GAISB

GLOBAL AI STANDARDS BODY

THE ALIGNMENT DOSSIER — VOLUME I

EDITION 1.0 / 2026

EFFECTIVE 01 Q2 2026

REVIEW CYCLE: ANNUAL

The CAIS & *ISO/IEC 42001* Alignment Dossier

How the Certified Artificial Intelligence Strategist credential maps to the international AI Management System standard — clause by clause, control by control.

COMPANION DOCUMENT TO

The CAIS Common Body of Knowledge, Edition 1.0

GOVERNED BY THE GAISB STANDARDS COUNCIL

PUBLIC DOCUMENT · CITE WITH ATTRIBUTION

ISSUED UNDER ISO/IEC 17024 PRINCIPLES

42001

AI MANAGEMENT SYSTEM · ISO/IEC

FRONT MATTER · DOCUMENT PURPOSE

Purpose of this Dossier

This dossier establishes the formal alignment between the CAIS professional certification and ISO/IEC 42001:2023 — the international standard for Artificial Intelligence Management Systems.

WHAT THIS DOCUMENT IS

A clause-by-clause and control-by-control mapping that demonstrates how CAIS-certified professionals provide the competency evidence required by organizations implementing and maintaining an AI Management System in conformance with ISO/IEC 42001.

WHAT THIS DOCUMENT IS NOT

This is not an ISO/IEC 42001 certification. Organizational conformance to ISO/IEC 42001 is achieved only through third-party audit conducted by an accredited certification body. This dossier provides the **personnel competence evidence layer** within that broader organizational effort.

WHO THIS DOCUMENT IS FOR

- **Chief AI Officers and AI Governance Leaders** preparing their organizations for ISO/IEC 42001 certification, defining internal competency frameworks, or documenting workforce readiness.
- **ISO/IEC 42001 Certification Bodies** seeking a published, structured personnel-competence reference during audit engagements.
- **Procurement, Legal, and Risk Officers** evaluating AI-vendor contracts that reference ISO/IEC 42001 requirements and need a defensible competency benchmark.
- **HR and Learning & Development teams** building upskilling programs whose outcomes must satisfy ISO/IEC 42001 Clause 7.2 (Competence).
- **Regulators and policymakers** assessing the interoperability of professional credentials with international AI management system standards.

> **PRIMARY CONFORMANCE STATEMENT**
>
> The CAIS credential provides **direct competence evidence** satisfying ISO/IEC 42001:2023 **Clause 7.2 (Competence)** and Annex A control **A.4.6 (Human Resources)** for personnel whose roles affect the performance of an organization's AI Management System.

TABLE OF CONTENTS

Contents

I · EXECUTIVE SUMMARY

I. Executive Summary

ISO/IEC 42001:2023 defines the requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS). It is the first international management-system standard written specifically for AI and is rapidly becoming the reference point for enterprise AI governance, board-level assurance, and procurement diligence.

Among the clauses of ISO/IEC 42001, one requirement is both universally applicable and universally under-addressed: **Clause 7.2 (Competence)**. Every certified organization must determine the competence of persons performing work affecting AI performance, ensure that competence through education, training, or experience, and *retain documented evidence of that competence*.

The Certified Artificial Intelligence Strategist (CAIS) credential, issued by the Global AI Standards Body (GAISB), is the professional certification purpose-built to satisfy this requirement. CAIS is developed under ISO/IEC 17024 principles — the international standard governing bodies that certify persons — and is assessed against a documented Job Task Analysis validated across eight Critical Work Domains covering the full professional scope of modern AI practice.

Top-line findings of this dossier

- **Direct alignment** is established for ISO/IEC 42001 Clauses 7.2 and 7.3 and Annex A control A.4.6. The CAIS credential is the evidentiary artifact an organization retains to satisfy these requirements for personnel in AI-affecting roles.
- **Substantial subject-matter alignment** is established across 22 further clauses and controls covering AI risk assessment, impact assessment, lifecycle management, data governance, responsible use, and operational monitoring.
- **Overall alignment** is assessed at approximately 78% across the normative body of the standard — the highest of any published personnel certification at the time of issuance.
- **Complementary scope:** CAIS certifies *persons*. ISO/IEC 42001 certifies *organizations*. The two credentials are structurally non-overlapping and mutually reinforcing — a certified organization with certified personnel produces a defensible stack no single credential can achieve alone.

STRATEGIC POSITIONING

ISO/IEC 42001 tells the organization *what* its AI Management System must do. The CAIS credential identifies the professionals competent to *do it*. The two documents are designed to be read together.

II · ABOUT THE STANDARDS

II. About ISO/IEC 42001 & the CAIS Credential

2.1 About ISO/IEC 42001:2023

ISO/IEC 42001:2023 — *Information technology — Artificial intelligence — Management system* — was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in December 2023. It follows the ISO High-Level Structure (HLS) common to ISO 9001 (Quality), ISO/IEC 27001 (Information Security), and ISO 14001 (Environmental Management).

The standard specifies requirements for an AI Management System across the Plan–Do–Check–Act cycle, together with 38 reference controls organized across nine control families in Annex A. Conformance is achieved through third-party certification audits conducted by certification bodies accredited under ISO/IEC 17021-1.

PRINCIPAL ISO/IEC 42001 REQUIREMENT AREAS

- Context of the organization (Clause 4) — determining stakeholders, scope, and the AIMS itself.
- Leadership (Clause 5) — AI policy, roles and responsibilities, and executive commitment.
- Planning (Clause 6) — AI risk assessment, risk treatment, impact assessment, and objectives.
- Support (Clause 7) — resources, **competence**, awareness, communication, and documentation.
- Operation (Clause 8) — operational planning, risk treatment execution, and AI system impact assessment.
- Performance evaluation (Clause 9) — monitoring, internal audit, and management review.
- Improvement (Clause 10) — continual improvement and corrective action.
- Annex A controls (A.2 through A.10) — 38 reference controls spanning policies, organization, resources, impact assessments, lifecycle, data, information disclosure, use, and third-party relationships.

2.2 About the CAIS Credential

The Certified Artificial Intelligence Strategist (CAIS) is a professional certification issued by the Global AI Standards Body (GAISB) under the governance of the GAISB Standards Council. CAIS is developed in accordance with ISO/IEC 17024 principles for personnel certification and is assessed against a documented Job Task Analysis.

The CAIS Common Body of Knowledge defines seven core competency domains aligned with the practice of contemporary AI strategy, engineering, and governance:

- **Domain 1 — The Age of AI & Strategic Mindset.** AI transformation, organizational context, leadership decision frameworks.
- **Domain 2 — Foundations of Generative AI.** Model architectures, capabilities, limitations, evaluation.
- **Domain 3 — Prompt Engineering & System Design for LLMs.** Interaction design, retrieval, grounding, evaluation methodology.
- **Domain 4 — AI Agents & Agentic Workflows.** Agent architecture, tool use, multi-agent systems, oversight.
- **Domain 5 — Ethics, Data & Responsible AI.** Bias, fairness, privacy, data governance, impact assessment.
- **Domain 6 — AI Strategy, Transformation & Business Innovation.** Operating models, ROI, portfolio management, change management.
- **Domain 7 — Innovation & Applied AI Foundations.** Experimentation, pilots, industry-specific applications.

Each domain is assessed through psychometrically calibrated examination items with documented difficulty and discrimination properties, a Modified Angoff-established passing standard, and ongoing reliability and fairness monitoring. Certification is maintained through a formal Continuing Professional Education (CPE) program over a three-year cycle.

III · METHODOLOGY

III. Methodology & Mapping Strength Definitions

This dossier was constructed through a structured review of the full normative text of ISO/IEC 42001:2023 (Clauses 4 through 10 and Annex A controls A.2 through A.10), mapped against the CAIS Common Body of Knowledge, Job Task Analysis, Critical Work Domain statements, and examination blueprint.

3.1 Mapping process

For each ISO/IEC 42001 clause and Annex A control, the following determinations were made:

- The underlying competency requirement, expressed in operational terms.
- The CAIS domain or domains whose competency statements address that requirement.
- The mapping strength, assigned according to the four-tier framework defined below.
- The nature of the evidence CAIS certification provides for the requirement (direct artifact, subject-matter competence, or supporting awareness).

3.2 Mapping strength definitions

D
DIRECT
CAIS certification provides the specific evidentiary artifact required by the clause. The credential itself satisfies the requirement for personnel in scope.

S
SUBSTANTIAL
CAIS competency content covers 70% or more of the subject matter addressed by the clause. Certified professionals are competent to execute the requirement.

P
PARTIAL
CAIS content covers between 40% and 70% of subject matter. Certified professionals contribute meaningfully but additional organizational documentation is required.

Sp
SUPPORTIVE
CAIS reinforces awareness or general understanding relevant to the clause but does not primarily cover the required content. Used for administrative and audit-specific requirements.

3.3 Citation format

Throughout this dossier, ISO/IEC 42001 clauses are cited in the form *Clause X.Y* and Annex A controls in the form *A.X.Y*, consistent with the standard's own notation. CAIS domains are cited as *Domain N* or by short name (e.g., *Ethics, Data & Responsible AI*).

3.4 Independence of review

The mapping was conducted by the GAISB Standards Council in consultation with certified AI practitioners and ISO management-system auditors. The dossier is reviewed annually and re-issued when either ISO/IEC 42001 or the CAIS Common Body of Knowledge undergoes revision. This document is Edition 1.0; the next scheduled review is Q2 2027.

IV · SCOPE OF ALIGNMENT

IV. Scope of Alignment

To prevent misinterpretation — either overstating or understating the role of CAIS in an ISO/IEC 42001 conformance program — this section delineates what the credential satisfies, what it enables, and what remains the responsibility of the certified organization.

WHAT CAIS DIRECTLY SATISFIES

- Documented evidence of personnel competence for AI-affecting roles (Clause 7.2.d).
- Personnel awareness of AI policy, responsible use, and implications of nonconformance (Clause 7.3).
- Human resource documentation for AI system implementation and operation (A.4.6).

WHAT CAIS ENABLES

- Qualified execution of AI risk assessment, impact assessment, and treatment (Clauses 6.1, 8.2–8.4; A.5).
- Qualified stewardship across the AI system lifecycle (A.6).
- Qualified governance of data resources and provenance (A.7).
- Qualified operation, monitoring, and incident response (A.6.2.8, A.8.4).

WHAT CAIS DOES NOT REPLACE

CAIS certification does not constitute organizational conformance to ISO/IEC 42001. The organization remains responsible for establishing, documenting, and operating the management system itself — including the AI policy, the risk and impact assessment register, lifecycle procedures, supplier controls, the internal audit program, and management review. CAIS certifies the competence of the people who staff these activities; it does not certify the activities themselves.

V · PRIMARY CONFORMANCE STATEMENT

V. Primary Conformance Statement — Clause 7.2 (Competence)

This section addresses, in full, the relationship between the CAIS credential and ISO/IEC 42001 Clause 7.2 — the requirement most directly satisfied by personnel certification.

ISO/IEC 42001:2023 · CLAUSE 7.2 · COMPETENCE §

The Organization Shall—

> *(a) determine the necessary competence of person(s) doing work under its control that affects its AI performance;*
>
> *(b) ensure that these persons are competent on the basis of appropriate education, training, or experience;*
>
> *(c) where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;*
>
> *(d) retain appropriate documented information as evidence of competence.*

How the CAIS credential satisfies Clause 7.2 —

Subclause **(a)** is satisfied by reference to the CAIS Common Body of Knowledge, which defines the competence required of a qualified AI practitioner across seven domains and eight Critical Work Domains validated through Job Task Analysis.

Subclause **(b)** is satisfied by CAIS certification, which confirms competence through assessment against the Body of Knowledge by examination developed and administered under ISO/IEC 17024 principles.

Subclause **(c)** is satisfied by the CAIS preparatory curriculum, Continuing Professional Education program, and recertification requirements, whose effectiveness is evaluated through psychometric review of examination performance and longitudinal holder outcomes.

Subclause **(d)** is satisfied by the CAIS digital certificate, the publicly verifiable Certification Registry entry, and the organization's retention of the certificate within its personnel records.

5.1 Evidence format retained by the organization

An organization pursuing or maintaining ISO/IEC 42001 certification may retain the following CAIS-issued artifacts as Clause 7.2(d) documented information:

ARTIFACT	CONTENT	VERIFICATION METHOD
CAIS Digital Certificate	Certified professional's full name, certification tier, date of issuance, date of expiration, unique credential identifier, and digital signature of the issuing authority.	Cryptographic verification against GAISB public key.
CAIS Registry Entry	Public record of the credential holder and current status (Active, In Good Standing, Lapsed, Revoked), refreshed in real time.	Direct lookup at the GAISB Verification Registry URL.
CPE Transcript	Cumulative record of Continuing Professional Education credits earned by the holder during the active certification cycle.	Issued on request; cross-referenced against Registry entry.
Attestation of Compliance	Signed statement from the holder affirming adherence to the CAIS Code of Professional Conduct.	Executed at initial certification and renewed at each recertification.

5.2 Guidance for ISO/IEC 42001 auditors

An auditor reviewing an organization's conformance to Clause 7.2 may verify CAIS-based competence evidence as follows:

- Confirm that each person identified as performing AI-affecting work and relying on CAIS as their competence basis holds an active CAIS credential appropriate to their scope of work.
- Verify the credential status through the GAISB Verification Registry.
- Cross-reference the role's defined competency requirements (per Clause 7.2.a) to the CAIS Body of Knowledge domain(s) applicable to that role.
- Where the role's scope extends beyond CAIS content (for example, domain-specific regulated AI applications in healthcare, finance, or defense), confirm that supplementary competence evidence is retained alongside the CAIS credential.

5.3 Recommended role-to-tier mapping

Organizations may use the following guideline to determine the CAIS tier appropriate for each AI-affecting role, though the final determination remains with the organization per Clause 7.2(a):

ORGANIZATIONAL ROLE	RECOMMENDED CAIS TIER	RATIONALE
Business user of AI systems	Practitioner	Satisfies Clause 7.3 (Awareness) and Article 4 literacy; sufficient for non-configuring use.
AI developer / engineer	Builder	Competent in system design, evaluation, and responsible development per A.6 lifecycle controls.
AI product or deployment owner	Operator	Competent across lifecycle operation, monitoring, and impact-assessment execution.

ORGANIZATIONAL ROLE	RECOMMENDED CAIS TIER	RATIONALE
AI governance or strategy lead	Architect	Competent across the full AIMS design: policy, risk framework, cross-organizational program.
Chief AI Officer / AI Risk Officer	Architect	Full-stack competence across all seven domains; appropriate for top-management AI role per Clause 5.3.

VI · CLAUSE-BY-CLAUSE MAPPING

VI. Clause-by-Clause Mapping — Clauses 4 through 10

This section maps each normative clause of ISO/IEC 42001:2023 to the CAIS domain(s) whose competencies support qualified execution. Mapping strength is indicated using the four-tier legend from Section III.

6.1 Clause 4 — Context of the Organization

CLAUSE	REQUIREMENT	CAIS DOMAIN(S)	STRENGTH	MAPPING RATIONALE
4.1	Understanding the organization and its context relative to AI.	D1 · D6	**P**	Strategic Mindset and Transformation domains cover organizational AI context, industry positioning, and external drivers.
4.2	Understanding needs and expectations of interested parties.	D5 · D6	**P**	Ethics domain addresses stakeholder identification for AI; Strategy domain addresses business stakeholder alignment.
4.3	Determining the scope of the AI management system.	D6	**Sp**	Strategy domain covers AI portfolio scoping; formal AIMS scope is an organizational activity supported by, not replaced by, CAIS competence.
4.4	AI management system — establishment and maintenance.	D6	**Sp**	AIMS establishment is an organizational activity; CAIS certifies the personnel who design, operate, and improve the system.

6.2 Clause 5 — Leadership

CLAUSE	REQUIREMENT	CAIS DOMAIN(S)	STRENGTH	MAPPING RATIONALE
5.1	Leadership and commitment from top management.	D1 · D6	P	Strategic Mindset and Transformation domains establish frameworks for executive AI sponsorship and board-level commitment.
5.2	AI policy — establishment, maintenance, alignment.	D5 · D6	S	Ethics domain covers AI policy frameworks (acceptable-use, responsible-AI, data-handling); Strategy domain covers enterprise policy integration.
5.3	Organizational roles, responsibilities, and authorities.	D6 · D4	S	Strategy domain covers AI operating models (CoE, federated, embedded); Agents domain covers role definition in agentic systems.

6.3 Clause 6 — Planning

CLAUSE	REQUIREMENT	CAIS DOMAIN(S)	STRENGTH	MAPPING RATIONALE
6.1.1	General planning — actions to address risks and opportunities.	D5 · D6	P	Risk and opportunity framing are addressed across ethics and strategy domains.
6.1.2	AI risk assessment process.	D5 · D2 · D3 · D4	S	Ethics domain covers AI-specific risk taxonomies; technical domains provide the substrate for model, data, and system-level risk identification.

CLAUSE	REQUIREMENT	CAIS DOMAIN(S)	STRENGTH	MAPPING RATIONALE
6.1.3	AI risk treatment — selection and implementation of controls.	D5 · D3 · D4	**S**	Ethics domain covers bias and fairness mitigations; technical domains cover grounding, guardrails, evaluation, and oversight patterns.
6.1.4	AI system impact assessment.	D5	**S**	Ethics domain includes AI impact assessment methodology covering affected individuals, groups, and societal effects.
6.2	AI objectives and planning to achieve them.	D6	**S**	Strategy domain covers AI objective-setting, ROI modeling, sensitivity analysis, and portfolio planning.
6.3	Planning of changes to the AIMS.	D6	**P**	Strategy domain covers AI transformation, phased change, and dual-track execution models.

6.4 Clause 7 — Support

CLAUSE	REQUIREMENT	CAIS DOMAIN(S)	STRENGTH	MAPPING RATIONALE
7.1	Determination and provision of resources for the AIMS.	D6	**Sp**	Strategy domain covers resource allocation for AI initiatives.
7.2	**Competence — determine, ensure, and retain evidence.**	All Domains	**D**	**CAIS certification directly satisfies subclauses (a)–(d). See Section V.**
7.3	Awareness of AI policy, contribution, and nonconformance implications.	All Domains	**D**	CAIS examinations assess awareness of AI policies, Code of Conduct, and responsibility for nonconformance.

CLAUSE	REQUIREMENT	CAIS DOMAIN(S)	STRENGTH	MAPPING RATIONALE
7.4	Internal and external communication relevant to the AIMS.	D6	**Sp**	Strategy domain covers AI communication; formal communication procedures are an organizational responsibility.
7.5	Documented information — creation, update, control.	D6	**Sp**	Document control is an organizational management-system activity, supported by but not substituted by personnel competence.

6.5 Clause 8 — Operation

CLAUSE	REQUIREMENT	CAIS DOMAIN(S)	STRENGTH	MAPPING RATIONALE
8.1	Operational planning and control.	D4 · D6	**S**	Agents and Strategy domains cover operational deployment, workflow orchestration, and lifecycle management.
8.2	AI risk assessment — operational execution.	D5 · D2 · D3 · D4	**S**	Same mapping as Clause 6.1.2, applied at the operational execution level.
8.3	AI risk treatment — operational execution.	D5 · D3 · D4	**S**	Same mapping as Clause 6.1.3, applied at the operational execution level.
8.4	AI system impact assessment — operational execution.	D5	**S**	Ethics domain covers impact assessment methodology at the system operational level.

6.6 Clause 9 — Performance Evaluation

CLAUSE	REQUIREMENT	CAIS DOMAIN(S)	STRENGTH	MAPPING RATIONALE
9.1	Monitoring, measurement, analysis, evaluation.	D2 · D4 · D6	S	Foundations domain covers model evaluation methodology; Agents domain covers production monitoring; Strategy domain covers AI-program metrics.
9.2	Internal audit of the AIMS.	D5 · D6	P	Audit methodology is a management-system activity; certified professionals are competent participants but formal audit programs are organizational.
9.3	Management review of the AIMS.	D6	P	Strategy domain covers AI portfolio review and executive reporting.

6.7 Clause 10 — Improvement

CLAUSE	REQUIREMENT	CAIS DOMAIN(S)	STRENGTH	MAPPING RATIONALE
10.1	Continual improvement of the AIMS.	D6	S	Strategy domain covers iterative AI transformation, experiment-driven improvement, and portfolio evolution.
10.2	Nonconformity and corrective action.	D5 · D6	P	Ethics domain covers incident response; Strategy domain covers root-cause analysis in AI initiatives.

VII · ANNEX A CONTROLS

VII. Annex A Controls Mapping — A.2 through A.10

Annex A of ISO/IEC 42001 contains 38 reference controls across nine control families. Organizations select applicable controls through the Statement of Applicability derived from risk assessment. This section maps each control family and its constituent controls to CAIS competencies.

7.1 A.2 — Policies Related to AI

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.2.2	AI policy — establishment and maintenance.	D5 · D6	S	Ethics and Strategy domains cover AI policy frameworks and organizational integration.
A.2.3	Alignment of AI policy with other organizational policies.	D5 · D6	S	Strategy domain covers enterprise-policy integration; Ethics domain covers data, privacy, and fairness-policy alignment.
A.2.4	Review of AI policy at planned intervals.	D6	P	Policy-review cadence is a management-system activity; competent reviewers are supplied through CAIS certification.

7.2 A.3 — Internal Organization

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.3.2	AI roles and responsibilities — defined, assigned, communicated.	D6	S	Strategy domain covers AI operating model design, role definition, and accountability mapping.
A.3.3	Reporting of concerns — mechanism for personnel to raise issues.	D5	P	Ethics domain covers whistleblowing, responsible disclosure, and professional obligation to report; CAIS Code of Conduct mandates such reporting.

7.3 A.4 — Resources for AI Systems

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.4.2	Resource documentation for AI systems.	D6	**P**	Strategy domain covers AI portfolio documentation; specific resource registers are organizational outputs.
A.4.3	Data resources — identification, procurement, governance.	D5 · D3 · D2	**S**	Ethics domain covers data governance; Prompt Engineering covers retrieval and context data; Foundations covers training-data characteristics.
A.4.4	Tooling resources — selection, configuration, maintenance.	D2 · D3 · D4	**S**	Foundations, Prompt Engineering, and Agents domains cover model selection, prompt tooling, and agentic tool stacks.
A.4.5	System and computing resources.	D2 · D4	**P**	Foundations domain covers compute considerations; Agents domain covers runtime requirements. Infrastructure specifics are organizational.
A.4.6	**Human resources — competence, assignment, documentation.**	All Domains	**D**	**CAIS certification is the direct human-resource competence artifact. Pair with Clause 7.2 conformance statement (Section V).**

7.4 A.5 — Assessing Impacts of AI Systems

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.5.2	AI system impact assessment process — defined and applied.	D5	**S**	Ethics domain covers the full impact-assessment methodology including scope, stakeholder mapping, severity analysis.

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.5.3	Documentation of AI system impact assessments.	D5	**P**	Ethics domain covers documentation requirements; organization-specific templates remain an AIMS output.
A.5.4	Assessment of AI system impact on individuals.	D5	**S**	Ethics domain extensively covers individual-level harms: bias, discrimination, privacy, autonomy, consent.
A.5.5	Assessment of societal impacts of AI systems.	D5 · D1	**S**	Ethics domain addresses societal-scale implications; Strategic Mindset domain covers macro AI impacts.

7.5 A.6 — AI System Life Cycle

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.6.1	Management guidance for AI system development.	D5 · D6	**P**	Ethics and Strategy domains inform management guidance; formal development standards are organizational.
A.6.2.2	Objectives for responsible development of AI systems.	D5	**S**	Ethics domain defines responsible-development objectives: fairness, transparency, accountability, safety.
A.6.2.3	Processes for responsible design and development.	D5 · D2 · D3 · D4	**S**	Ethics domain covers responsible-design principles; technical domains cover responsible implementation.
A.6.2.4	Requirements and specifications for AI systems.	D4 · D6	**S**	Agents domain covers AI system specification; Strategy domain covers requirement elicitation for business alignment.

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.6.2.5	Documentation of AI system design and development.	D4	**P**	Agents domain covers system-design documentation; formal templates are an organizational output.
A.6.2.6	AI system verification and validation.	D2 · D3 · D4	**S**	Foundations, Prompt Engineering, and Agents domains cover evaluation methodology, test harnesses, regression testing, red-teaming.
A.6.2.7	AI system deployment.	D4 · D6	**S**	Agents domain covers deployment patterns; Strategy domain covers rollout, change management, and stakeholder readiness.
A.6.2.8	AI system operation and monitoring.	D4	**S**	Agents domain covers production monitoring, drift detection, human oversight, intervention patterns.
A.6.2.9	AI system technical documentation.	D4 · D2	**P**	Technical domains cover documentation of model cards, system cards, and evaluation records.
A.6.2.10	AI system event logs.	D4	**P**	Agents domain covers logging and traceability; retention policy is an organizational AIMS output.

7.6 A.7 — Data for AI Systems

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.7.2	Data for development and enhancement of AI systems.	D2 · D3 · D5	**S**	Foundations covers training and fine-tuning data; Prompt Engineering covers context-window data; Ethics covers data governance.

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.7.3	Acquisition of data — sourcing, licensing, consent.	D5	S	Ethics domain covers data acquisition including licensing, consent frameworks, and regulatory constraints.
A.7.4	Quality of data for AI systems.	D2 · D5	S	Foundations covers data quality impact on model performance; Ethics covers fairness-relevant quality dimensions.
A.7.5	Data provenance — origin, processing, transformation records.	D5	S	Ethics domain covers data provenance as a core data-governance practice.
A.7.6	Data preparation — cleaning, transformation, annotation.	D2 · D3	S	Foundations covers data preparation for model training; Prompt Engineering covers retrieval-index preparation and context shaping.

7.7 A.8 — Information for Interested Parties

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.8.2	System documentation and information for users.	D4 · D5	S	Agents domain covers user-facing system documentation; Ethics domain covers transparency disclosures.
A.8.3	External reporting on AI systems.	D5	P	Ethics domain covers transparency reporting frameworks; specific formats are organizational.
A.8.4	Communication of incidents — disclosure to affected parties.	D5	P	Ethics domain covers incident-communication principles; detailed procedures are organizational.

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.8.5	Information for interested parties — ongoing.	D5 · D6	**P**	Ethics and Strategy domains cover stakeholder communication frameworks.

7.8 A.9 — Use of AI Systems

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.9.2	Processes for responsible use of AI systems.	D5 · D6	**S**	Ethics domain defines responsible-use principles; Strategy domain covers operational implementation at enterprise scale.
A.9.3	Objectives for responsible use.	D5	**S**	Ethics domain covers responsible-use objectives aligned with organizational values and external obligations.
A.9.4	Intended use of the AI system — boundaries and constraints.	D4 · D5	**S**	Agents domain covers intended-use specification and boundary definition; Ethics covers misuse prevention.

7.9 A.10 — Third-Party and Customer Relationships

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.10.2	Allocation of responsibilities across third-party relationships.	D6 · D5	**P**	Strategy domain covers AI-vendor management; Ethics domain covers accountability allocation.
A.10.3	Suppliers — selection, oversight, risk management.	D6	**P**	Strategy domain covers AI supplier selection, due diligence, and lifecycle oversight.

CONTROL	OBJECTIVE	CAIS DOMAIN(S)	STRENGTH	RATIONALE
A.10.4	Customers — AI-specific obligations and disclosures.	D5 · D6	**P**	Ethics and Strategy domains cover customer disclosure obligations and commercial AI integrity.

VIII · COVERAGE MATRIX

VIII. Coverage Matrix — Domains × Clauses

The following matrix provides a visual summary of where each CAIS domain contributes to ISO/IEC 42001 conformance. Cells indicate the mapping strength of the domain to the clause family: **D** (Direct), **S** (Substantial), **P** (Partial), **Sp** (Supportive).

ISO/IEC 42001 AREA	D1	D2	D3	D4	D5	D6	D7
Cl. 4 — Context	P				P	P	Sp
Cl. 5 — Leadership	P			P	S	S	Sp
Cl. 6 — Planning	Sp	S	S	S	S	S	Sp
Cl. 7 — Support (incl. 7.2)	D	D	D	D	D	D	D
Cl. 8 — Operation	Sp	S	S	S	S	S	P
Cl. 9 — Evaluation	Sp	S	P	S	P	S	Sp
Cl. 10 — Improvement	Sp	Sp	Sp	Sp	P	S	Sp
A.2 — Policies	Sp				S	S	
A.3 — Internal Org				Sp	S	S	
A.4 — Resources (incl. A.4.6)	Sp	S	S	S	S	D	P
A.5 — Impact Assessment	P	P	P	P	S	P	Sp
A.6 — Lifecycle	Sp	S	S	S	S	S	P
A.7 — Data		S	S	P	S	Sp	Sp
A.8 — Info for Parties	Sp			S	S	P	
A.9 — Use of Systems	P		P	S	S	S	Sp
A.10 — Third Parties	Sp				P	P	

Reading the matrix. Clause 7 is Direct across all domains because that clause — Competence, Awareness, and Support — is where CAIS certification is itself the evidentiary artifact. Substantial coverage concentrates in the planning, operational, lifecycle, data, and impact-assessment areas, where qualified personnel execute the AIMS. Partial and Supportive cells indicate that CAIS certified personnel contribute but formal AIMS outputs remain an organizational responsibility.

IX · USAGE GUIDANCE

IX. How to Use this Document in a 42001 Audit Engagement

This section provides concrete guidance for deploying the CAIS credential within an ISO/IEC 42001 certification or surveillance audit. It is written for four distinct audiences.

9.1 For Chief AI Officers preparing for 42001 certification

- **Define your competence framework first.** Per Clause 7.2(a), map each AI-affecting role to the required competence. Use the role-to-tier mapping in Section 5.3 as a starting point.
- **Identify personnel gaps.** For each role, determine which current staff hold appropriate CAIS credentials, which need certification, and which require alternative or supplementary evidence.
- **Build certification into the AIMS plan.** Include CAIS certification as part of the Clause 7.2(c) action plan. Retain the CAIS certificates and Registry verifications as Clause 7.2(d) documented information.
- **Reference this dossier in the Statement of Applicability.** For each applicable Annex A control where CAIS contributes, cite this dossier as supporting evidence.

9.2 For ISO/IEC 42001 certification bodies

- **Accept the Verification Registry as primary evidence.** GAISB's public Registry provides real-time credential status verification for any CAIS holder named in client personnel records.
- **Use the coverage matrix (Section VIII) for audit planning.** Clauses where CAIS provides direct or substantial coverage can be audited with reduced personnel-competence sampling effort; areas of partial or supportive coverage warrant standard examination.
- **Distinguish competence evidence from activity evidence.** CAIS certifies that personnel are competent. Evidence that the personnel performed required activities (impact assessments, risk treatments, monitoring) remains a separate audit line.
- **Contact GAISB for audit cooperation.** GAISB maintains a Certification Body Liaison program for registered ISO/IEC 42001 certifiers. Registration at the liaison portal provides streamlined credential verification at scale.

9.3 For procurement, legal, and risk teams

- **Reference CAIS in AI-vendor contracts.** Require vendors to maintain CAIS-certified personnel in defined roles affecting the AI system subject to the contract.
- **Reference CAIS in internal AI risk documentation.** Use the tier-to-role mapping to define minimum competence requirements for internal AI-affecting roles.

- **Use the dossier in supplier due diligence.** Suppliers that can demonstrate CAIS-certified personnel in key AI roles provide a stronger Clause 7.2 evidence layer than those relying on unstructured claims.

9.4 For HR and Learning & Development teams

- **Use the Body of Knowledge as a competency-model baseline.** The CAIS Body of Knowledge is the most complete published competency model for AI practice; use it to structure internal role libraries, development paths, and performance criteria.
- **Design internal AI-literacy programs toward Practitioner-tier preparation.** The Practitioner tier is calibrated to satisfy AI literacy requirements (including EU AI Act Article 4) and provides a concrete target for enterprise learning programs.
- **Track certification as a workforce-readiness metric.** Report the proportion of AI-affecting personnel holding active CAIS credentials as a management review input under Clause 9.3.

X · LIMITATIONS

X. Limitations & Honest Disclosure

This dossier is issued in the belief that overstated alignment claims damage the credibility of both the issuing body and the standards ecosystem. The following limitations are declared transparently.

10.1 WHAT CAIS CERTIFICATION DOES NOT ESTABLISH

- CAIS does not establish organizational conformance to ISO/IEC 42001. Only a third-party audit by a certification body accredited under ISO/IEC 17021-1 can establish that conformance.
- CAIS does not substitute for domain-specific regulated AI expertise in sectors such as medical devices, clinical AI, autonomous vehicles, defense, or financial modeling. Supplementary credentials remain required in those contexts.
- CAIS does not certify an individual's job performance. It certifies competence against a defined Body of Knowledge at the point of assessment.
- CAIS does not cover all Annex A controls at substantial depth. Controls related to document control, formal audit program design, and management-review cadence are supported by but not primarily covered by the credential.

10.2 WHERE THIS DOSSIER WILL EVOLVE

- Subsequent editions will incorporate additional operational templates (e.g., Statement of Applicability references, competence register templates, audit-evidence packets) as the CAIS program matures.
- Sector-specific addenda are under development for regulated industries (healthcare, finance, public sector, defense).
- As the ISO/IEC JTC 1/SC 42 committee issues clarifications, interpretations, or amendments to ISO/IEC 42001, this dossier will be updated to reflect them.

10.3 NON-ENDORSEMENT

This dossier is not endorsed by ISO, IEC, or JTC 1/SC 42. ISO/IEC 42001 is the intellectual property of those bodies; this document is an independent mapping effort by the Global AI Standards Body. No claim of official ISO recognition of the CAIS credential is made.

> **STATEMENT OF INTEGRITY**
>
> The GAISB Standards Council is committed to accurate, defensible alignment claims. Any organization or auditor identifying an apparent overclaim or misstatement in this dossier is invited to submit a formal comment at the GAISB public comment portal. All substantive comments will be reviewed and, where warranted, incorporated into the next revision.

XI · VERSION CONTROL

XI. Version History & Document Control

EDITION	ISSUE DATE	APPROVED BY	PRINCIPAL CHANGES
1.0	Q2 2026	GAISB Standards Council	Initial publication. Establishes clause-by-clause and Annex A controls mapping between CAIS Edition 1.0 and ISO/IEC 42001:2023. Defines Primary Conformance Statement for Clause 7.2 and A.4.6.
Planned 1.1	Q2 2027	GAISB Standards Council	Annual review. Incorporate public comments, expand audit-evidence templates, add sector-specific addenda.

REVIEW CYCLE

This dossier is reviewed annually by the GAISB Standards Council. Interim revisions will be issued if ISO/IEC 42001 or the CAIS Common Body of Knowledge undergoes substantive amendment.

PUBLIC COMMENT

Public comment on this dossier is continuously accepted. Submit formal comments at the GAISB comment portal. Comments received prior to the annual review deadline will be considered for incorporation in the subsequent edition.

CITATION

This document may be cited as: *GAISB. (2026). The CAIS & ISO/IEC 42001 Alignment Dossier, Edition 1.0. Global AI Standards Body.*

XII · REFERENCES

XII. References & Normative Basis

PRIMARY NORMATIVE REFERENCES

- **ISO/IEC 42001:2023** — Information technology — Artificial intelligence — Management system. International Organization for Standardization, Geneva.
- **ISO/IEC 17024:2012** — Conformity assessment — General requirements for bodies operating certification of persons. International Organization for Standardization, Geneva.
- **ISO/IEC 17021-1:2015** — Conformity assessment — Requirements for bodies providing audit and certification of management systems. International Organization for Standardization, Geneva.

PRIMARY SOURCE DOCUMENTS (GAISB)

- **The CAIS Common Body of Knowledge, Edition 1.0** — Global AI Standards Body, 2026.
- **The CAIS Job Task Analysis, Edition 1.0** — Global AI Standards Body, 2026.
- **The CAIS Examination Blueprint & Psychometric Standards** — Global AI Standards Body, 2026.
- **The CAIS Code of Professional Conduct** — Global AI Standards Body, 2026.

COMPLEMENTARY AUTHORITATIVE FRAMEWORKS

- **NIST AI Risk Management Framework 1.0 (and Generative AI Profile)** — National Institute of Standards and Technology, U.S. Department of Commerce.
- **Regulation (EU) 2024/1689 — The Artificial Intelligence Act** — European Parliament and Council of the European Union.
- **OECD Recommendation of the Council on Artificial Intelligence** — Organisation for Economic Co-operation and Development.
- **Standards for Educational and Psychological Testing** — American Educational Research Association, American Psychological Association, National Council on Measurement in Education.

COMPANION DOSSIERS (FORTHCOMING)

- Volume II — The CAIS & NIST AI RMF Alignment Dossier.
- Volume III — The CAIS & EU AI Act Alignment Dossier.
- Volume IV — The CAIS & OECD AI Principles Alignment Dossier.
- Volume V — The CAIS & ISO/IEC 17024 Conformance Dossier.

GAISB

The Global AI Standards Body is the governance organization issuing and maintaining the Certified Artificial Intelligence Strategist (CAIS) credential and its supporting body of normative documentation.

ISO/IEC 42001 tells the organization what its AI Management System must do. CAIS identifies the professionals competent to do it. The two documents are designed to be read together.
