CIRCOLARE TECNICA

Prot. DC2026SPM050 **Milano**, 19-02-2026

A tutti gli Organismi di certificazione accreditati/accreditandi
Alle Associazioni degli Organismi di valutazione della conformità
A tutti gli Ispettori/Esperti del Dipartimento DC

Loro sedi

OGGETTO: Circolare tecnica DC N° 08/2026 - Disposizioni in merito all'accreditamento UNI CEI EN ISO/IEC 17021-1 degli Organismi di Certificazione a fronte della norma UNI CEI ISO/IEC 42001

Premessa

Il presente documento fornisce disposizioni e indirizzi per l'accreditamento degli Organismi di certificazione (in seguito OdC) operanti in conformità alla UNI CEI EN ISO/IEC 17021-1 per la certificazione di sistemi di gestione dell'intelligenza artificiale a fronte della norma UNI CEI ISO/IEC 42001 (d'ora in avanti abbreviata in ISO/IEC 42001).

Come noto, nel corso del 2024, il Parlamento europeo ha approvato il Regolamento UE 2024/1689 che stabilisce regole armonizzate sull'intelligenza Artificiale, cosiddetto "AI Act".

Il nuovo Regolamento mira a garantire che i sistemi di Intelligenza Artificiale immessi sul mercato europeo siano sicuri e rispettino i diritti e i valori fondamentali dei Cittadini comunitari e delle Persone extracomunitarie ma a qualunque titolo presenti nell'Unione Europea. L'AI Act, inoltre, si pone l'obiettivo di stimolare gli investimenti e l'innovazione nel settore dell'intelligenza artificiale e facilitare lo sviluppo di un mercato unico per applicazioni di intelligenza artificiale lecite, sicure e affidabili, posizionando l'UE tra i principali attori a livello mondiale.

In risposta al consistente affermarsi dell'utilizzo di applicazioni di Intelligenza Artificiale e in considerazione dei rischi di tali applicazioni, si sono attivati anche gli enti di normazione internazionali ISO e IEC che hanno sviluppato la norma ISO/IEC 42001, emessa nel 2023, il cui obiettivo è supportare le organizzazioni nell'utilizzo affidabile e responsabile dei sistemi di IA al fine di salvaguardare tutte le risorse coinvolte e creare fiducia nell'applicazione di tali sistemi.

La ISO/IEC 42001:2023, anche se non armonizzata al Regolamento AI Act, è l'unico strumento certificabile al momento da parte di Organismi di Certificazione di Sistemi di Gestione accreditati a fronte della norma UNI CEI EN ISO/IEC 17021-1.

Per ottenere l'Accreditamento a fronte della Norma citata, gli OdC devono soddisfare non solo i requisiti della norma UNI CEI EN ISO/IEC 17021-1, ma anche quelli della norma UNI CEI ISO/IEC 42006:2025 (d'ora in avanti abbreviata in ISO/IEC 42006), quale norma di Livello 4 secondo il documento EA 1/06.

Il principale obiettivo che ha portato allo sviluppo della ISO/IEC 42001 è legato alla necessità di soddisfare le esigenze di gestione dei rischi riferibili all'uso dei sistemi di IA, con riferimento ai requisiti definiti nei diversi ambiti giuridici e alle specificità degli ambiti tecnologici, tenendo in considerazione anche le minacce tradizionalmente conosciute. La "governance" che la norma ISO/IEC 42001 richiede di creare nelle organizzazioni che adottano sistemi di AI, prevede politiche di governo dei rischi che possono interessare i sistemi di AI nel loro ciclo di vita, dalla fase di predisposizione dei dati necessari per l'addestramento degli algoritmi e della validazione dei modelli ottenuti, sino alla gestione degli usi non autorizzati delle soluzioni rese operative.

La harmonized structure della norma ISO/IEC 42001 consente alle organizzazioni di integrare i requisiti previsti con quelli di un altro sistema di gestione già adottato nell'ambito della propria struttura (es. ISO/IEC 9001, ISO/IEC 27001, ISO/IEC 27701).

Pur trattandosi di uno standard volontario, si evidenzia che lo stesso legislatore europeo nell'AI Act al fine di mitigare i rischi per la salute, la sicurezza, i diritti e le libertà fondamentali degli esseri umani scaturenti, in modo volontario e non, dai sistemi di Intelligenza Artificiale classificabili ad alto rischio ha individuato l'obbligo di implementazione proprio di un Sistema di gestione, strumento volto a garantire la continua affidabilità, durante l'intero ciclo di vita, di prodotti o servizi che impiegano sistemi di Intelligenza Artificiale.

Si rappresenta che i contenuti della presente circolare sono frutto di alcuni progetti pilota che ACCREDIA-DC ha condotto prima della pubblicazione definitiva dello standard ISO/IEC 42006.

Le caratteristiche del servizio di valutazione della conformità

Lo scopo della norma ISO/IEC 42001 è garantire che i sistemi siano sviluppati e utilizzati in modo responsabile:

a. promuovendo lo sviluppo e l'utilizzo di sistemi di IA che siano affidabili, trasparenti e responsabili nel rispetto delle leggi e dei regolamenti in materia di protezione dei dati o degli obblighi nei confronti delle parti interessate;

b. valorizzando i principi etici nell'impiego dei sistemi di IA, come l'equità, la non discriminazione e il rispetto della privacy;

c. supportando le organizzazioni nell'individuare e gestire i rischi legati all'implementazione dell'IA, garantendo l'adozione di misure di mitigazione adeguate.

La norma, basata anch'essa sulla struttura HS e sul ciclo PDCA, prevede come step iniziale un'analisi accurata del contesto, in cui devono essere individuate le esigenze delle parti interessate interne ed esterne rilevanti per il suo scopo e in grado di influenzare la capacità del suo sistema di gestione dell'IA di raggiungere il risultato desiderato. Una volta definita la soluzione o il sistema di AI da adottare, viene richiesto che tali effetti

sulle persone, gruppi o sulla società nel suo complesso, siano oggetto di una “valutazione di impatto”, capace di evidenziare come tutte le fasi del ciclo di vita siano tali da garantire i diritti e le libertà delle Persone che possono esserne interessate. Ne deriva che, oltre all’aspetto tipicamente tecnologico, venga messa in evidenza l’esigenza di un approccio etico di salvaguardia e accrescimento del bene comune e gli OdC saranno chiamati a valutare senz’altro i percorsi tecnologici e di business che portano le organizzazioni all’adozione delle soluzioni e sistemi di AI, ma soprattutto l’approccio di governo riferito ai valori superiori della protezione dei diritti e libertà dei Cittadini. Questa visione vuole “premiare” le scelte consapevoli ed eticamente responsabili in ottica di sostenibilità delle organizzazioni clienti e della società tutta. Appare naturale, in questa ottica, che l’approccio di valutazione sia sempre basato su una logica di rischio e la Norma UNI CEI ISO/IEC 42001:2023 adottando la struttura ISO armonizzata, è indirizzata proprio in tal senso. Infatti, una volta definito il contesto e le esigenze delle parti interessate, l’organizzazione, attraverso la propria struttura organizzativa e il suo management, deve dotarsi di una politica che definisca gli obiettivi del sistema IA, individui le risorse coinvolte, le responsabilità alle stesse associate e le esigenze di formazione e pianifichi le operazioni di valutazione dei rischi e raggiungimento degli obiettivi, nonché le fasi di controllo e monitoraggio continuo dell’efficacia del sistema IA implementato, fino a completare il ciclo PDCA.

Dal punto di vista tecnico, la norma ISO/IEC 42001 fa riferimento diretto o indiretto anche ad altre norme tecniche rilevanti, talune delle quali essenziali nel processo di valutazione di un AIMS:

Norma	*Descrizione*	*Ambito di applicazione*
ISO/IEC 22989	Concetti e terminologia dell'intelligenza artificiale.	Definizione dei concetti fondamentali e dei ruoli nell'ecosistema IA.
ISO/IEC 23894	Guida alla gestione del rischio per sistemi di IA.	Identificazione, valutazione e trattamento dei rischi legati all'IA.
ISO/IEC TR 24027	Bias nei sistemi IA e nel decision making.	Identificazione e mitigazione dei bias nei dati e nei modelli IA.
ISO/IEC TR 24368	Panoramica delle problematiche etiche e sociali dell'IA.	Supporto alla valutazione dell'impatto sociale dei sistemi IA.
ISO/IEC 5338	Processi per il ciclo di vita dei sistemi di IA	Definizione dei processi tecnici del ciclo di vita dei sistemi IA (selezione algoritmi, training, validazione continua), supporta l’implementazione tecnica del concetto di AI responsabile
Serie ISO/IEC 5259	Qualità dei dati utilizzati in analisi e sistemi di apprendimento automatico (machine learning)	Modelli, misure, reportistica, requisiti e linee guida per la gestione della qualità dei dati
ISO/IEC 25024	Misurazione della qualità dei dati.	Valutazione della qualità dei dati utilizzati nei sistemi IA.
ISO/IEC 25059	Modelli di qualità specifici per i sistemi di IA	Definizione di un modello tecnico per valutare la qualità dei sistemi IA comprese caratteristiche come spiegabilità, equità, robustezza
ISO/IEC 42005	Valutazione di impatto dei sistemi di IA	Linee guida sull’applicazione di metodi di valutazione di impatto
Serie ISO/IEC TR 24029	Valutazione della robustezza dei modelli basati su reti neurali per sistemi di IA	Strumenti tecnici per valutare la robustezza dei modelli IA con applicazione di metodi formali e statistici per validare il comportamento del sistema
ISO/IEC TS 4213	Metodologie per la valutazione delle prestazioni di classificazione nei	Valuta le prestazioni tecniche dei modelli ML, supporto alla selezione e il monitoraggio dei modelli

	modelli, sistemi e algoritmi di machine learning (ML)	
ISO/IEC 23053	Quadro concettuale per i sistemi di intelligenza artificiale (AI) basati su machine learning (ML)	Modello concettuale per descrivere sistemi AI basati su ML, supporto all'identificazione e attestazione dei componenti e delle funzioni del sistema
ISO/IEC 31000	Linee guida generali per la gestione del rischio	Base metodologica per la gestione del rischio, contribuisce a strutturare il pensiero strategico e operativo sul rischio
ISO/IEC 38500 e 38507	Governance dell'IT e implicazioni dell'uso dell'IA.	Supporto alla definizione di politiche, ruoli, responsabilità e strategie IT, promozione della trasparenza e della responsabilità
ISO/IEC 27001 e 27701	Gestione della sicurezza delle informazioni e della privacy	Quadro per la sicurezza delle informazioni e la privacy per garantire un'IA affidabile e responsabile

In analogia ad altre norme sui sistemi di gestione, anche la ISO/IEC 42001 è dotata di un elenco di controlli (Appendice A Normativa) utili per il raggiungimento/misurazione degli obiettivi in relazione all'uso dell'IA e ad affrontare le minacce individuate nel processo di valutazione del rischio relativo alla progettazione, sviluppo e funzionamento dei sistemi di IA.

Il testo della norma è poi arricchito di una serie di Appendici utili a configurare una guida, ancorché non esaustiva, per:

a. implementare i controlli (rif. Appendice B normativa);
b. delineare i potenziali obiettivi organizzativi e le fonti di rischio associate (rif. Appendice C informativa);
c. utilizzare il sistema di gestione dell'IA in diversi domini o settori e la sua integrazione con altri MS.

Regole di Certificazione

Si applicano le prescrizioni della norma UNI CEI EN ISO/IEC 17021-1 integrata dalla ISO/IEC 42006. Nel processo di certificazione l'OdC deve dimostrare inoltre la conoscenza e applicazione documentata degli standard a corollario della ISO/IEC 42001.

Calcolo delle durate dei tempi di audit	Si applicano i requisiti applicabili della UNI CEI EN ISO/IEC 17021-1 integrati dalla ISO/IEC 42006 con specifico riferimento agli Annex A e B. E' responsabilità dell'OdC applicare, con approccio basato sul rischio, l'Opzione A o B delineate nell'Annex B dello standard stesso.
Durata del certificato e frequenze di audit	Si applicano i requisiti applicabili della UNI CEI EN ISO/IEC 17021-1 integrati dalla ISO/IEC 42006.

Criteri di competenza del personale addetto alla valutazione della conformità	Si applicano i requisiti applicabili della UNI CEI EN ISO/IEC 17021-1 integrati dalla ISO/IEC 42006. In relazione a quanto osservato nei processi di accreditamento, si ritiene fornire i seguenti indirizzi in merito al processo di selezione e qualifica degli auditor partendo da quanto stabilito dalla Tab. 1 della ISO/IEC 42006: 1. Formazione: la conoscenza di standard tecnici deve essere dimostrata mediante evidenza di attestati di formazione completi di programmi e durate adeguate ai contenuti della formazione stessa. In alternativa si ritengono accettabili evidenze documentate di attività pertinenti e correlate in contesti di docenza, ricerca scientifica, sviluppo in commissioni tecniche normative. Nel valutare gli attestati di frequenza di corsi, l'OdC deve dimostrare la adeguatezza dei sillabi e l'efficacia della formazione medesima con adeguati test o simulazioni di audit. E' cruciale, in tal senso, che l'OdC abbia adeguate informazioni sulle capacità degli auditor di comprendere i diversi ruoli (es. AI producer, AI provider, AI customer/user) e di valutare la loro influenza sui requisiti di certificazione. 2. Esperienza: nel valutare i requisiti di esperienza, l'OdC deve tenere in considerazione la pertinenza e l'attualità dell'esperienza operativa maturata, con riferimento a tecnologie, rischi e metodologie attuali nel campo dell'intelligenza artificiale (ad esempio: machine learning, computer vision, gestione dei dati di training e dei bias, etica e governance dei modelli, etc.). Tale esperienza deve essere stata acquisita in modo continuativo secondo i paradigmi moderni dell'AI. Il team di valutazione deve essere incaricato considerando i settori di business del cliente (rif. Tab.1 §7.1.2 ISO/IEC 42006) così come previsti dalla codifica IAF nel documento ID01 per il QMS Accreditation Scope. L'OdC deve predisporre e mantenere opportuna documentazione di riscontro dei criteri di qualifica (es.: schede di qualifica) per il personale qualificato come application reviewer, lead auditor e auditor (compresi eventuali esperti tecnici per l'area di business del cliente) e technical reviewer/decision maker.
Documenti IAF applicabili	Trovano applicazione tutti i documenti IAF relativi ai sistemi di gestione.

Banca dati ACCREDIA delle certificazioni rilasciate

Come noto, gli OdC sono tenuti a trasmettere ad ACCREDIA-DC tramite il servizio web – SIAC i dati relativi ai soggetti in possesso di certificazioni da essi rilasciate, secondo le procedure definite da ACCREDIA-DC e i relativi Regolamenti (RG01 §1.10.7).

Regole di Accreditamento

A	OdC già accreditato in accordo alla UNI CEI EN ISO/IEC 17021-1:2015	• Esame documentale di 1 g/u; • Verifica ispettiva presso la sede dell'OdC della durata di 2 g/u • 1 Verifica in accompagnamento di durata adeguata.

B	OdC non ancora accreditato secondo la UNI CEI EN ISO/IEC 17021-1:2015 ma accreditato per altri schemi di accreditamento (Livello 3)	• Esame documentale di 1 g/u; • Verifica ispettiva presso la sede dell'OdC della durata di 3 g/u; • 1 Verifica in accompagnamento di durata adeguata.
C	OdC non accreditato	• Esame documentale di 1 g/u da svolgersi, se possibile, in parte in modalità sincrona da remoto; • Verifica ispettiva presso la sede dell'OdC della durata di 4 g/u; • 1 Verifica in accompagnamento di durata adeguata.
Mantenimento dell'Accreditamento	Si ricorda che ACCREDIA-DC, in ogni caso, deve condurre annualmente una verifica presso la sede degli OdC per valutarne la conformità alla UNI CEI EN ISO/IEC 17021-1. ACCREDIA effettuerà almeno una verifica di mantenimento presso la sede dell'OdC all'anno e n. 1 verifica in accompagnamento nel ciclo di accreditamento. Tuttavia ACCREDIA si riserva comunque la possibilità di modificare le tempistiche di sorveglianza di cui sopra in funzione di un approccio basato sul rischio che tenga conto di diversi fattori quali, ad esempio, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'Organismo o altre situazioni similari, criticità legate allo schema (es. richiesta diffusa in bandi di gara ecc..), elevato numero di certificazioni emesse, ricezione di reclami/segnalazioni sull'operato del CAB e/o su aziende certificate, andamento avuto dal CAB nello schema, specifiche delibere del competente CSA, etc.	

Documentazione da presentare ad ACCREDIA-DC per l'esame documentale

Oltre a quanto elencato nella domanda di accreditamento DA-01 si richiede l'invio di:

a. Liste di riscontro, linea guida, istruzioni predisposte dall'OdC per il GVI;

b. Criteri di qualifica e curricula del personale addetto al riesame del contratto, degli auditor (compresi eventuali esperti tecnici per l'area di business del cliente) e dei technical reviewer/decision maker con le relative schede di qualifica;

c. Procedure applicabili al processo commerciale per la definizione dei tempi di audit, nonché le procedure per la gestione della pratica di certificazione.

L'occasione è gradita per porgere cordiali saluti.

Dott.ssa Mariagrazia Lanzanova

Vice-Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da: MARIAGRAZIA LANZANOVA
Data: 20/02/2026 09:16:02