same Charter, and the resulting record is a structured documentation event recording the response.

Re-decision triggers are the structural shape of "significant performance change" sensitivity. Section 3 of the Standard requires every Charter to declare at minimum one outcome-evidence trigger and one market-evidence trigger that re-open decisions under the Charter for review. Manage 4.1's continuous-documentation expectation presumes the organization is sensitive to post-deployment signals. The re-decision trigger is the named structural commitment a Charter makes to act on those signals when they fire. The trigger is not a substitute for the deployer's AI risk-management function. It is the structural input that function uses to demonstrate that the deployer's decision-making was responsive to the post-deployment evidence the AI RMF Manage function expects organizations to monitor.

A.4.3 Non-claim

The Decision Provenance Standard does not satisfy, ensure, or certify any outcome under the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0, NIST AI 100-1, January 2023), including under the Manage function and Manage 4.1 specifically. The AI RMF is a voluntary framework; it does not impose obligations and is not certified or attested in the manner of statutory or accredited frameworks. The Standard does not opine on any of the following: whether a deployer's broader AI risk management program meets the AI RMF's Govern, Map, Measure, or Manage functional outcomes; whether Manage 4.1's continuous-documentation expectation is met for AI systems outside the decision class governed by a Charter under this Standard; the interaction between AI RMF 1.0 and the NIST AI 600-1 Generative AI Profile companion for generative-AI-specific risk categories; the cross-walk between AI RMF Manage outcomes and the Standard's conformance levels (Section 7); or whether the deployer's AI risk management function has the necessary resourcing, organizational placement, and authority to act on the documentation the Charter and decision records produce. Those determinations are made by the deployer's qualified personnel — the AI risk management function, internal audit, and where applicable counsel admitted in the relevant U.S. jurisdiction. The Standard structures the inputs; the deployer's qualified personnel make the determinations.

A.5 ISO/IEC 42001:2023 — AI Management Systems

A.5.1 What ISO/IEC 42001:2023 certifies

ISO/IEC 42001:2023 — *Information technology — Artificial intelligence — Management system — Requirements* (rendered per the ISO catalog form per Appendix G §12.2.1) is an international management-system standard. It specifies requirements for establishing, implementing, maintaining, and continually improving an artificial-intelligence management system (AIMS) within an organization. The standard follows the harmonized ISO management-system structure (Annex SL). It specifies requirements on the context of the organization, leadership and commitment, planning, support, operation, performance evaluation, and improvement, applied to the management of AI systems and their related risks, opportunities, and impacts.

ISO/IEC 42001 is **certifiable**. An accredited certification body conducts a third-party audit against the standard and, where the AIMS conforms, issues a certificate. Certification is a determination by the certification body about the AIMS as a whole; it is not a determination about any individual AI system, decision, or artifact. The locus of certification is the management system — the organization's structures, policies, processes, roles, competence, and continual-improvement mechanisms for managing AI risks and opportunities — not any one output the management system produces.

A.5.2 How the Standard's primitives map (Charter mechanism as one input among many)

The Decision Provenance Standard's Charter mechanism (Section 3) and decision-record schema (Section 6) are **one input among many** to a deployer's AIMS conformance assessment under ISO/IEC 42001:2023. The mapping runs through three points of intersection:

The Charter mechanism is a process artifact within the AIMS scope, where the AIMS includes governed decision-making about AI use. ISO/IEC 42001 §6 (Planning) and §7 (Support) require the organization to determine the processes needed for the AIMS, the resources and competence necessary, and the documented information required. Some AIMS scopes include governed decision-making about the use of AI systems inside business decisions, and not all do. Where the scope does, the Charter mechanism is a process artifact the organization can declare as part of its AIMS documented information. It is the structural primitive that records the organization's commitment to a documented decision-making mechanism for AI-mediated decisions. The Charter is not an AIMS; it is a process artifact within an AIMS.

The decision-record schedule is documented information per Annex SL clause 7.5. The schedule of records (Section 6) is documented information about the operation of the Charter-governed decision-making process. ISO/IEC 42001 follows the Annex SL convention for documented information. The standard specifies what must be retained as documented information and how it must be controlled. Where a deployer chooses to integrate the Charter and its decision-record schedule into its AIMS, the schedule becomes documented information subject to the deployer's documented-information control procedures. The integration is a deployer choice, not a Standard claim.

The conformance levels (Section 7) are not ISO/IEC 42001 maturity levels. The Standard's conformance levels (Section 7, Levels 1–3) are tiers at which a Charter or decision record meets the Standard's structural requirements. They are not ISO/IEC 42001 maturity levels, and there is no defined cross-walk between them. A Charter's Conformance Level 3 declaration under the Standard does not translate into a corresponding AIMS performance evaluation outcome, and the Standard does not produce an AIMS conformance assessment by aggregating conformance-level declarations across Charters. Aggregation is a function of the AIMS, conducted by the deployer's qualified personnel.

A.5.3 Non-claim

The Decision Provenance Standard does not satisfy, ensure, or certify any requirement of ISO/IEC 42001:2023 — *Information technology — Artificial intelligence — Management system — Requirements*. The Standard does not produce an AI management system, does not produce an AIMS conformance assessment, and does not stand in any defined relationship to ISO/IEC 42001 certification. A deployer pursuing ISO/IEC 42001 certification engages an accredited certification body. That body conducts the third-party audit and issues the certificate where conformance is determined. The Standard's Charter and decision records are inputs the deployer's AIMS function and the certification body may, in their discretion, consider; they are not, and are not held out as, AIMS conformance evidence. The Standard does not opine on any of the following: AIMS scope determination; the design of the deployer's AI policy under ISO/IEC 42001 §5; the AI risk assessment under

§6.1; the AI system impact assessment requirements; the AIMS performance-evaluation regime under §9; or the cross-walk between ISO/IEC 42001 and the EU AI Act, NIST AI RMF, or any other framework. Those determinations are made by the deployer's qualified personnel — the AIMS function, internal audit, the accredited certification body, and counsel where applicable — independently of the Standard.

A.6 Caremark / Marchand v. Barnhill — Board-of-Directors Oversight Duties

A.6.1 Framework citation

Appendix G §12.2.3 cites *In re Caremark International Inc. Derivative Litigation*, Delaware Court of Chancery, 698 A.2d 959 (Del. Ch. 1996), with the neutral descriptor: "Delaware Court of Chancery decision in the subject domain of board-of-directors oversight duties under Delaware corporate law."

Appendix G §12.2.3 cites *Marchand v. Barnhill*, Supreme Court of Delaware, 212 A.3d 805 (Del. 2019), with the neutral descriptor: "Supreme Court of Delaware decision in the subject domain of board-of-directors oversight duties, decided in 2019."

The pointer URL for both decisions, per Appendix G §12.2.3, is `https://courts.delaware.gov/opinions/`.

A.6.2 Subject domain

The Caremark / Marchand line addresses, as its subject domain, the duties of directors of Delaware corporations with respect to the oversight of the corporations they serve. What those duties substantively require, how they are tested in litigation, what conduct discharges them, and what conduct fails them are matters of substantive Delaware corporate law that this sub-section does not characterize. Counsel admitted in Delaware performs that substantive analysis under the engagement letter applicable to the matter in front of them. Companion A's cross-reference is structural. It shows how the Standard's primitives produce the kind of audit-ready decision provenance a board, its committees, and its counsel may use as input when preparing their own oversight work product.

A.6.3 Primitives mapping

The Standard's primitives map onto the Caremark / Marchand subject domain as follows.

The Charter mechanism (Section 3) and the `accountable_owner` field. The Charter binds an organization to a decision-making mechanism for a recurring decision class, and the `accountable_owner` field (per Section 3) declares one and only one named human accountable for the Charter. A board may elevate certain decisions to Charter governance — board-reserved decision classes such as material capital allocation, major strategic commitments, compensation actions for the executive officer set, or decisions implicating the corporation's mission-critical operational risks. For those decisions, the Charter mechanism produces a structured record of

who held the decision-making authority, on what cadence the authority operated, what the inside-decisions / outside-decisions boundary was, and what re-decision triggers were declared at the time the decision was made. This structured record is the kind of material a board, board committee, or board-retained counsel may use as input when preparing oversight work product. The Charter mechanism does not, by its existence, discharge any board oversight duty. The discharge of the duty is performed by the board, through the board's own deliberative process, in conformity with the standards Delaware case law sets and counsel interprets.

The decision-record schema (Section 6) and the schedule of records. The decision-record schema produces a single instantiated record per decision under a Charter, capturing inputs, reviewers, dispatch mode, sign-offs, and the Charter under which the decision was made. The schedule of records is the enumerated set of decision records a Charter commits to maintain. Together, the per-decision record and the schedule produce continuous, non-event-driven documentation. From that documentation, a board, a board committee, or counsel may reconstruct the operational decision-making activity that surrounds matters the board is overseeing. The schedule is "findable in 30 seconds by someone not in the room" (the Standard's findability hygiene rule), and the records are structured rather than narrative. The cross-reference from individual records to the Charter under which they were dispatched permits a reviewer to traverse from a single decision back to the authority and process under which it was made. None of this discharges a board oversight duty. It produces a substrate counsel and the board may use as input.

Section 5 lifecycle: the affirmation-and-seal record on board-overseen decisions. Per Section 5, a decision record progresses from `draft` through `reviewed` to `affirmed`, and the `affirmed` event carries a seal binding the named affirming authority to the record state at affirmation. Where a Charter governs a board-overseen decision class, the lifecycle's affirmation event produces a sealed record. That record captures the moment the named authority took accountability for the decision as documented. The board, board committee, or board-retained counsel preparing oversight work product may consult the affirmation seal as input substrate documenting when and by whom the decision was bound. The lifecycle does not, by its existence, discharge any oversight duty; it produces the structural input the board's substantive review consumes.

The Mode 1 / Mode 2 dispatch state and the disclosure-metadata pointer. Some decisions in scope of board oversight involve AI-system contributions — whether as Mode 2 substantive authoring or as the Mode 1 edge case of an embedded AI-generated summary in a human-authored decision. For those decisions, the dispatch state and the Article 50 disclosure metadata block produce a structured record of what the AI system contributed, who the named declaring authority was, and what jurisdictional applicability the disclosure was scoped against. This record is potentially relevant to a board engaged in oversight of decisions where AI involvement is itself a matter of board-level concern. Whether the board's oversight obligation extends to this kind of decision, and what the board must do to discharge it, are again substantive matters for counsel. The Standard produces the structured record on top of which counsel and the board operate.

The conformance-level grading (Section 7). A Charter at conformance Level 3 (`level-3-continuously-auditable`) produces records on schedule, fires re-decision triggers when their conditions are met, and exports its schedule of records for counsel and auditor review. This continuous-by-design property is potentially relevant to a board that oversees a function whose operational decision-making activity is high-volume,

distributed, or otherwise difficult to reconstruct event-by-event. Level 3 is a structural conformance grade against the Standard; it is not a board oversight finding, and it does not certify that the board's duty has been discharged.

A.6.4 Non-claim

The Decision Provenance Standard does not constitute Caremark or Marchand compliance. It does not satisfy a board's oversight duties. It does not certify, attest, or otherwise opine that any board has adequately monitored mission-critical risks or established appropriate information systems. The legal sufficiency of any board's oversight under the Caremark / Marchand line is a substantive determination by counsel admitted in Delaware (or, where applicable, by a court adjudicating a derivative claim). The Standard's primitives are an input substrate. Whether and how a board, its counsel, and its committees use the substrate to support their own oversight work product is a determination the board and its counsel make, on their own engagement.

A.6.5 Reviewer / consumer note

The actor in the reader's organization who consumes the Standard's primitives in this cross-reference is, primarily, the corporate secretary's office (for Charter and schedule-of-records hygiene) and the board-retained counsel (for legal sufficiency analysis under Caremark / Marchand). The actor who performs the substantive oversight is the board itself, through its committees, in conformity with Delaware corporate law as interpreted by counsel admitted in the relevant jurisdiction.

A.7 COSO 2013 — Internal Control – Integrated Framework

A.7.1 Framework citation

Appendix G §12.2.2 cites the Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework*, 2013 edition, with the pointer URL `https://www.coso.org/guidance-on-ic` and the neutral descriptor: "U.S. internal-control framework articulating five components and seventeen principles used by organizations to design, implement, and assess internal control over financial reporting and over operations and compliance."

The five components named by the COSO 2013 framework are: Control Environment; Risk Assessment; Control Activities; Information and Communication; and Monitoring Activities. The framework articulates seventeen principles distributed across these components. This sub-section maps the Standard's primitives onto the five components at the component level; principle-level mapping is reserved for the reader's internal-controls personnel and external auditors operating under their own engagement letters, with one exception named at Monitoring Activities below where the alignment with Principles 16–17 is distinctive enough to surface.

A.7.2 Subject domain

COSO 2013 governs, as its subject domain, the design, implementation, and assessment of internal control by organizations operating in scope of the framework. The framework is voluntary in its issuance but is widely adopted. That adoption includes its use as the operative framework underlying U.S. management assessments of ICFR under SOX § 404 (see §A.8 below). What the framework substantively requires of any specific organization, what design or operating effectiveness deficiencies it identifies in any specific control environment, and what remediation it implies are matters the reader's internal-controls personnel and external auditors determine under their own professional standards. Companion A does not characterize those substantive requirements.

A.7.3 Primitives mapping

The Standard's primitives map onto the five COSO 2013 components as follows.

Control Environment. The Control Environment component addresses the tone, structures, processes, and standards that provide the basis for carrying out internal control across the organization. The Standard's Charter mechanism (Section 3) maps onto Control Environment as a documenting primitive. For the recurring decision classes a Charter governs, it documents the named accountable owner, the inside-decisions and outside-decisions boundary, the cadence on which decisions are made, and the escalation rule that is invoked when the Charter's conditions are exceeded. A Charter is not, in itself, a Control Environment artifact in the sense COSO uses the term. The structured commitments a Charter makes are, however, inputs internal-controls personnel may use when designing or assessing the entity-level control environment surrounding the decision class the Charter governs.

Risk Assessment. The Risk Assessment component addresses the identification, analysis, and management of risks relevant to the achievement of the entity's objectives. The Standard's `re_decision_triggers` field on the Charter (per Section 3) requires at minimum one outcome-evidence trigger and one market-evidence trigger. These triggers are the Standard's structural mechanism for ensuring that decisions made under a Charter are revisited when their underlying assumptions are stressed. This trigger structure is an input to the Risk Assessment component. The trigger declarations identify the risk events to which the Charter is sensitive, and the firing-and-record behavior produces records that internal-controls personnel may use when assessing whether risks identified at decision-time are being managed over time.

Control Activities. The Control Activities component addresses the policies, procedures, and other actions that help ensure management's directives are carried out. The Standard's Mode 1 / Mode 2 dispatch state machine (per Section 4) is a documenting primitive. For each decision under a Charter, it records which actor authored the substantive content, which actor reviewed it, and what dispatch-mode-specific control behaviors applied. The Mode 1 enforcer pattern (an AI worker checking a human's work against the Charter) and the Mode 2 disclosure block (Article 50 metadata attached at decision-close) are themselves a kind of structured control behavior that produces records consumable by internal-controls personnel.

Information and Communication. The Information and Communication component addresses the organization's mechanisms for obtaining, generating, and using relevant information to support the functioning of internal control. The Standard's schedule of records (per Section 6) is the primitive that maps most directly onto Information and Communication. The schedule is the enumerated set of decision records a Charter commits to maintain, located at a `record_location` that resolves and is queryable, with the Standard's findability rule applied. This is, by design, an Information-and-Communication-shaped artifact: structured, locatable, and traversable. Whether the schedule meets the COSO 2013 Information and Communication principles for the reader's specific internal control system is a determination the internal-controls personnel make.

Monitoring Activities. The Monitoring Activities component addresses ongoing evaluations, separate evaluations, or some combination of the two, used to ascertain whether each of the five components is present and functioning. The Standard's conformance-level grading (Section 7), and specifically the Level 3 grade (`level-3-continuously-auditable`), maps onto Monitoring Activities. It produces records on schedule, fires triggers when their conditions are met, and exports the schedule of records for review. The schedule of records is continuous-by-design: it is produced as a routine output of decision-making activity rather than as a special audit-event harvest. That property is structurally aligned with the COSO 2013 emphasis on ongoing evaluations integrated with operations rather than separate-evaluation-only monitoring. Per Section 5, each record in the schedule progresses through the lifecycle from `draft` to `affirmed`, and the affirmation event itself becomes a dated entry in the schedule of records. This supplies internal-controls personnel with a structured ongoing-evaluation evidence trail rather than a periodic-snapshot one. Again, whether the resulting records meet the Monitoring principles for the reader's specific internal control system is a determination the internal-controls personnel and external auditors make.

The Monitoring Activities component is the one place in this cross-reference where principle-level mapping illuminates the structural alignment more than the component-level summary alone. The Standard's continuous-by-design schedule of records is most distinctively aligned with COSO 2013 Principles 16 and 17. Principle 16 is that the organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. Principle 17 is that the organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors as appropriate. The Charter's `re_decision_triggers` and the schedule of records together produce the structural primitives that ongoing-evaluation-and-deficiency-communication work consumes. The triggers are the named conditions under which a decision is re-opened for review, and the schedule of records carries the resulting records as ongoing-evaluation evidence available for timely communication to the parties responsible. Principle-level mapping at the other four components (Control Environment, Risk Assessment, Control Activities, Information and Communication) is reserved for the deployer's internal-controls personnel; the Standard's primitives map onto those components at the component level only.

A.7.4 Non-claim

The Decision Provenance Standard does not constitute COSO 2013 compliance. The Charter mechanism, the decision-record schema, the Mode 1 / Mode 2 dispatch state, the schedule of records, and the conformance-level grading are not, individually or in combination, an internal control system. They are structured records of how recurring-class decisions are made and documented. An internal control system, in the COSO 2013 sense, encompasses substantially more than the structured records of decision activity. It includes the entity-level control environment, the operating-level control activities, the information systems, the monitoring functions, and the personnel who design, operate, and assess them. The Standard's primitives are an input substrate to that broader system, not a substitute for it. The design and operating effectiveness of the reader's internal control system, against COSO 2013 or any other framework, is a determination by qualified personnel under their own professional standards.

A.7.5 Reviewer / consumer note

The actor in the reader's organization who consumes the Standard's primitives in this cross-reference is the internal-controls function. That function sometimes resides within Internal Audit, sometimes within Finance, and sometimes within a dedicated internal-controls office. Where the organization is in scope of an external attestation, the external auditor also consumes the primitives. Both consume the records as input to their own work product. The Standard's role is to produce structured records; the reviewer's role is to evaluate whether those records, in context, support a conclusion about the reader's internal control system. The two roles are not interchangeable.

A.8 SOX § 404 — Management Assessment of Internal Control over Financial Reporting

A.8.1 Framework citation

Appendix G §12.2.2 cites the Sarbanes-Oxley Act of 2002, Public Law 107-204, Section 404 (Management Assessment of Internal Controls), enacted 30 July 2002 and codified at 15 U.S.C. § 7262, with the pointer URL `https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf` and the neutral descriptor: "U.S. federal statute, Section 404 of which addresses management assessment of internal control over financial reporting and the related external auditor attestation."

A.8.2 Subject domain and applicability scope

SOX § 404 governs, as its subject domain, the management assessment of internal control over financial reporting (ICFR) at issuers (subject to the Act's applicability) and the related external auditor attestation. Several questions fall to the reader's management, internal-controls personnel, and external auditors: what § 404 substantively requires, what control deficiencies it identifies in any specific issuer's ICFR, what disclosure

obligations attach to deficiencies of various severity classes, and what remediation it implies. They determine those matters under the Act, the related rules of the U.S. Securities and Exchange Commission, the Public Company Accounting Oversight Board (PCAOB) standards, and the engagement letters under which the auditors operate.

A scope note belongs at the top of this cross-reference. SOX § 404 is provider- and issuer-specific in its applicability. The Act applies, in the first instance, to issuers as defined in the Securities Exchange Act of 1934 — broadly, public companies whose securities are registered under the 1934 Act. Many organizations that adopt the Decision Provenance Standard are not issuers in this sense and are accordingly outside § 404's direct scope. Such organizations may engage with the Standard's primitives without § 404 being triggered. They may do so for their own internal control reasons, for service-organization assurance reasons (see §A.9 SOC 2), for board-oversight reasons (see §A.6 Caremark), or for their own internal-controls program reasons under COSO 2013 (see §A.7). Where a deployer's organization is — or expects to become — an issuer in scope of § 404, that deployer's management, internal-controls personnel, and external auditors verify § 404 applicability and scope against the engagement they operate under.

A.8.3 Primitives mapping

The Standard's primitives, where § 404 applicability has been independently established by the deployer's qualified personnel, map onto § 404 as follows. The mapping below assumes COSO 2013 as the underlying internal-control framework against which § 404 is evaluated, since COSO 2013 is the predominant framework adopted for this purpose by U.S. issuers. Where a different framework is used, the mapping is adjusted accordingly by the deployer's internal-controls personnel.

The Charter mechanism, the schedule of records, and the management assessment surface. The management assessment under § 404 is, in structural terms, an exercise of evaluating and documenting the design and operating effectiveness of ICFR over a defined period. For each in-scope decision class, the Standard's Charter mechanism produces a structural commitment: who the accountable owner is, what the inside / outside decision boundary is, and what re-decision triggers govern the decision class over time. The schedule of records produces the per-decision documentation as a routine output. Some decision classes are in scope of ICFR, for example revenue-recognition policy decisions, material accounting estimate decisions, and disclosure-judgment decisions. For those, the Charter mechanism and schedule of records produce structured records the management assessment may use as input when documenting the design and operating effectiveness of the controls surrounding those decision classes.

The decision-record schema and the audit-trail function. The decision-record schema produces a single, structured record per decision under a Charter, with sign-offs, reviewers, inputs, and the dispatch mode all captured at decision-close. Some § 404 ICFR controls are decision-shaped — controls in which a human or AI-assisted human reaches a judgment, applies a policy, or exercises an estimate. For those, the decision record is potentially relevant as part of the audit trail surrounding the control. Per Section 5, each record progresses through the lifecycle from `draft` through `reviewed` to `affirmed`. The `affirmed` event with its seal is itself a dated entry in the audit trail, capturing when the named authority bound the record state. This sealed-

affirmation event is the structural input the external auditor's audit-trail testing consumes; the record does not, by its existence, constitute an ICFR control. The control is the underlying judgment-and-review activity, of which the decision record is the structured documentation. Whether the documentation is sufficient for § 404 purposes is a determination the external auditor makes under PCAOB AS 2201 and the engagement letter the auditor operates under.

The Mode 1 / Mode 2 dispatch state and the AI-assisted-control surface. Some ICFR controls incorporate AI assistance — Mode 1 (a human author with AI checking the human's work against a Charter) or Mode 2 (AI authoring substantive content with human review). For those, the dispatch state and the Article 50 disclosure metadata block produce a structured record of what the AI contributed, who reviewed it, and what jurisdictional applicability applied. AI-assisted ICFR controls are an active subject in audit guidance, and the records the Standard produces are inputs the external auditor may consider when evaluating the design and operating effectiveness of such controls. They do not, by their existence, satisfy any audit standard. The auditor's evaluation is the determinative work; the records are the substrate that work consumes.

The conformance-level grading. A Charter at conformance Level 3 produces records continuously, fires triggers on schedule, and exports the schedule of records for review. Continuous-by-design documentation is an attribute internal-controls personnel and external auditors may consider when evaluating the operating effectiveness of a control over a period rather than at a point-in-time. Level 3 is a structural conformance grade against the Standard; it is not an ICFR design or operating-effectiveness conclusion. The conclusion is reached by the management assessment and the auditor attestation, on their own.

A.8.4 Non-claim

The Decision Provenance Standard does not constitute SOX § 404 compliance. It does not satisfy management's responsibility to assess ICFR or the external auditor's responsibility to attest to ICFR. It does not, individually or in combination with COSO 2013 or any other framework, produce a management assessment or an auditor attestation. The structured records the Standard produces are inputs to the assessment-and-attestation work performed by the deployer's management, internal-controls personnel, and external auditors. Those personnel and auditors operate under the Act, the SEC's rules, the PCAOB's standards, and the engagement letters under which they work. § 404 applicability to a specific organization is verified by the organization's qualified personnel, not by the Standard.

A.8.5 Reviewer / consumer note

Several actors in the reader's organization consume the Standard's primitives in this cross-reference: management (specifically, the principal executive officer and principal financial officer who certify the assessment under § 404), the internal-controls function, internal audit, and external audit. Where the reader's organization is not an issuer in scope of § 404, this cross-reference is informational rather than operational. The COSO 2013 cross-reference at §A.7 may still apply for the reader's own internal-controls program reasons.

A.9 SOC 2 Type II — AICPA Trust Services Criteria

A.9.1 Framework citation

Appendix G §12.2.2 cites the American Institute of Certified Public Accountants, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP Section 100, 2017 Trust Services Criteria, with 2022 revisions to Points of Focus), with the pointer URL `https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2` and the neutral descriptor: "U.S. assurance reporting framework under which an independent CPA evaluates and reports on the design and operating effectiveness of a service organization's controls relevant to security, availability, processing integrity, confidentiality, or privacy."

The Trust Services Criteria are organized into five categories: Security (the common criteria, applicable across all SOC 2 engagements); Availability; Processing Integrity; Confidentiality; and Privacy. A SOC 2 Type II report addresses the suitability of the design and the operating effectiveness of controls over a defined period, distinguishing it from a SOC 2 Type I report that addresses suitability of design at a point in time.

A.9.2 Subject domain

The AICPA Trust Services Criteria, in the form addressed by a SOC 2 Type II report, govern the assurance reporting on service-organization controls relevant to one or more of the five categories. Several questions fall to the service organization's management and the engaging service auditor (an independent CPA firm): what the criteria substantively require, what design or operating effectiveness deficiencies they identify in any specific service organization's control set, and what disclosure obligations attach to deficiencies. They determine those matters under the framework, the AICPA's professional standards (including AT-C Section 205 for SOC 2 examinations), and the engagement letter the service auditor operates under.

A.9.3 Primitives mapping

The Standard's primitives map onto the Trust Services Criteria as follows. The mapping is criterion-category-shaped rather than control-by-control, on the same logic as the COSO 2013 cross-reference at §A.7. Control-by-control mapping is a substantive exercise reserved for the reader's internal personnel and the engaged service auditor.

Common Criteria (Security). The Common Criteria address security, organized around control environment, communication and information, risk assessment, monitoring activities, and control activities (mirroring, in part, the COSO 2013 component structure). The Standard's Charter mechanism, schedule of records, and conformance-level grading map onto the Common Criteria along the same axes as the §A.7 COSO 2013 cross-reference. Some decision classes in scope of a SOC 2 Type II engagement are governed by a Charter — for example, decisions about access provisioning for sensitive systems, decisions about incident-response escalations, or decisions about security-control changes. For those, the Charter and the schedule of records produce structured records the service organization's management may use as input when describing its control environment and operating-effectiveness narrative to the service auditor. Per Section 5, each record

progresses through the lifecycle from `draft` to `affirmed`, and the affirmation event is itself a dated, sealed entry the service auditor may consult as operating-effectiveness evidence over the engagement period. The service auditor consumes the records as one of many inputs in the engagement.

Availability. The Availability category addresses controls relevant to the system being available for operation and use as committed or agreed. The Standard's primitives engage Availability in two ways. First, through the re-decision-trigger structure on the Charter: decisions about availability commitments, capacity planning, and incident-driven re-architecting are decision-class-shaped in many service organizations and benefit from Charter governance. Second, through the schedule of records' continuous-by-design property, which produces records of availability-relevant decisions across the engagement period rather than only at point-in-time intervals.

Processing Integrity. The Processing Integrity category addresses controls relevant to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing-Integrity-relevant decisions — for example, decisions about data validation rules, decisions about exception-handling, decisions about reconciliation cadence — are decision-class-shaped. They benefit from the Charter / decision-record / schedule-of-records primitive set in the same way as the Common Criteria and Availability mappings. The Mode 1 / Mode 2 dispatch state is potentially relevant where Processing Integrity controls incorporate AI assistance. An AI-assisted exception-handling control, for example, produces a Mode 1 or Mode 2 record set whose dispatch state and disclosure metadata are inputs the service auditor may evaluate as part of operating-effectiveness testing.

Confidentiality. The Confidentiality category addresses controls relevant to information designated as confidential being protected as committed or agreed. The Standard's primitives engage Confidentiality primarily through the schedule of records' `record_location` field and the resolvability requirement. The schedule must be locatable but, where applicable, must also respect access restrictions on the underlying records — a design point internal to the deployer's implementation of the schedule. The Charter `accountable_owner` field and the decision-record reviewer field are also potentially relevant where confidentiality-handling decisions are themselves under Charter governance.

Privacy. The Privacy category addresses controls relevant to the collection, use, retention, disclosure, and disposal of personal information. Privacy-relevant decisions — for example, decisions about lawful-basis declarations, decisions about retention-schedule commitments, decisions about data-subject-rights-request handling — are decision-class-shaped and benefit from Charter governance. The Article 50 disclosure metadata block (per Section 4 §4.6) is, in particular, the primitive most directly engaged where AI-system involvement in personal-information processing produces decisions that are themselves in scope of the Privacy category. The AI/ISO trio sub-section above (§A.1–§A.5) covers the Article 50 substantive engagement. This Privacy-category cross-reference is therefore limited to noting that the Article 50 metadata block produces structured records the service organization's management and the service auditor may consume as input when evaluating Privacy-category controls implicating AI systems. The substantive Article 50 engagement lives at §A.3 above.

A.9.4 Type I vs Type II distinction

A SOC 2 Type I report addresses the suitability of the design of controls at a point in time. A SOC 2 Type II report addresses both the suitability of design and the operating effectiveness of controls over a defined period (commonly six or twelve months). The Standard's schedule of records is continuous-by-design. Records are produced as a routine output of decision-making activity, on the cadence the Charter declares, with re-decision triggers firing on their conditions and producing back-pointed records. The schedule is therefore structurally aligned with the operating-effectiveness-over-period evaluation a SOC 2 Type II engagement performs. A Charter at conformance Level 3 (`level-3-continuously-auditable`) produces records continuously and exports the schedule of records for review; this aligns more naturally with Type II evaluation than with Type I. None of this satisfies a Type II engagement; the alignment is structural, and the engagement is performed by the service auditor under AT-C Section 205 and the engagement letter.

A.9.5 Non-claim

The Decision Provenance Standard does not constitute SOC 2 Type II compliance and does not produce a SOC 2 Type II report. The Charter mechanism, the decision-record schema, the Mode 1 / Mode 2 dispatch state, the Article 50 disclosure metadata block, the schedule of records, and the conformance-level grading are not, individually or in combination, a control set. They are structured records of how recurring-class decisions are made and documented. They are also an input substrate: the service organization's management may use them when describing its controls to the service auditor, and the service auditor may consume them as one input among many in the engagement. The opinion the SOC 2 Type II report communicates is the service auditor's opinion, reached under the Trust Services Criteria, the AICPA's professional standards, and the engagement letter — not the Standard's.

A.9.6 Reviewer / consumer note

Three actors consume the Standard's primitives in this cross-reference. The first is the service organization's management, who prepares the system description and the assertions on which the engagement is performed. The second is the internal-controls or security-and-compliance function, which often coordinates the engagement internally. The third, externally, is the engaged service auditor — an independent CPA firm operating under AT-C Section 205. The structured records the Standard produces are inputs to all three. The determinative work product (the system description, the management's assertions, and the service auditor's opinion) is the responsibility of those actors.

A.10 Cross-Cutting Notes

A.10.1 The "input substrate" framing

Across all nine cross-references in this Companion, the Standard's primitives function as an **input substrate**. They are structured records that compliance, audit, and governance personnel may use when preparing their

own work product. The framing is consistent because the underlying logic is consistent. The Standard documents process; counsel, auditors, and internal-controls personnel make substantive determinations. Decision provenance is upstream of those determinations; it is not the determinations themselves.

This framing is not a diminution of what the Standard does. Producing structured, locatable, traversable records of how decisions are made, by whom, against which inputs, with what review, is a non-trivial discipline — and it is, by design, the discipline that most directly produces the kind of material counsel and auditors find useful. The framing is, however, an honest scope statement. The Standard is what it is; it is not what it is not.

A.10.2 Boundary between the AI/ISO trio and the traditional frameworks

The AI/ISO trio sub-section above (§A.1–§A.5) addresses EU AI Act Articles 14 (Human Oversight), 17 (Quality Management System), and 50 (Transparency); NIST AI RMF Manage 4.1; and ISO/IEC 42001:2023. The traditional-frameworks sub-section (§A.6–§A.9) addresses Caremark / Marchand; COSO 2013; SOX § 404; and SOC 2 Type II. EU AI Act Article 14 (Human Oversight), in particular, sits at §A.1 within the AI/ISO trio and is not addressed in §A.6–§A.9. Where the Caremark / Marchand cross-reference at §A.6 touches board-level AI oversight, the structural engagement is with the Delaware corporate-law oversight duty. The EU AI Act human-oversight obligation, where it is in scope for a deployer, is engaged at §A.1.

The two sub-sections are designed to be read in sequence, in either order, without overlap. A reader engaging with AI-specific frameworks reads §A.1–§A.5 in priority; a reader engaging with traditional internal-control and oversight frameworks reads §A.6–§A.9 in priority; a reader engaging with both reads the full Companion.

A.10.3 Jurisdictional analogues

The traditional frameworks engaged in §A.6–§A.9 are predominantly U.S. in origin. Readers operating in jurisdictions other than the U.S. may have local analogues. In the United Kingdom, common reference points are the Corporate Governance Code (governance), ISA 315 and ISA 330 in lieu of COSO + SOX (internal-control assurance), and ISAE 3402 (service-organization assurance). In the European Union, the various national corporate governance codes and the European Sustainability Reporting Standards' internal-control implications are relevant. In Israel, Companies Law obligations and ISA-based assurance frameworks apply. This Companion does not engage those analogues. Where a reader's matter concerns a non-U.S. jurisdiction, the cross-reference engagement with local analogues is performed by the reader's counsel admitted in that jurisdiction. The AI/ISO trio's primary anchor is the EU AI Act (already in scope as a named secondary jurisdiction per Section 1 §1.6); jurisdictional analogues for the trio surface as the deployer's matter requires.

A.10.4 Phased applicability and currency

Three phased-applicability and currency notes apply across this Companion.

First, SOX § 404 applicability has phasing of its own. Smaller reporting companies have differing § 404(b) external-auditor-attestation obligations than accelerated filers and large accelerated filers under SEC rules. Where the deployer's organization is in or near a phasing transition, the deployer's qualified personnel verify the applicable obligations against the SEC's rules and the engagement letter under which the auditor operates.

Second, COSO 2013 is the operative edition cited by Appendix G §12.2.2 and the version this Companion maps onto. If COSO issues a revision to the Internal Control – Integrated Framework that supersedes the 2013 edition between this Companion's verification and the Standard's publication, Appendix G §12.5.1 governs the version-specific re-verification responsibility, and this Companion is updated accordingly.

Third, PCAOB and AICPA guidance on AI-assisted controls is evolving; any specific engagement applies the guidance current at engagement time. The mapping in §A.8 (SOX § 404) and §A.9 (SOC 2 Type II) above engages the dispatch state and the Article 50 disclosure metadata block as inputs an external auditor may consider when evaluating AI-assisted ICFR or service-organization controls. What specific PCAOB AS or AICPA AT-C requirement governs the auditor's evaluation in any given engagement is determined under the guidance current at engagement time, not under the Standard. This currency caveat is also the reason the corresponding Cannot-Assess-Without item below remains live across the publication horizon: AI-assisted-controls audit guidance is a moving target the Standard does not, and cannot, lock to.

A.bis Other-Jurisdiction Erasure-Right Cross-References

The §5.5 redaction-event record pattern and the §6.2.3 redaction-event schema accommodate erasure-right regimes beyond GDPR Article 17 (engaged at §A.2.bis above). This sub-section briefly cross-references the parallel regimes the schema's `redaction_basis` enum (§6.2.3) accommodates. The cross-reference is uniform across regimes. Erasure operates on the operational data store. The archival record is preserved under a named legal basis that the deployer's counsel selects. The redaction-event record documents both. The Standard structures the input; the deployer's counsel applies the substantive jurisdictional rule.

United Kingdom — UK GDPR + Data Protection Act 2018. Following the UK's departure from the EU, the right of erasure under UK GDPR Article 17 mirrors EU GDPR Article 17 in substance, with the Data Protection Act 2018 providing supplementary provisions. The redaction-event schema accommodates a UK-basis redaction by setting `redaction_basis` to `uk_dpa_2018_erasure`. Where a deployer is subject to both EU GDPR and UK GDPR, the redaction event SHOULD be authored against the more demanding standard.

California — CCPA / CPRA. California Civil Code §1798.105 grants California consumers the right to request deletion of personal information. §1798.105(d) enumerates exceptions. These include completing the transaction, detecting security incidents, exercising free speech, complying with a legal obligation, and using the information for internal uses consistent with consumer expectations. The redaction-event schema accommodates a CCPA-basis redaction by setting `redaction_basis` to `ccpa_right_to_delete` (or `cpra_right_to_delete` where the CPRA expansion is the operative basis) and populating `archival_record_retention_basis` with the named exception.

Israel — Protection of Privacy Law 5741-1981. Israel's PPL 5741, as amended (including the 2024 amendments expanding data-subject rights), establishes a right to request correction or deletion of personal data. The redaction-event schema accommodates an Israeli-basis redaction by setting `redaction_basis` to `israeli_privacy_law_erasure`.

Brazil (LGPD), China (PIPL), South Africa (POPIA), Quebec (Law 25), U.S. state consumer laws. Each of these regimes establishes some form of erasure or deletion right. The `redaction_basis` enum carries discrete values for the major regimes (`lgpd_article_18`, `pipl_article_47`, `popia_erasure`, `quebec_law_25_erasure`). It also carries an umbrella value (`us_state_consumer_law_erasure`) for proliferating U.S. state regimes (Virginia CDPA, Colorado CPA, Connecticut CTDPA, and parallel regimes). The `other_named_statute` value with `redaction_basis_detail` accommodates regimes not enumerated.

Non-claim. The Standard does not opine on any of the following: whether any specific data-subject request is substantively valid under any specific regime; the position of any individual regulator (UK ICO, California Privacy Protection Agency, Israeli Privacy Protection Authority, Brazilian ANPD, China CAC, or others) on the redaction-as-new-affirmed-record framing; or the substantive adequacy of any specific `deletion_method` under any specific jurisdiction's interpretation. Deployers operating in regimes not enumerated SHOULD use `other_named_statute` with the specific statute named in `redaction_basis_detail`, and the substantive determination is the deployer's counsel's. The Standard records the deployer's selection; the deployer's qualified personnel discharge the obligation.

A.11 HR-Side Framework Cross-References

The cross-references in §A.1–§A.10 address AI-governance frameworks (EU AI Act Articles 14, 17, 50; NIST AI RMF; ISO/IEC 42001) and the traditional internal-control / oversight backbone (Caremark / Marchand; COSO 2013; SOX § 404; SOC 2). This subsection §A.11 addresses the HR-side regulatory regimes. Those regimes engage when the Standard's records describe natural persons at sub-executive altitudes, per the §3 use-case scope-limit declaration and the Appendix G §G.11.3 per-altitude consent posture. The locked §A.0 lead paragraph ("Decision Provenance Standard records inform — without satisfying — regulatory frameworks") governs every cross-reference in §A.11 without paraphrase.

NYC Local Law 144 — Automated Employment Decision Tools. NYC LL 144 imposes bias-audit, public-summary, and candidate-notice obligations on AEDTs used in hiring, promotion, retention, or termination decisions in NYC. A deployer using Decision Provenance Standard records as input to an AEDT under NYC LL 144's scope is the AEDT operator. The AEDT bias-audit, public-summary, and candidate-notice obligations belong to the deployer. The Standard's records inform the deployer's AEDT bias-audit work; they do not satisfy NYC LL 144.

Colorado SB 24-205 / Illinois HB 3773 / California ADMT (proposed CPPA regs). State-level employment-AI regimes impose risk-assessment, anti-discrimination, and notice-and-explanation obligations on consequential employment decisions made or substantially assisted by automated systems. The Standard's records inform the deployer's risk-assessment and notice-and-explanation work; they do not satisfy any state-level regime.

EU AI Act Annex III (employment-side high-risk classifications). EU AI Act Annex III names employment-side AI systems (recruitment, performance evaluation, work allocation, monitoring) as high-risk. A deployer using Decision Provenance Standard records as input to a high-risk Annex III system is subject to the EU AI Act's high-

risk-system obligations under Articles 8–17. The Standard's records inform the deployer's Annex III conformity-assessment work; they do not satisfy the EU AI Act.

EU GDPR Article 22 — Automated individual decision-making. GDPR Article 22 imposes constraints on decisions based solely on automated processing producing legal or similarly significant effects on a natural person. Those constraints include explicit consent, human-in-the-loop guarantees, and Article 22(3) safeguards. A deployer using Decision Provenance Standard records as input to an Article 22 decision is the controller, and the Article 22 obligations belong to the controller. The Standard's records inform the controller's Article 22 work; they do not satisfy GDPR.

EU Platform Work Directive. Where the deployer engages platform workers and uses Decision Provenance Standard records as input to algorithmic management decisions, the EU Platform Work Directive's transparency, consultation, and human-in-the-loop obligations apply. The Standard's records inform; they do not satisfy.

UK ICO Monitoring Guidance (2023). UK ICO guidance on workplace monitoring imposes proportionality, transparency, and consultation obligations on employer monitoring systems. A deployer whose Decision Provenance Standard installation monitors workers in the UK is subject to the guidance. The Standard's records inform; they do not satisfy.

Israel Privacy Protection Law 5741-1981 (employment data). Israel PPL 5741 and PPA opinions on employment data impose consent, purpose-limitation, and data-subject-rights obligations on employer data. The Standard's records inform; they do not satisfy.

Closing non-claim. The HR-side regulatory regimes named in this §A.11 have **direct private-right-of-action exposure** that the AI-governance regimes in §A.1–§A.5 largely do not yet have. The "informs without satisfying" firewall is **stricter** on the HR-side than on the AI-governance side because the litigation pathway is shorter. Adopting organizations remain responsible for their own HR-side regulatory posture; the Standard structures the inputs the deployer's HR-of-record, employment counsel, privacy counsel, and works councils consume. The Standard does NOT authorize, validate, certify, or recommend any deployer's use of Decision Provenance Standard records as input to employment decisions under any HR-side regime; the deployer's qualified personnel govern that use under the deployer's local law.