GAISB

GLOBAL AI STANDARDS BODY
THE ALIGNMENT DOSSIER SERIES · VOLUME I

EDITION 1.0.1 / 2026
EFFECTIVE Q2 2026
REVIEW CYCLE: ANNUAL
ISO-DSR-2026-01

PERSONNEL-COMPETENCE ALIGNMENT

The GAISB & *ISO/IEC 42001* Alignment Dossier

How the GAISB credentials (GAISB AI Essentials, GAISB AI Practitioner, GAISB AI Team Architect) map to the international AI Management System standard, clause by clause, control by control.

COMPANION DOCUMENT TO
The GAISB Common Body of Knowledge, Edition 1.0.1

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 sets out the alignment between the GAISB professional credentials and ISO/IEC 42001:2023, the international standard for Artificial Intelligence Management Systems (AIMS).

WHAT THIS DOCUMENT IS

A clause-by-clause and control-by-control mapping that shows where GAISB-certified professionals provide competence evidence useful to organizations implementing and maintaining an AI Management System in conformance with ISO/IEC 42001, and where they do not.

WHAT THIS DOCUMENT IS NOT

This is not an ISO/IEC 42001 certification, and it is not endorsed by ISO, IEC, or JTC 1/SC 42. Organizational conformance to ISO/IEC 42001 is established only through a third-party audit conducted by an accredited certification body. This dossier is an internal GAISB assessment of the personnel-competence 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 support 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**
>
> A GAISB credential is documented evidence of assessed competence that an organization may retain under ISO/IEC 42001:2023 Clause 7.2(d) (Competence) and cite under Annex A control A.4.6 (Human Resources) for personnel whose roles affect the performance of its AI Management System. The determination of which competences each role requires (Clause 7.2(a)) remains the organization's.

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 becoming a 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 frequently under-evidenced: Clause 7.2 (Competence). Every certified organization must determine the competence of persons performing work affecting AI performance, ensure competence through education, training, or experience, and retain documented evidence of that competence.

The GAISB credentials, issued by the Global AI Standards Body (GAISB™), are professional certifications designed to serve as that documented evidence. GAISB operates under ISO/IEC 17024 principles for bodies certifying persons and assesses candidates against a Common Body of Knowledge derived from a documented Job Task Analysis across seven competency domains.

TOP-LINE FINDINGS OF THIS DOSSIER

- **Direct alignment** is established for ISO/IEC 42001 Clause 7.2 (Competence) and Annex A control A.4.6 (Human Resources). A GAISB credential is an evidentiary artifact an organization may retain for these requirements for personnel in AI-affecting roles.
- **Substantial subject-matter alignment** is assessed across 35 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 77%** of the normative body of the standard under the weighting set out in Section III (§3.5), with a defensible range of roughly 70% to 77% under alternative weightings. This is an internal GAISB assessment of personnel-competence coverage, not an ISO measurement.
- **Complementary scope.** GAISB certifies persons. ISO/IEC 42001 certifies organizations. The two are structurally non-overlapping and mutually reinforcing: a certified organization with certified personnel produces a more complete evidence stack than either achieves alone.

> **STRATEGIC POSITIONING**
>
> ISO/IEC 42001 tells the organization what its AI Management System must do. A GAISB credential evidences that a named professional has been assessed as competent to do it. The two documents are designed to be read together.

II · ABOUT THE STANDARDS

II. About ISO/IEC 42001 & the GAISB Credentials

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 Harmonized Structure 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 objectives in Annex A. Conformance is established through third-party certification audits conducted by certification bodies accredited under ISO/IEC 17021-1 and ISO/IEC 42006.

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 GAISB Credentials

The GAISB credentials are professional certifications issued by the Global AI Standards Body (GAISB™) under the governance of the GAISB Standards Council. GAISB operates in accordance with ISO/IEC 17024 principles for personnel certification and assesses candidates against a documented Job Task Analysis. GAISB is not, at this edition, accredited by any national or international accreditation body; its accreditation roadmap is published in the Common Body of Knowledge, Section XIX.

The GAISB Common Body of Knowledge defines seven competency domains:

- **Domain 1: AI Strategy & the Modern AI Economy.** The strategic, economic, and professional landscape of the AI era.
- **Domain 2: Foundations of Generative AI.** Technical and conceptual foundations of modern AI systems.
- **Domain 3: Prompt Engineering & LLM System Design.** The craft and engineering discipline of reliable LLM systems, built on the RTCF framework.
- **Domain 4: AI Agents & Agentic Workflows.** Design, deployment, and governance of autonomous AI systems.
- **Domain 5: Ethics, Data & Responsible AI.** Ethical, legal, regulatory, and operational responsibility.
- **Domain 6: AI Strategy, Transformation & Business Innovation.** Translating AI capability into enterprise-scale business outcomes.
- **Domain 7: Innovation & Applied AI Foundations.** Shipping real AI systems from prototype to production, including monitoring, incident handling, and iteration.

The GAISB pathway comprises three earned credentials (GAISB AI Essentials™, GAISB AI Practitioner™, and GAISB AI Team Architect™) plus two by-request specialty credentials, GAISB-Sec™ (Security) and GAISB-Gov™ (Governance). Examinations are developed under the psychometric standards set out in the Common Body of Knowledge (Section XII), including a Modified Angoff passing-standard method and published targets for item difficulty, discrimination, and reliability; psychometric results are

published per administration cycle in the GAISB Technical Report Series as they become available. Certification is maintained through a Continuing Professional Education (CPE) program on a two-year renewal cycle.

III · METHODOLOGY

III. Methodology, Mapping Strength & Alignment Derivation

This dossier was constructed through a structured review of the normative text of ISO/IEC 42001:2023 (Clauses 4 through 10 and Annex A controls A.2 through A.10), mapped against the GAISB Common Body of Knowledge, Job Task Analysis, 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 GAISB domain or domains whose learning outcomes address that requirement.
- The mapping strength, assigned according to the four-tier framework defined below.
- The nature of the evidence GAISB certification provides for the requirement (direct artifact, subject-matter competence, or supporting awareness).

3.2 Mapping strength definitions

D

DIRECT

GAISB certification provides a specific evidentiary artifact the clause calls for. The credential itself is retainable evidence for personnel in scope.

S

SUBSTANTIAL

GAISB competency content covers 70% or more of the subject matter addressed by the clause. Certified professionals are assessed as competent to execute the requirement.

P

PARTIAL

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

Sp

SUPPORTIVE

GAISB content covers less than 40% of the subject matter, reinforcing awareness relevant to the clause. 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. GAISB domains are cited as Domain N or D-N, or by short name (e.g., Ethics, Data & Responsible AI).

3.4 Basis of review

The mapping was conducted by the GAISB Standards Council, in consultation with GAISB-certified practitioners and management-system auditors. It is an internal assessment; no external body has reviewed or endorsed it. The dossier is reviewed annually and re-issued when either ISO/IEC 42001 or the GAISB Common Body of Knowledge undergoes revision. This document is Edition 1.0.1; the next scheduled review is Q2 2027.

3.5 Deriving the overall alignment figure

The headline alignment figure is a weighted coverage assessment across the 65 normative requirements mapped in Sections VI and VII (27 clauses and 38 Annex A controls). Each requirement is scored by its mapping strength using the coverage weights below, then averaged across all mapped requirements.

- **Coverage weights (primary):** Direct = 1.00 · Substantial = 0.90 · Partial = 0.65 · Supportive = 0.35. These sit at the upper part of each band's definition in §3.2.
- **Mapped requirements (Sections VI + VII):** 2 Direct · 35 Substantial · 23 Partial · 5 Supportive = 65 total.
- **Weighted score:** (2 × 1.00) + (35 × 0.90) + (23 × 0.65) + (5 × 0.35) = 50.20
- **Overall alignment:** 50.20 ÷ 65 = 0.772 ≈ **77%**
- **Sensitivity check (band midpoints):** Direct = 1.00 · Substantial = 0.85 · Partial = 0.55 · Supportive = 0.20 gives (2.00 + 29.75 + 12.65 + 1.00) ÷ 65 = 0.698 ≈ **70%**.

The figure is therefore reported as approximately 77%, with a defensible range of 70% to 77%, rounded to the nearest whole percent. It reflects the degree to which the GAISB competency framework covers the personnel-competence dimension of the standard. It is not a measure of organizational conformance, which is established only by accredited third-party audit (see Section X), and it is not an ISO measurement.

IV · SCOPE OF ALIGNMENT

IV. Scope of Alignment

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

WHAT A GAISB CREDENTIAL DIRECTLY EVIDENCES

- Documented evidence of assessed personnel competence for AI-affecting roles (Clause 7.2(b) and 7.2(d)).
- Human resource competence documentation for AI system implementation and operation (A.4.6).

WHAT A GAISB CREDENTIAL SUPPORTS

- The organization's determination of required competence for AI-affecting roles (Clause 7.2(a)), for which the Common Body of Knowledge may serve as a reference model.
- Personnel awareness of responsible AI practice and the implications of nonconformance (Clause 7.3), while awareness of the organization's own AI policy remains organization-specific.

WHAT A GAISB CREDENTIAL ENABLES

- Qualified execution of AI risk assessment, impact assessment, and treatment (Clauses 6.1, 8.2 to 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.6.2.6, A.8.4).

WHAT GAISB DOES NOT REPLACE

GAISB 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. GAISB certifies the assessed competence of the people who staff these activities; it does not certify the activities themselves, and it does not certify an individual's on-the-job performance.

V · PRIMARY CONFORMANCE STATEMENT

V. Primary Conformance Statement: Clause 7.2 (Competence)

This section addresses the relationship between a GAISB credential and ISO/IEC 42001 Clause 7.2, the requirement most directly supported by personnel certification.

ISO/IEC 42001:2023 · CLAUSE 7.2 · COMPETENCE (SUMMARY)

In summary, Clause 7.2 requires the organization to (a) determine the competence needed by persons whose work affects its AI performance; (b) ensure those persons are competent on the basis of education, training, or experience; (c) where applicable, act to acquire the needed competence and evaluate the effectiveness of those actions; and (d) retain documented information as evidence of competence. The authoritative text is the published standard; the summary above is a paraphrase and is not a substitute for it.

HOW A GAISB CREDENTIAL RELATES TO CLAUSE 7.2

Subclause (a) is the organization's own determination. The GAISB Common Body of Knowledge, which defines the competence expected of a qualified AI practitioner across seven domains validated through Job Task Analysis, may be used as a reference model for that determination, but does not replace it.

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

Subclause (c) is supported by GAISB preparatory learning, the Continuing Professional Education program, and recertification requirements. Evaluation of the effectiveness of competence actions remains the organization's responsibility; GAISB examination results and CPE records are inputs to that evaluation.

Subclause (d) is evidenced by the GAISB certificate, the Public Verification 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 GAISB-issued artifacts as Clause 7.2(d) documented information:

ARTIFACT	CONTENT	VERIFICATION METHOD
GAISB Certificate	Certified professional's full name, credential, date of issuance, date of expiration, and unique credential identifier.	Lookup of the credential identifier at the GAISB Public Verification Registry.
GAISB Registry Entry	Public record of the credential holder and current status (Active, Lapsed, Suspended, Revoked).	Direct lookup at the GAISB Public Verification Registry (registry.gaisb.org).
Attestation of Adherence	Signed declaration from the holder affirming adherence to the GAISB Professional Code of Conduct (COC-2026-01, Article XIV).	Executed at initial certification and renewed at each recertification; retained by GAISB.
CPE Record	Record of Continuing Professional Education credits earned during the active certification cycle.	Held by the credential holder; submitted to GAISB annually under the CPE program.

5.2 Guidance for ISO/IEC 42001 auditors

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

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

5.3 Recommended role-to-credential mapping

Organizations may use the following guideline to determine the GAISB credential appropriate for each AI-affecting role. The final determination remains with the organization per Clause 7.2(a).

ORGANIZATIONAL ROLE	RECOMMENDED GAISB CREDENTIAL	RATIONALE
Business user of AI systems	GAISB AI Essentials™	Supports Clause 7.3 (Awareness) and is designed as evidence toward the EU AI Act Article 4 AI literacy obligation; sufficient for non-configuring use.
AI developer / engineer	GAISB AI Practitioner™	Applied competence in system design, evaluation, and responsible development per A.6 lifecycle controls.
AI product or deployment owner	GAISB AI Practitioner™	Competence across lifecycle operation, monitoring, and impact-assessment execution.
AI governance or strategy lead	GAISB AI Team Architect™	Competence across AIMS design inputs: policy, risk framework, cross-organizational program.
Chief AI Officer / AI Risk Officer	GAISB AI Team Architect™	Competence across all seven domains; appropriate for a top-management AI role per Clause 5.3.
Security or governance specialist (regulated)	GAISB-Sec™ / GAISB-Gov™ (by request)	Domain-specific competence for AI security hardening or governance and oversight in regulated environments.

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 GAISB 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	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
4.1	Understanding the organization and its context relative to AI.	D1 · D6	P	Domains 1 and 6 cover organizational AI context, industry positioning, and external drivers.
4.2	Understanding needs and expectations of interested parties.	D5 · D6	P	The Ethics domain addresses stakeholder identification for AI; the Strategy domain addresses business stakeholder alignment.
4.3	Determining the scope of the AI management system.	D6	Sp	The Strategy domain covers AI portfolio scoping; formal AIMS scope is an organizational activity supported by, not replaced by, GAISB competence.
4.4	AI management system: establishment and maintenance.	D6	Sp	AIMS establishment is an organizational activity; GAISB certifies the personnel who design, operate, and improve the system.

6.2 Clause 5: Leadership

CLAUSE	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
5.1	Leadership and commitment from top management.	D1 · D6	P	Domains 1 and 6 establish frameworks for executive AI sponsorship and board-level commitment.
5.2	AI policy: establishment, maintenance, alignment.	D5 · D6	S	The Ethics domain covers AI policy frameworks (acceptable-use, responsible-AI, data-handling); the Strategy domain covers enterprise policy integration.
5.3	Organizational roles, responsibilities, and authorities.	D6 · D4	S	The Strategy domain covers AI operating models (CoE, federated, embedded); the Agents domain covers role definition in agentic systems.

6.3 Clause 6: Planning

CLAUSE	REQUIREMENT	GAISB 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 the Ethics and Strategy domains.
6.1.2	AI risk assessment process.	D5 · D2 · D3 · D4	S	The Ethics domain covers AI-specific risk taxonomies; the technical domains provide the substrate for model, data, and system-level risk identification.

6.1.3	AI risk treatment: selection and implementation of controls.	D5 · D3 · D4	S	The Ethics domain covers bias and fairness mitigations; the technical domains cover grounding, guardrails, evaluation, and oversight patterns.
6.1.4	AI system impact assessment.	D5	S	The Ethics domain includes AI impact-assessment methodology aligned to ISO/IEC 42005, covering affected individuals, groups, and societal effects.
6.2	AI objectives and planning to achieve them.	D6	S	The Strategy domain covers AI objective-setting, ROI modeling, sensitivity analysis, and portfolio planning.
6.3	Planning of changes to the AIMS.	D6	P	The Strategy domain covers AI transformation, phased change, and dual-track execution models.

6.4 Clause 7: Support

CLAUSE	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
7.1	Determination and provision of resources for the AIMS.	D6	Sp	The Strategy domain covers resource allocation for AI initiatives; provisioning is an organizational responsibility.
7.2	Competence: determine, ensure, and retain evidence.	All Domains	D	A GAISB credential is retainable evidence for subclauses (b) and (d) and supports (a) and (c). See Section V.
7.3	Awareness of AI policy, contribution, and nonconformance implications.	All Domains	P	GAISB examinations and the Code of Conduct assess awareness of responsible AI practice and professional accountability. Awareness of the organization's own AI policy is organization-specific and must be evidenced by the organization.
7.4	Internal and external communication relevant to the AIMS.	D6	Sp	The 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	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
8.1	Operational planning and control.	D4 · D6 · D7	S	The Agents, Strategy, and Applied domains cover operational deployment, workflow orchestration, rollout strategy, 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	The Ethics domain covers impact-assessment methodology at the system operational level.

6.6 Clause 9: Performance Evaluation

CLAUSE	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
9.1	Monitoring, measurement, analysis, evaluation.	D2 · D4 · D6 · D7	S	The Foundations domain covers model evaluation methodology; the Agents and Applied domains cover production monitoring and measurement dashboards; the 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	The Strategy domain covers AI portfolio review and executive reporting.

6.7 Clause 10: Improvement

CLAUSE	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
10.1	Continual improvement of the AIMS.	D6 · D7	S	The Strategy domain covers iterative AI transformation and portfolio evolution; the Applied domain covers experiment-driven iteration of deployed systems.
10.2	Nonconformity and corrective action.	D5 · D6 · D7	P	The Ethics and Applied domains cover incident response and post-incident lessons; the 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 objectives. Organizations select applicable controls through the Statement of Applicability derived from risk assessment. This section maps each control to GAISB competencies.

7.1 A.2: Policies Related to AI

CONTROL	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
A.2.2	AI policy: establishment and maintenance.	D5 · D6	S	The 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	The Strategy domain covers enterprise-policy integration; the 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 GAISB certification.

7.2 A.3: Internal Organization

CONTROL	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
A.3.2	AI roles and responsibilities: defined, assigned, communicated.	D6	S	The 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	The Ethics domain covers whistleblowing, responsible disclosure, and the professional obligation to report; the GAISB Code of Conduct (Article IX) mandates such reporting.

7.3 A.4: Resources for AI Systems

CONTROL	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
A.4.2	Resource documentation for AI systems.	D6	P	The Strategy domain covers AI portfolio documentation; specific resource registers are organizational outputs.
A.4.3	Data resources: identification, procurement, governance.	D5 · D3 · D2	S	The 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	The 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	The Foundations domain covers compute considerations; the Agents domain covers runtime requirements. Infrastructure specifics are organizational.
A.4.6	Human resources: competence, assignment, documentation.	All Domains	D	A GAISB credential is a human-resource competence artifact. Pair with the Clause 7.2 conformance statement (Section V).

7.4 A.5: Assessing Impacts of AI Systems

CONTROL	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
A.5.2	AI system impact assessment process: defined and applied.	D5	S	The Ethics domain covers impact-assessment methodology aligned to ISO/IEC 42005, including scope, stakeholder mapping, and severity analysis.
A.5.3	Documentation of AI system impact assessments.	D5	P	The Ethics domain covers documentation requirements; organization-specific templates remain an AIMS output.
A.5.4	Assessment of AI system impact on individuals or groups.	D5	S	The Ethics domain covers individual-level harms: bias, discrimination, privacy, autonomy, consent.
A.5.5	Assessment of societal impacts of AI systems.	D5 · D1	S	The Ethics domain addresses societal-scale implications; Domain 1 covers macro AI impacts.

7.5 A.6: AI System Life Cycle

CONTROL	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
A.6.1.2	Objectives for responsible development of AI systems.	D5	S	The Ethics domain defines responsible-development objectives: fairness, transparency, accountability, safety.
A.6.1.3	Processes for responsible design and development of AI systems.	D5 · D2 · D3 · D4	S	The Ethics domain covers responsible-design principles; the technical domains cover responsible implementation.
A.6.2.2	AI system requirements and specification.	D4 · D6 · D7	S	The Agents domain covers AI system specification; the Strategy and Applied domains cover requirement elicitation and use-case scoping.
A.6.2.3	Documentation of AI system design and development.	D4 · D3	P	The Agents and Prompt Engineering domains cover system-architecture documentation; formal templates are an organizational output.
A.6.2.4	AI system verification and validation.	D2 · D3 · D4	S	The Foundations, Prompt Engineering, and Agents domains cover evaluation methodology, test harnesses, regression testing, and red-teaming.
A.6.2.5	AI system deployment.	D4 · D6 · D7	S	The Agents domain covers deployment patterns; the Applied domain covers rollout strategies (dark launch, canary, ring); the Strategy domain covers change management and stakeholder readiness.
A.6.2.6	AI system operation and monitoring.	D4 · D7	S	The Agents and Applied domains cover production monitoring, drift detection, LLMOps, human oversight, and intervention patterns.
A.6.2.7	AI system technical documentation.	D4 · D2	P	The technical domains cover documentation of model cards, system cards, and evaluation records.
A.6.2.8	AI system recording of event logs.	D4 · D7	P	The Agents and Applied domains cover logging, tracing, and observability; retention policy is an organizational AIMS output.

7.6 A.7: Data for AI Systems

CONTROL	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING 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.
A.7.3	Acquisition of data: sourcing, licensing, consent.	D5	S	The 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	The 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	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
A.8.2	System documentation and information for users.	D4 · D5	S	The Agents domain covers user-facing system documentation; the Ethics domain covers transparency disclosures.
A.8.3	External reporting on AI systems.	D5	P	The Ethics domain covers transparency reporting frameworks; specific formats are organizational.
A.8.4	Communication of incidents: disclosure to affected parties.	D5 · D7	P	The Ethics domain covers incident-communication principles; the Applied domain covers in-production incident handling; detailed procedures are organizational.
A.8.5	Information for interested parties: ongoing.	D5 · D6	P	The Ethics and Strategy domains cover stakeholder communication frameworks.

7.8 A.9: Use of AI Systems

CONTROL	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
A.9.2	Processes for responsible use of AI systems.	D5 · D6	S	The Ethics domain defines responsible-use principles; the Strategy domain covers operational implementation at enterprise scale.
A.9.3	Objectives for responsible use.	D5	S	The 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	The Agents domain covers intended-use specification and boundary definition; the Ethics domain covers misuse prevention.

7.9 A.10: Third-Party and Customer Relationships

CONTROL	REQUIREMENT	GAISB DOMAIN(S)	STRENGTH	MAPPING RATIONALE
A.10.2	Allocation of responsibilities across third-party relationships.	D6 · D5	P	The Strategy domain covers AI-vendor management; the Ethics domain covers accountability allocation.
A.10.3	Suppliers: selection, oversight, risk management.	D6	P	The Strategy domain covers AI supplier selection, due diligence, and lifecycle oversight.
A.10.4	Customers: AI-specific obligations and disclosures.	D5 · D6	P	The Ethics and Strategy domains cover customer disclosure obligations and commercial AI integrity.

VIII · COVERAGE MATRIX

VIII. Coverage Matrix: Domains × Clauses

The matrix reports, for each GAISB domain, the highest mapping strength that domain achieves within the clause family, as recorded in the clause-by-clause and Annex A tables (Sections VI and VII). Cells indicate strength: D (Direct), S (Substantial), P (Partial), Sp (Supportive). An empty cell means the domain is not cited for that family in the detail tables.

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

Reading the matrix. Two families reach Direct across all seven domains, Clause 7 (Support) and Annex A.4 (Resources), because the Competence requirement (Clause 7.2) and the Human Resources control (A.4.6) each map to every domain; these are the personnel-competence core of the standard, and the credential is itself retainable evidence for them. The Awareness requirement (7.3) is rated Partial because awareness of the organization's own AI policy is organization-specific; the remaining sub-clauses in those families (7.1, 7.4, 7.5) are organizational activities rated Supportive. Substantial coverage concentrates in the planning, operational, lifecycle, data, and impact-assessment areas, where qualified personnel execute the AIMS; Domain 7 (Applied) carries the deployment, monitoring, and incident-handling competencies in Clauses 8 to 10 and A.6. Partial and Supportive cells indicate that GAISB-certified personnel contribute but the formal AIMS outputs remain an organizational responsibility.

IX · USAGE GUIDANCE

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

This section provides practical guidance for using a GAISB 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-credential mapping in Section 5.3 as a starting point, not as the determination itself.
- **Identify personnel gaps.** For each role, determine which current staff hold appropriate GAISB credentials, which need certification, and which require alternative or supplementary evidence.
- **Build certification into the AIMS plan.** Include GAISB certification as part of the Clause 7.2(c) action plan. Retain the GAISB 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 GAISB contributes, this dossier may be cited as supporting rationale; the auditor determines its weight.

9.2 For ISO/IEC 42001 certification bodies

- **The Public Verification Registry is the primary verification channel.** The Registry provides credential status for any GAISB holder named in client personnel records.
- **Use the coverage matrix (Section VIII) as audit-planning context.** It indicates where a GAISB credential may be treated as corroborating competence evidence and where it should not be. Sampling and evidence sufficiency remain the certification body's determination under ISO/IEC 17021-1 and ISO/IEC 42006.
- **Distinguish competence evidence from activity evidence.** GAISB certifies that personnel have been assessed as competent. Evidence that the personnel performed required activities (impact assessments, risk treatments, monitoring) remains a separate audit line.
- **Contact GAISB with verification questions.** Certification bodies may direct credential-verification questions to the GAISB Standards Office through the channels published on the GAISB website.

9.3 For procurement, legal, and risk teams

- **Reference GAISB in AI-vendor contracts.** Vendors may be required to maintain GAISB-certified personnel in defined roles affecting the AI system subject to the contract.
- **Reference GAISB in internal AI risk documentation.** Use the credential-to-role mapping to define minimum competence requirements for internal AI-affecting roles.
- **Use the dossier in supplier due diligence.** Suppliers that can demonstrate GAISB-certified personnel in key AI roles provide a more structured Clause 7.2 evidence layer than those relying on unstructured claims.

9.4 For HR and Learning & Development teams

- **Use the Common Body of Knowledge as a competency-model baseline.** It is a published competency model for AI practice; use it to structure internal role libraries, development paths, and performance criteria.
- **Design internal AI-literacy programs toward GAISB AI Essentials™ preparation.** Essentials is designed as evidence toward 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 GAISB 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 GAISB CERTIFICATION DOES NOT ESTABLISH

- GAISB does not establish organizational conformance to ISO/IEC 42001. Only a third-party audit by a certification body accredited under ISO/IEC 17021-1 and ISO/IEC 42006 can establish that conformance.
- GAISB 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.
- GAISB does not certify an individual's job performance. It certifies competence against a defined Body of Knowledge at the point of assessment.
- GAISB does not cover all clauses and controls at substantial depth. Document control (Clause 7.5), internal audit program design (Clause 9.2), and management-review cadence (Clause 9.3) are supported by but not primarily covered by the credential.
- GAISB is not itself accredited under ISO/IEC 17024 at this edition. It operates under 17024 principles and has published its accreditation roadmap in the Common Body of Knowledge, Section XIX.

10.2 ON THE ALIGNMENT FIGURE

- The approximately 77% figure (§3.5) is an internal, weighted GAISB assessment of personnel-competence coverage, not a certified metric and not an ISO measurement. Under band-midpoint weightings it is approximately 70%; it is reported as an assessment with a 70% to 77% range, not a precise value.

10.3 WHERE THIS DOSSIER WILL EVOLVE

- Subsequent editions are planned to incorporate operational templates (Statement of Applicability references, competence-register templates, audit-evidence packets) as the GAISB program matures. None of these exist at this edition.
- Sector-specific addenda for regulated industries (healthcare, finance, public sector, defense) are planned and not yet issued.
- As ISO/IEC JTC 1/SC 42 issues clarifications, interpretations, or amendments to ISO/IEC 42001, this dossier will be updated to reflect them.

10.4 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 and paraphrases rather than reproduces the standard's text. No claim of official ISO recognition of the GAISB credentials 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 through the channels published on the GAISB website. 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. Clause-by-clause and Annex A controls mapping between GAISB Edition 1.0 and ISO/IEC 42001:2023. Primary Conformance Statement for Clause 7.2 and A.4.6; weighted alignment derivation (§3.5); headline figure 78%.
1.0.1	2026	GAISB Standards Council	Interim amendment. Credential naming aligned to the GAISB brand; Domain 7 mappings added to Clauses 8 to 10 and A.6, A.8; Clause 7.3 re-rated from Direct to Partial; headline figure revised to 77% with a disclosed 70% to 77% range; "satisfies" language replaced with "evidences" or "supports" where the organization retains the determination; Clause 7.2 text paraphrased rather than reproduced; unverified operational claims removed; ISO/IEC 42005, 42006, 23894 and NIST AI 600-1 added to references; companion reference updated to CBK Edition 1.0.1; editorial pass.
Planned 1.1	Q2 2027	GAISB Standards Council	Annual review. Incorporate public comments, add audit-evidence templates and sector-specific addenda as they are completed.

DOCUMENT CONTROL

Instrument: ISO-DSR-2026-01 · Edition 1.0.1 · Effective Q2 2026 · Review cycle: annual · Governed by the GAISB Standards Council.

REVIEW CYCLE

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

PUBLIC COMMENT

Public comment on this dossier is continuously accepted through the channels published on the GAISB website. Comments received prior to the annual review deadline will be considered for incorporation in the subsequent edition.

CITATION

> *GAISB. (2026). The GAISB & ISO/IEC 42001 Alignment Dossier, Edition 1.0.1 (ISO-DSR-2026-01). 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 42005:2025. Information technology. Artificial intelligence. AI system impact assessment. International Organization for Standardization, Geneva.
- ISO/IEC 42006:2025. Information technology. Artificial intelligence. Requirements for bodies providing audit and certification of artificial intelligence management systems. International Organization for Standardization, Geneva.
- ISO/IEC 23894:2023. Information technology. Artificial intelligence. Guidance on risk management. 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 GAISB Common Body of Knowledge, Edition 1.0.1 (CBK-2026-01). Global AI Standards Body, 2026.
- The GAISB Job Task Analysis, Edition 1.0 (JTA-2026-01). Global AI Standards Body, 2026.
- The GAISB Examination Blueprint & Cut-Score Methodology (EXM-2026-01). Global AI Standards Body, 2026.
- The GAISB Professional Code of Conduct, Edition 1.0.1 (COC-2026-01). Global AI Standards Body, 2026.

COMPLEMENTARY AUTHORITATIVE FRAMEWORKS

- NIST AI Risk Management Framework 1.0 and the Generative AI Profile (NIST AI 600-1). National Institute of Standards and Technology, U.S. Department of Commerce.
- Regulation (EU) 2024/1689, the Artificial Intelligence Act, including Article 4 (AI literacy). European Parliament and Council of the European Union.
- OECD Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). 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 (PLANNED, NOT YET ISSUED)

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

GAISB

The Global AI Standards Body (GAISB™) is the governance organization issuing and maintaining the GAISB credentials (GAISB AI Essentials, GAISB AI Practitioner, GAISB AI Team Architect) and their supporting body of normative documentation.

ISO/IEC 42001 tells the organization what its AI Management System must do.
A GAISB credential evidences that a named professional has been assessed as competent to do it.