GSDC · GLOBAL SKILL DEVELOPMENT COUNCIL

ISO 42001 vs ISO 27001

A Side-by-Side Comparison Guide

What each standard requires, where they overlap, and why one integrated management system beats two separate implementations.

WEBINAR DATE	FORMAT
21 July 2026	Live Online · 2 Hours

Complimentary resource for GRC professionals, auditors, and compliance leads · gsdcouncil.org

What is ISO 27001?

Scope

Information security management systems (ISMS) — covering the confidentiality, integrity, and availability of information assets across an organisation.

Who Needs It

Any organisation handling sensitive data — financial services, healthcare, technology, government, and any sector where data breaches carry regulatory or reputational risk.

Core Requirements

→ Annex A controls — access control, incident response, supplier relationship management, and internal audit

→ The Plan-Do-Check-Act (PDCA) cycle as the operational model for continual improvement

→ Risk assessment and treatment — identify threats, assess likelihood and impact, define treatment options

→ ISMS scope definition — what information assets are in scope, what are excluded, and why

Certification Body

Accredited third-party certification body — the same body can certify both ISO 27001 and ISO 42001 simultaneously.

Typical Timeline

6–18 months depending on organisation size, existing controls, and scope complexity.

What is ISO 42001?

Scope

Artificial intelligence management systems (AIMS) — covering the responsible development, deployment, monitoring, and decommissioning of AI systems that have a material impact on people or operations.

Who Needs It

Any organisation developing, deploying, or using AI systems — including those procuring third-party AI tools — where those systems influence decisions affecting individuals or business operations.

Core Requirements

→ AI risk assessment — identifying and treating risks specific to AI systems, including bias, errors, and misuse

→ Bias and fairness controls — demographic testing, mitigation strategies, and AI impact assessments

→ Human oversight mechanisms — accountability structures, escalation paths, and human-in-the-loop requirements

→ AI lifecycle governance — controls from system design through deployment, monitoring, and decommission

→ Transparency and explainability — documenting how AI systems reach conclusions

How It Differs from ISO 27001

ISO 42001 adds AI-specific controls not addressed by information security — algorithmic bias, explainability, human oversight, and AI impact assessments. It uses the same Annex SL high-level structure as ISO 27001, which means organisations with an existing ISMS have a significant head start.

Typical Timeline

4–12 months for organisations with an existing ISO 27001 ISMS. Starting from scratch with both standards simultaneously: 12–18 months depending on AI portfolio complexity.

Side-by-Side Comparison

Requirement Area	ISO 27001	ISO 42001	Shared?	Notes
Scope definition	Clause 4	Clause 4	Yes	Shared Annex SL structure
Leadership & commitment	Clause 5	Clause 5	Yes	AI-specific accountability added
Risk assessment	Clause 6	Clause 6	Partial	ISO 42001 adds AI impact assessment
Access control	Annex A 5.15	Implied	Partial	ISO 42001 extends to AI system access
Incident response	Annex A 5.26	Clause 8.5	Partial	ISO 42001 adds AI-specific failure modes
Supplier management	Annex A 5.19	Clause 8.6	Partial	ISO 42001 adds AI vendor due diligence
Audit & review	Clause 9	Clause 9	Yes	Same PDCA evaluation cycle
Bias & fairness controls	Not present	Clause 8.4	No	ISO 42001 only — new requirement
Human oversight	Not present	Clause 8.3	No	ISO 42001 only — new requirement
AI lifecycle governance	Not present	Clause 8.2	No	ISO 42001 only — new requirement

The Convergence Case

Annex SL: A Shared Architectural Foundation

Both ISO 27001 and ISO 42001 use the ISO Annex SL high-level structure — the same clause numbering and the same framework for scope, leadership, planning, support, operation, evaluation, and improvement. An organisation that has implemented ISO 27001 already has 60–70% of the structural foundation required for ISO 42001. The remaining effort is targeted at the AI-specific controls — not the management system architecture.

One PDCA Cycle, Two Standards

Plan-Do-Check-Act is the operating model for both standards. One continual improvement process serves both simultaneously — there is no need to run separate review cycles, separate management reviews, or separate internal audit programmes. This alone represents a significant reduction in ongoing compliance overhead.

Unified Risk Management

One risk register can cover both information security risks and AI system risks. The methodology is identical — identify threats, assess likelihood and impact, define treatment options, monitor and review. The risk sources are different, but the framework that manages them does not need to be.

Organisations with an existing ISO 27001 ISMS typically achieve ISO 42001 certification within 4–8 months — because the management system foundation is already in place.

What's Genuinely New in ISO 42001

These are the controls that are not covered by ISO 27001 and require separate implementation effort. They represent the true incremental scope of ISO 42001 for an organisation that already holds ISO 27001 certification.

Bias and Fairness Controls	AI impact assessments identifying potential for discriminatory or harmful outputs. Demographic testing across protected characteristics. Documented mitigation strategies for identified bias risks, with periodic review as models are updated or retrained.
Human Oversight	Accountability structures that define who is responsible for AI system outputs. Escalation paths for cases where AI decisions affect individuals adversely. Human-in-the-loop requirements for high-risk AI decisions — particularly those affecting employment, credit, healthcare, or access to services.
AI Lifecycle Governance	Controls that apply from initial system design through development, testing, deployment, monitoring, and eventual decommissioning. This includes change management for model updates, version control, and documented decommission procedures when AI systems are retired.
Transparency and Explainability	Requirements to document how AI systems reach conclusions — particularly for systems that affect individuals. This does not require publication of proprietary model details, but does require the organisation to be able to explain the basis for AI-influenced decisions upon request.
AI-Specific Supplier Due Diligence	Assessing AI vendors and third-party model providers for bias in training data, data provenance and lineage, model drift management, security of model APIs, and contractual accountability for AI system behaviour. Standard supplier assessments under ISO 27001 Annex A 5.19 do not cover these areas.

Your Path to Dual Certification

Where to Start

Step 1	Begin with an ISO 27001 gap assessment if not already certified. Identify what controls are in place and what is missing.
Step 2	Map your existing controls to ISO 42001 requirements using the Annex SL structure as your guide.
Step 3	Identify the genuine gaps — typically bias controls, human oversight mechanisms, and AI lifecycle governance.
Step 4	Build a unified ISMS that serves both standards within a single policy and control framework.
Step 5	Run a single internal audit covering both standards simultaneously — one audit programme, two scope coverages.
Step 6	Engage an accredited certification body for dual assessment. Many accredited bodies now offer joint ISO 27001 and ISO 42001 audits.

How Long It Takes

Starting point	Typical timeline
Existing ISO 27001 certification	4–8 months to achieve ISO 42001
ISO 27001 in progress, ISO 42001 alongside	8–12 months for both
Starting from scratch with both standards	12–18 months depending on AI portfolio complexity

GSDC · WEBINAR REMINDER

ISO 27001 + ISO 42001 Two Standards. One Management System.

Date: Monday, 21 July 2026

Time: 10:30 PM SGT | 8:00 PM IST | 10:30 AM EDT

Duration: 2 Hours — Live Online

Includes: GSDC Attendance Certificate · Worth $129 · Complimentary

Reserve your seat:

https://www.gsdcouncil.org/certification-program/iso-27001-and-42001-webinar-2026

GSDC · Global Skill Development Council · gsdcouncil.org