Regulatory Crosswalk

How the Decision Protocol method maps to NIST AI RMF 1.0 and ISO/IEC 42001:2023

A condensed mapping at the function-and-objective level, for executives evaluating the framework before adoption.

Version 0.2 · Restricted / Internal Review
decisionprotocolinstitute.com

SECTION

Why a Crosswalk

The buyer of an AI governance framework has two questions, in order. Is this serious? And will it operate in my environment? The first question is about credibility. The second is about whether the artifacts the framework produces can be presented as evidence under the standards the buyer's board, auditor, or regulator already recognizes.

This document answers the second. It maps every component of the Decision Protocol method to the two AI governance frameworks most likely to be raised in a North American procurement or audit conversation — NIST AI RMF 1.0 and ISO/IEC 42001:2023 — and discloses honestly where coverage is partial or out of scope.

A buyer who adopts the Decision Protocol does not become certified under either standard. What the buyer obtains is a documentation discipline whose outputs can be presented as evidence under both — and a vocabulary that translates directly between the two.

SECTION

The Three Operating Principles

The method rests on three operating principles. They are not the Institute's invention; they are what regulatory review, audit, internal inquiry, and litigation actually look for. Both NIST AI RMF and ISO 42001 are organized around the same expectations.

Contemporaneity. A defensible record is created before the consequences of a decision are known. Every Decision Protocol instrument is completed at the time the decision is taken and timestamped to ISO 8601, so contemporaneity is auditable.

Adequate Information. A defensible record documents that risks, alternatives, assumptions, and cognitive distortions were actively considered. The classification logic, triage questions, options analysis, and (in the Shielded tier) pre-mortem operationalize this.

Conscious Trade-Off. A defensible record names the risk accepted, the benefit sought, and the reason the trade-off was considered proportionate. Section §6 of every Decision Record is a recorded trade-off statement.

SECTION

Coverage at a Glance

NIST AI RMF 1.0 (4 FUNCTIONS, 19 CATEGORIES, 72 SUBCATEGORIES)

Function	Coverage
GOVERN — culture of AI risk management, accountability, supply chain	Strong. 13 of 19 subcategories Direct, 5 Partial, 1 Out of scope.
MAP — establishing the context in which AI risks arise	Strong. 11 of 18 subcategories Direct, 6 Partial, 1 Out of scope.
MEASURE — technical evaluation of AI systems (TEVV)	By design largely out of scope. 1 of 22 subcategories Direct, 7 Partial, 14 Out
MANAGE — risk treatment, decommissioning, post-deployment	Strong. 7 of 13 subcategories Direct, 6 Partial.

The Decision Protocol's design intent is reflected in this asymmetry. It is built to be strong on governance, classification, decision documentation, and accountability — and intentionally minimal on technical model evaluation and on external stakeholder mechanisms, which are responsibilities of the vendor, the developer, or the adopter's privacy, communications, and legal functions.

ISO/IEC 42001:2023 (7 MANAGEMENT-SYSTEM CLAUSES + 38 ANNEX A CONTROLS IN 9 OBJECT

ISO 42001 area	Coverage
Clauses 4–8 Context · Leadership · Planning · Support · Operation	Strong. All Direct. The Scoping Memorandum (Agency Edition), the AUP and
Clauses 9–10 Performance evaluation · Improvement	PARTIAL
A.2 Policies related to AI (3 controls)	DIRECT
A.3 Internal organisation (2 controls)	DIRECT
A.4 Resources for AI systems (5 controls)	DIRECT
A.5 Assessing impacts of AI systems (4 controls)	DIRECT
A.6 AI system life cycle (9 controls)	Asymmetric. Strong on the deployment and operation end of the lifecycle (A.6
A.7 Data for AI systems (5 controls)	DIRECT
A.8 Information for interested parties (4 controls)	DIRECT
A.9 Use of AI systems (3 controls)	DIRECT

ISO 42001 area	Coverage
A.10 Third-party and customer relationships (3 controls)	DIRECT

Aggregate ISO 42001: of 38 Annex A controls plus 7 management-system clauses, the Decision Protocol provides Direct coverage for 22 (49%), Partial coverage for 16 (36%), and is Out of scope for 7 (16%).

SECTION

Where Coverage is Strongest

The Decision Protocol's coverage concentrates where audit committees, regulators, and counsel actually demand evidence:

- AI policy and use governance (NIST GOVERN 1.x; ISO 42001 A.2, A.9). The AI Acceptable Use Policy and the Triage Tool are the artifacts that close the gap between we have a policy and we can show the decision record.
- Vendor and third-party governance (NIST GOVERN 6.x, MANAGE 3.x; ISO 42001 A.10). The AI Vendor Review Checklist's six domains — with concrete sub-criteria including AES-256, TLS 1.2+, SOC 2 Type II, 72-hour breach notification, 30-day post-termination deletion — operate as a procurement gate that closes before any data is shared.
- Decision-record discipline (NIST GOVERN 1.4, 4.2; MAP 3.x; MANAGE 1.x; ISO 42001 A.5.2–A.5.4, clause 8). The 9-section Decision Record schema — combined with the three-tier proportionality (Express / Standard / Shielded) — is the artifact a regulator or plaintiff's counsel asks to see when the question becomes show me how you reasoned this at the time.
- Accountability and oversight (NIST GOVERN 2.x, 3.2; ISO 42001 A.3, clause 5). The Control Ownership & Approval Matrix and the Vendor Escalation Matrix make explicit who approves what, with five named governance roles and three escalation thresholds.

SECTION

Where Coverage is Out of Scope (Honest Gaps)

The Decision Protocol does not deliver, and is not intended to deliver, the following:

1. Continuous post-deployment performance monitoring. DPI provides the governance trigger and the audit-ready record schema; technical drift detection and telemetry are the adopter's MLOps or vendor-supplied infrastructure. 2. Adversarial testing and red-teaming. The Shielded tier captures a bias audit and a pre-mortem; neither is an adversarial test. Where required, this is a separate workstream. 3. Quantitative model performance metrics. DPI is qualitative governance; the metrics themselves are the data science function's or vendor's TEVV evidence. 4. Incident response procedures. DPI defines escalation triggers and the governance pathway into incident review; the IR runbook itself integrates with the adopter's existing security incident response capability. 5. Transparency to data subjects and affected parties. Shadow AI disclosure is internal; external-facing transparency is the adopter's privacy office and counsel.

These gaps are not defects. They are choices about what a documentation discipline should and should not try to be. The Decision Protocol is the spine — the governance documentation that ties together the adopter's existing technical, legal, and operational capabilities. It is not a substitute for those capabilities.

SECTION

How to Use This Document

For an executive, this summary answers: if my internal auditor or external counsel asks how the framework maps to a recognized standard, what can I show them? The full crosswalk gives the line-by-line answer, including direct citations to NIST subcategory codes and ISO Annex A control identifiers.

For an advisor, this summary is the conversation opener. The full crosswalk, under the Agency Edition license, can be reproduced under the firm's branding when it is delivered to a client.

For an internal auditor, the records produced by the Decision Protocol are direct evidence for the subcategories and controls marked Direct in the full crosswalk; corroborating evidence for those marked Partial; and explicitly Out of scope for those marked as such — each of which the adopter is expected to address through other capabilities.

The full subcategory-level mapping document — Volume 1 of 2 · NIST AI RMF 1.0 and ISO/IEC 42001:2023 — is available on request via decisionprotocolinstitute.com. Volume 2 extends the mapping to the EU AI Act (Regulation 2024/1689) and Federal Reserve SR 26-2 (the Revised Guidance on Model Risk Management issued jointly with OCC Bulletin 2026-13 and the FDIC on April 17, 2026, which supersedes SR 11-7).

SECTION

Document Status

DOCUMENT STATUS	
Title	DPI Regulatory Crosswalk — Executive Summary
Companion	DPI Regulatory Crosswalk Volume 1 of 2 (full subcategory mapping)
Version	0.2 (Draft, internal review)
Date	April 2026
Author	The Decision Protocol Institute
Founder	Lamberto Iezzi — see decisionprotocolinstitute.com/our-mission for background
Standards referenced	NIST AI 100-1 (AI RMF 1.0, January 2023). ISO/IEC 42001:2023 (December 2023).
Disclaimer	Educational and procurement-evaluation document. Not a certification, audit, or legal opin…

THE DECISION PROTOCOL INSTITUTE™

Regulatory Crosswalk

Executive Summary · Confidential

This summary accompanies the full two-volume crosswalk and is provided for evaluation purposes only. Not for redistribution or reproduction.

decisionprotocolinstitute.com