

ALLEGATO REGOLAMENTO GENERALE DI CERTIFICAZIONE – ISO/IEC 42001

Il presente documento descrive le regole generali per le Organizzazioni che intendano far valutare da una parte terza qualificata la conformità del proprio Sistema di Gestione dell'Intelligenza Artificiale ai requisiti della norma ISO/IEC 42001.

La ISO/IEC 42001, pubblicata nel dicembre 2023, definisce i requisiti e fornisce una guida per la creazione, l'attuazione, l'implementazione, il mantenimento e il miglioramento continuo di un sistema di gestione dell'IA (intelligenza artificiale) nel contesto di un'organizzazione.

La conformità ai requisiti normativi può dare evidenza della responsabilità (responsibility) e della affidabilità (accountability) dell'Organizzazione, in relazione al proprio ruolo, nei confronti dei sistemi di IA.

Per le parti generali e ulteriori approfondimenti (*es. sospensione e revoca della certificazione, reclami, ricorsi e contenziosi, ecc.*) si rimanda al Regolamento di Certificazione dei sistemi di gestione RG CE.01, di cui il presente allegato rappresenta una integrazione; entrambi i documenti rivestono carattere contrattuale e sono resi disponibili sul sito internet: www.acmcert.net. Il richiedente che abbia sottoscritto un accordo contrattuale con ACM Cert Srl (di seguito ACM) si impegna a prendere visione e rispettare quanto in essi indicato.

1. SCOPO E CAMPO DI APPLICAZIONE

Le attività di valutazione della conformità dell'Organizzazione alla norma ISO/IEC 42001 sono condotte per attestare, con un adeguato livello di fiducia, che l'Organizzazione attua, mantiene e implementa in modo continuo un Sistema di Gestione dell'Intelligenza Artificiale con l'obiettivo di:

- *operare responsabilmente in relazione ai sistemi di Intelligenza Artificiale, in relazione al proprio ruolo e alla loro applicazione/uso*
- *valutare e gestire rischi e impatti dell'Intelligenza Artificiale (§4 documentazione)*
- *pianificare i controlli operativi e confrontarli con l'allegato A*
- *stabilire ed attuare processi per la gestione delle problematiche legate all'affidabilità (trustworthiness) dei sistemi di intelligenza artificiale in relazione ad aspetti di sicurezza (security), salvaguardia delle persone/incolumità (safety), correttezza (fairness), trasparenza (transparency), qualità dei dati e qualità dei sistemi di IA durante il loro ciclo di vita e processi relativi alla gestione dei dati e alla validazione dei sistemi AI*
- *verificare la soddisfazione dei requisiti di normativa cogente relativa allo sviluppo e all'uso consapevole in azienda di sistemi di IA, con particolare riferimento al Regolamento (UE) AI Act e al Regolamento (UE) 2016/679 (GDPR) e ad eventuale normativa nazionale che predisponga misure specifiche adatte al contesto italiano per mitigare i rischi e cogliere le opportunità dell'intelligenza artificiale.*
- *definire processi per la gestione di fornitori, partner e terze parti che forniscono o sviluppano sistemi di IA per l'organizzazione*

Si applica a tutte le Organizzazioni, indipendentemente da dimensioni e tipologia di attività, che fornisca o utilizzi prodotti o servizi che avvalgono di sistemi di Intelligenza Artificiale.

2. RIFERIMENTI E DEFINIZIONI

I principali riferimenti normativi per le attività che rientrano nel campo di applicazione del presente regolamento sono (riferimenti non esaustivi):

- ISO/IEC 42001 "Information Technology – Artificial intelligence – Management system"
- ISO/IEC 22989 "Information technology — Artificial intelligence — Artificial intelligence concepts and terminology"
- ISO/IEC 23053 "Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)"
- ISO/IEC 23894 "Information technology — Artificial intelligence — Guidance on risk management"
- ISO/IEC 42005 "Tecnologia dell'informazione — Intelligenza artificiale (AI) Valutazione d'impatto dei sistemi IA"
- ISO/IEC 4213 "Information technology — Artificial intelligence — Assessment of machine learning classification performance"
- ISO/IEC 5259 1-5 "Data quality for analytics and machine learning (ML)"
- ISO/IEC 24368 "Information technology — Artificial intelligence — Overview of ethical and societal concerns"
- ISO/IEC NP TR 24030: "Tecnologia dell'informazione — Intelligenza artificiale (AI) — Casi d'uso"
- ISO/IEC 5338 "Information technology — Artificial intelligence — AI system life cycle processes"
- ISO/IEC TR 24027 "Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making"
- NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0)

- UNI CEI EN ISO/IEC 17021-1 “Valutazione della conformità. Requisiti per gli organismi che forniscono audit e certificazione di sistemi di gestione”
- UNI EN ISO 19011 “Linea Guida per audit di sistemi di gestione”
- IAF MD applicabili (es. IAF MD1, MD 11, ecc)
- Regolamenti e Circolari dell’Ente di Accreditamento applicabili allo Schema

Nota: per le certificazioni sotto accreditamento Accredia i regolamenti e le Circolari Tecniche applicabili allo Schema sono reperibili sul sito www.accredia.it.

Si richiamano nel seguito i principali riferimenti alla normativa cogente per le attività che rientrano nel campo di applicazione del presente regolamento, con riferimento a categorie interessate e obblighi:

Categoria normativa	Norma	Applicabile a	Obblighi
Intelligenza Artificiale	AI Act (UE 2024/1689)	Tutti i soggetti operanti in UE	- Classificazione del rischio del sistema IA - Requisiti per i sistemi ad alto rischio (Art. 8–15) - Obblighi per fornitori, importatori, distributori, utilizzatori (Artt. 16–29) - Registrazione, sorveglianza, auditabilità, sicurezza, trasparenza
Protezione dati	GDPR (UE 2016/679)	Se i dati sono personali ma anche a dati pseudonimizzati o raccolti da fonti aperte	- Liceità del trattamento (Art. 6) - Informazione e consenso (Art. 7–13) - Limitazione della finalità e minimizzazione - DPIA (Data Protection Impact Assessment, Art. 35) se vi è rischio elevato - Trasferimenti internazionali di dati (Capo V)
Sicurezza ICT	NIS2 (UE 2022/2555)	Se operante in settori critici o fornitore di tecnologia e a chi fornisce sistemi IA come servizio cloud, software o piattaforma.	- Misure di sicurezza cibernetica proporzionate - Notifica di incidenti significativi - Governance della sicurezza dell’informazione
Sicurezza prodotto	Direttiva Macchine e Nuovo Regolamento Macchine (2023/1230), CE	Se IA è integrata in prodotti fisici	- Valutazione della conformità e marcatura CE - Obblighi specifici per “sistemi di comando” o IA che influenzano sicurezza meccanica
Responsabilità civile	Direttiva 85/374/CEE + proposta su IA	Fornitori e distributori	- Ambito: Responsabilità civile per danni causati da sistemi IA - Rilevanza: Permette di garantire tracciabilità e documentazione tecnica, in caso di contenzioso
ePrivacy / tracciamento	Direttiva 2002/58/CE + cookie laws	Se dati raccolti online	- Obbligo di consenso per l’uso di dati da siti web, tracker, log, ecc. - Compatibilità con il GDPR
Normativa nazionale	Codice Privacy, IP, settori regolati	Tutte le aziende in ambito giurisdizionale nazionale	- Codice Privacy (D. Lgs. 196/2003 aggiornato) - Leggi sul diritto d’autore per uso di contenuti raccolti da internet (es. immagini, testi) - Regolamenti settoriali: - Sanità: Regolamento UE 2017/745 (Dispositivi Medici) - Finanza: Regolamenti ESMA, EBA, PSD2, DORA - Trasporti: Normativa su sistemi autonomi

Ai fini del presente documento si applicano le seguenti definizioni:

- ✓ **Organizzazione:** Persona o gruppo di persone avente funzioni proprie con responsabilità, autorità e relazioni per conseguire i propri obiettivi. Se l’organizzazione è parte di una entità più grande, il termine “organizzazione” si riferisce soltanto a quella parte dell’entità più ampia che rientra nel campo di applicazione del sistema di gestione.

Sono compresi nel concetto chi opera singolarmente, società, gruppi, aziende, imprese, autorità, partnership, enti di beneficenza o istituzioni, o loro parti o combinazioni, costituiti in persona giuridica o meno, pubblici o privati.

- ✓ **Parte interessata:** Persona od organizzazione che può influenzare, essere influenzata, o percepire sé stessa come influenzata, da una decisione o attività.

Nota: è importante che l’organizzazione definisca il proprio ruolo rispetto al sistema di IA

- ✓ **Fornitori di IA (AI Providers):** organizzazione entità che fornisce prodotti o servizi che utilizzano uno o più sistemi di IA. I fornitori di IA comprendono i fornitori di piattaforme di IA e i fornitori di prodotti o servizi di IA.

- **Fornitore di piattaforme di IA:** organizzazione o entità che fornisce servizi che consentono ad altri soggetti di produrre servizi o prodotti di IA

- **Fornitore di prodotti o servizi di IA:** organizzazione o entità che fornisce servizi o prodotti di IA direttamente utilizzabili da un cliente o un utente di IA o da integrare in un sistema che utilizza l’IA insieme a componenti non IA.

- ✓ Produttori di IA (AI Producers, compresi gli Sviluppatori di AI,): organizzazione o un'entità che progetta, sviluppa, testa e distribuisce prodotti o servizi che utilizzano uno o più sistemi di IA.
 - Sviluppatore di IA (AI Developers): organizzazione o entità che si occupa dello sviluppo di servizi e prodotti di IA.

A titolo di esempio: Model designer: entità che riceve i dati e le specifiche di un problema e crea un modello di IA; Model Implementer: entità che riceve un modello di IA e specifica quale calcolo eseguire (l'implementazione da utilizzare e su quali risorse di calcolo, ad esempio CPU, GPU, ASIC, FPGA); Verificatore di calcolo: entità che verifica che un calcolo venga eseguito come progettato; Verificatore del modello: entità che verifica che il modello di intelligenza artificiale funzioni come progettato.
- ✓ Clienti dell'IA (Customers, tutti gli utilizzatori): organizzazione o entità che utilizza un prodotto o un servizio di IA direttamente o tramite la sua fornitura agli utenti dell'IA.
 - Utente di IA: organizzazione o entità che utilizza prodotti o servizi di IA.
- ✓ Partner di IA: organizzazione o entità che fornisce servizi nel contesto dell'AI. Possono eseguire lo sviluppo tecnico di prodotti o servizi di IA, condurre test e convalide di prodotti e servizi di IA, verificare l'utilizzo dell'IA, valutare prodotti o servizi di IA ed eseguire altri compiti.

A titolo di esempio : Integratore di sistemi di AI organizzazione o entità che si occupa dell'integrazione di componenti di IA in sistemi più ampi, potenzialmente comprendenti anche componenti non di IA; Fornitore di dati: organizzazione o entità che si occupa di fornire dati utilizzati da prodotti o servizi di IA; auditor di AI: organizzazione o ente che si occupa dell'audit di organizzazioni che producono, forniscono o utilizzano sistemi di IA, per valutare la conformità a standard, politiche o requisiti legali; valutatore di AI: organizzazione o entità che valuta le prestazioni di uno o più sistemi di IA.
- ✓ Soggetto di IA: organizzazione o entità che viene influenzata dai sistemi di IA

A titolo di esempio:

Soggetto dei dati di addestramento, quando i dati relativi a un'organizzazione o a un essere umano vengono utilizzati per l'addestramento di un sistema di IA, possono esserci implicazioni per la sicurezza e la privacy, in particolare quando il soggetto è un individuo umano.

Altre organizzazioni o entità interessate da un sistema, servizio o prodotto di IA possono essere, ad esempio, individui o comunità. Ad esempio, i consumatori che interagiscono con un social network che fornisce raccomandazioni basate sull'IA, i conducenti di veicoli con automazione basata sull'IA.
- ✓ Autorità rilevanti: organizzazioni o entità che possono avere un impatto su un sistema, un servizio o un prodotto di IA es. Responsabili di politiche a livello internazionale/nazionale/industriale, o enti regolatori che hanno il compito di far rispettare i requisiti legislativi
- ✓ Dichiarazione di applicabilità (Statement of applicability, SoA): Documentazione di tutti i controlli necessari e motivazione di eventuali esclusioni/inclusioni -riferimento Appendice A della norma

Nota: L'organizzazione può non richiedere tutti i controlli elencati nell'Appendice A o integrare con controlli aggiuntivi definiti in autonomia l'elenco dell'Appendice A
- ✓ Controllo: Misura che mantiene e/o modifica il rischio. Comprende qualsiasi processo, politica, dispositivo, pratica o altre condizioni e/o azioni che mantengono e/o modificano il rischio

In base al Regolamento Europeo AI Act 2024/1689
- ✓ "fornitore": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito;
- ✓ "deployer": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale;
- ✓ distributore: una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione
- ✓ «importatore»: una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo;
- ✓ «finalità prevista»: l'uso di un sistema di IA previsto dal fornitore, compresi il contesto e le condizioni d'uso specifici, come dettagliati nelle informazioni comunicate dal fornitore nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica;
- ✓ «istruzioni per l'uso»: le informazioni comunicate dal fornitore per informare il deployer in particolare della finalità prevista e dell'uso corretto di un sistema di IA;

- ✓ Valutazione dell'impatto del sistema di AI: Processo formale e documentato attraverso il quale si identificano, valutano e affrontano gli impatti sugli individui/gruppi e sulle società da parte di un'organizzazione che sviluppa, fornisce o utilizza prodotti o servizi che si avvalgono dell'intelligenza artificiale
- ✓ Ciclo di vita: evoluzione di un sistema, di un prodotto, di un servizio, di un progetto o di un'altra entità creata dall'uomo, dalla sua concezione fino alla sua dismissione

3. DOMANDA DI CERTIFICAZIONE

Per intraprendere l'iter di certificazione per la ISO/IEC 42001 l'Organizzazione presenta ad ACM via e-mail la Domanda di certificazione, compilando e firmando il questionario informativo e allegando Visura Camerale ordinaria aggiornata (con data non antecedente i 6 mesi).

Sono richieste una serie di dati/informazioni iniziali per valutare il grado di complessità dell'Organizzazione e dei suoi processi/servizi e consentire la formulazione dell'offerta:

- le generalità dell'Organizzazione come Ragione Sociale, indirizzi della sede legale, sede operativa principale, altri siti, nominativi e riferimenti di contatto;
- il campo di applicazione della ISO/IEC 42001 (scopo di certificazione);
- sito/i produttivo/i oggetto di verifica, con indicazione dello scopo/attività, se diverso dal sito principale;
- nominativi di eventuali consulenti/società di consulenza che hanno progettato e realizzato il sistema di gestione dell'AI;
- il motivo della richiesta (certificazione iniziale, rinnovo, estensione di scopo, transfer)
- data in cui l'Organizzazione sarà pronta per l'audit;
- numero addetti in ogni sito coinvolti nel Sistema di Gestione dell'Intelligenza Artificiale e che devono lavorare in conformità ai requisiti del Sistema di Gestione
- informazioni aggiuntive sul personale, turni e orari di lavoro
- processi affidati all'esterno;
- tipologia di organizzazione (multisito, appartenente ad un gruppo o consorzio)
- possesso di altre certificazioni di sistemi di gestione
- ruolo dell'organizzazione e complessità sistemi AI che richiede la certificazione rispetto all'AI (produttore, utilizzatore,)
- tipologia dei sistemi di gestione, applicazione e uso
- categoria di rischio del sistema AI
- presenza di sistemi di AI ad alto rischio/sensibili nell'ambito dello scopo di certificazione
- numero di controlli previsti dalla dichiarazione di applicabilità (previsti da ISO/IEC 42001, in numero inferiore, controlli aggiuntivi)
- altre informazioni di dettaglio utili ai fini della formulazione dell'offerta

Al momento della presentazione della richiesta di certificazione l'Organizzazione deve dimostrare di avere un Sistema di Gestione per l'Intelligenza Artificiale attivo da almeno tre (3) mesi, conforme ai requisiti della ISO/IEC 42001 (si veda anche quanto indicato al §5. *Documentazione richiesta*).

Qualora il sistema di Gestione dell'IA comprenda documentazione/informazioni considerate come riservate o sensibili che non possono essere rese disponibili ai fini della certificazione, ACM si riserva di valutare se sussistono le condizioni per proseguire l'iter di certificazione.

La completezza e veridicità dei dati forniti è requisito essenziale per la corretta formulazione dell'offerta. ACM si riserva di richiedere integrazioni delle informazioni fornite qualora non siano sufficienti per la redazione dell'offerta e relativa quotazione economica. ACM riesamina gli elementi presenti nella domanda di certificazione per valutare il possesso dei requisiti di accreditamento e di competenza richiesta e redige l'offerta indicando la descrizione del servizio, le sedi da certificare, l'impegno in termini di giornate/uomo per le attività di audit previste dal triennio, la quotazione economica.

L'accettazione dell'offerta implica l'impegno dell'Organizzazione a uniformarsi ai requisiti indicati nei Regolamenti di ACM, Regolamento Generale di Certificazione, il presente allegato integrativo. L'Organizzazione si impegna inoltre a mantenere conformi i propri processi, prodotti e servizi a tutti i requisiti normativi e cogenti applicabili, a cooperare con il personale ispettivo consentendo l'accesso alle aree di valutazione, alla documentazione e alle registrazioni, e a comunicare ad ACM le modifiche organizzative e di processo che possono avere influenza sulle condizioni del servizio.

È facoltà dell'Organizzazione, previo accordo contrattuale tra le parti, richiedere un Pre-Audit, al fine di verificare lo stato di implementazione del Sistema di Gestione dell'Intelligenza Artificiale dell'Organizzazione prima dell'Audit di Certificazione in relazione ai requisiti normativi e identificare quelle situazioni /carenze che potrebbero influenzarne negativamente l'esito.

Gli accordi contrattuali stipulati hanno una validità triennale e prevedono il pagamento degli importi per le attività di audit descritte nell'offerta economica. Il mancato adempimento comporta provvedimenti di sospensione o revoca, secondo quanto indicato nei paragrafi pertinenti del presente Allegato/ Regolamento di Certificazione dei sistemi di gestione RG CE.01.

4. DOCUMENTAZIONE RICHIESTA

A seguito della formalizzazione degli accordi contrattuali l'Organizzazione deve rendere disponibile al personale di verifica designato da ACM, quando richiesto, ogni informazione, documentazione e registrazione a supporto della verifica.

A titolo esemplificativo e non esaustivo:

- Manuale/Procedure, registrazioni, modulistica ed altra documentazione utile a documentare il Sistema di Gestione dell'Intelligenza Artificiale dell'Organizzazione e soddisfare i requisiti della ISO/IEC 42001 e a descrivere la modalità di gestione di processi/attività/servizi svolti
- Organigramma nominale, comprensivo funzioni responsabili e persone specifiche in funzione dell'applicazione/uso del sistema AI per le attività previste dalla norma o altro documento in cui sia descritta la struttura organizzativa e le responsabilità assegnate;
- Campo di applicazione dell'AIMS
- Requisiti legali, regolamentari e contrattuali
- Analisi del contesto, compresi requisiti legali applicabili e usi vietati dell'AI, tipi di sistemi AI, modelli e dati
- Inventario delle risorse
- Politiche relative a sviluppo e uso sistemi AI, risorse dei dati, risorse dei tools, sistemi e computer, segnalazione di anomalie
- Obiettivi di Sistemi di Intelligenza Artificiale, sviluppo responsabile AI, indicatori di monitoraggio e valutazione delle prestazioni
- Processo di valutazione e trattamento del rischio
- Dichiarazione di applicabilità SoA (Allegato A)
- Pianificazione e controlli operativi (*Appendice A della norma*)
- Valutazione dell'Impatto del sistema AI sia sulle persone, gruppi di individui, che sulla società
- Valutazione del rischio AI e analisi delle tipologie dei sistemi in quale ambito rientrano (alto rischio, basso, proibiti, etc.), piano di trattamento dei rischi, riesame periodico e risultati:

Ad esempio:

- *organizzazione;*
- *processi e procedure;*
- *routine di gestione;*
- *personale;*
- *ambiente fisico;*
- *dati;*
- *configurazione del sistema di IA;*
- *ambiente di diffusione;*
- *hardware, software, risorse e servizi di rete;*
- *dipendenza da soggetti esterni.*
- Complessità ambientale: Sono considerati scenari dinamici, variabili operative e incertezza nei risultati dei sistemi AI.
- Scarsa trasparenza/spiegabilità: L'organizzazione ha previsto misure per rendere comprensibili gli output AI alle parti interessate.
- Livello di automazione impattante: Esistono controlli o supervisione umana per mitigare effetti su sicurezza, equità, protezione degli utenti.
- Qualità e raccolta dati: Presenza di controlli sulla qualità, integrità e rappresentatività dei dati usati nei sistemi AI.
- Errori infrastrutturali: Identificazione dei rischi dovuti a componenti hardware/software non affidabili, con relative contromisure.
- Debolezze nel ciclo di vita AI: Procedure per la gestione completa del ciclo di vita AI: progettazione, test, rilascio, manutenzione, dismissione, validazione, riuso
- Tecnologie immature: L'organizzazione valuta maturità e affidabilità delle tecnologie AI prima dell'adozione.
- Rischi derivanti dal ML: Il comportamento del ML dipende sia dagli algoritmi che dai dati che dall'addestramento
- Problemi del Sistema: Errori nell'HW e nel SW, trasferimento di modelli ML, errori da remoto (rete, banda)
- Uso previsto (intended use), evidenziando le finalità e le modalità operative per cui esso è progettato.
- Usi ragionevolmente prevedibili (reasonable foreseeable misuses), inclusi gli scenari in cui il sistema AI potrebbe essere impiegato in maniera non conforme alle intenzioni originarie, analizzando i potenziali rischi e le relative implicazioni.
- Controlli su robustezza, accuratezza e qualità dei dati (trustworthiness) e misure implementate, illustrando le metodologie adottate per monitoraggio, aggiornamento e verifica dei processi correlati.
- Accessibilità e trasparenza di informazioni e documentazioni, loro organizzazione e accessibilità.

- Procedura di risposta agli incidenti
- Procedura per documentare gli obblighi di segnalazione delle informazioni sul sistema di IA alle parti interessate
- Evidenze della comunicazione alle parti interessate interne ed esterne
- Tenuta sotto controllo della documentazione e delle registrazioni
- Soddisfazione dei requisiti minimi che devono essere inclusi nella documentazione tecnica dei sistemi di intelligenza artificiale (in particolare di quelli ad alto rischio), richiesti dall'Allegato IV del Regolamento (UE) 2024/1689 (AI Act).
- Riesame della Direzione
- Pianificazione ed esecuzione di audit interni
- Piano azioni correttive a fronte dei rilievi evidenziati da ACM in fase di certificazione/mantenimento e stato di avanzamento delle azioni pianificate
- Documentazione relativa alle competenze (istruzione, formazione, esperienza e qualifiche) del personale coinvolto nel Sistema di gestione dell'AI e che influenza le prestazioni di AI;
- Documentazione delle risorse (dati, tool, persone, componenti, sistemi, finanziarie, etc.)
- Documentazione tecnica del sistema AI
- Documentazione relativa all'uso del sistema AI
- Registrazioni delle verifiche e delle validazioni
- Registri delle attività dei sistemi AI
- Risultati del monitoraggio e della misurazione e monitoraggio continuo
- Documentazione relativa al monitoraggio dei log

E' facoltà del personale ispettivo richiedere altra documentazione integrativa che si rendesse necessaria per condurre un'analisi documentale efficace, prima della valutazione in campo.

Si richiede la compilazione del modulo Self Assessment, con l'elenco delle informazioni documentate obbligatorie, da rendere disponibile, per la verifica da parte del Gruppo di Audit, in fase di Stage 1; il modulo verrà archiviato come registrazione di audit.

5. PIANIFICAZIONE ED ATTIVITA' DI CERTIFICAZIONE

Risolti gli aspetti contrattuali l'iter prevede la selezione del Gruppo di Audit (GA) per l'assegnazione dell'incarico e la pianificazione delle date delle attività di audit. L'Organizzazione ha la facoltà di recusare per motivi fondati, non di natura tecnica, i nominativi del personale auditor. In tal caso ACM provvederà ad una nuova assegnazione; in assenza di riscontri i nominativi dei valutatori si intendono tacitamente confermati, come indicato negli accordi contrattuali.

Il Lead Auditor con congruo anticipo rispetto alla data di audit predispone il piano di audit che comprende il programma temporale di siti/sedi/processi/attività/turni da verificare e le funzioni dell'Organizzazione coinvolte. Il Piano di audit potrà essere variato, anche nel corso dell'audit, in conseguenza di esigenze dell'Organizzazione, delle necessità di audit e del Gruppo di Audit.

Lo svolgimento dell'audit si articola in:

- **Riunione iniziale** : In sede di riunione iniziale in presenza della Direzione dell'Organizzazione e, ove appropriato, dei responsabili delle funzioni e dei processi da sottoporre a verifica viene presentato il GA, descritto lo scopo e le modalità dell'audit, stabiliti i canali di comunicazione, confermati il campo di applicazione della certificazione, il n° di addetti, il piano d'audit, la disponibilità delle risorse necessarie al gruppo d'audit (umane ed infrastrutturali), gli aspetti relativi alla sicurezza e riservatezza. L'Organizzazione può porre domande o chiedere informazioni al GA. Vengono anche individuate le persone appartenenti all'Organizzazione che fungeranno da guide per ciascun componente del gruppo di audit, al fine di facilitarne il compito, che, tuttavia, non devono influenzare o interferire con il processo di audit.

Il Lead Auditor segnala ad ACM eventuali scostamenti rilevati rispetto ai dati in precedenza comunicati dall'Organizzazione (in relazione a scopo, sedi e numero addetti); ACM si riserva di sospendere e posticipare l'audit, rivedere ed eventualmente modificare i documenti contrattuali.

- **Condizione dell'audit**: Il Gruppo di Audit procede alla valutazione dell'effettiva applicazione e conformità del Sistema di Gestione dell'Intelligenza artificiale e della conformità legislativa riferibile al campo di applicazione della certificazione.

Le informazioni relative agli obiettivi, al campo di applicazione ed ai criteri di audit, vengono raccolte attraverso un campionamento, che può prevedere l'effettuazione di interviste, osservazione di processi e attività, il riesame della documentazione e delle registrazioni. In caso di GA costituito da due o più auditor, gli auditor lavoreranno, per quanto possibile, separatamente al fine di massimizzare l'utilizzo dei tempi di verifica. Se necessario il Gruppo di Audit può essere affiancato da un Esperto Tecnico.

Nel corso dell'audit, il GA valuta periodicamente lo stato di avanzamento dell'audit stesso e scambia le conseguenti informazioni.

Le evidenze raccolte nel corso d'audit per dimostrare la conformità ai requisiti e/o dettagliare i rilievi emersi, vengono registrate nei documenti di audit al fine di consentire una decisione informata circa la certificazione, il relativo mantenimento o il rinnovo. I rilievi riscontrati vengono discussi con l'Organizzazione per garantire che l'evidenza sia accurata e che essi siano compresi.

Al termine dell'attività valutazione, il GA si riunisce per riesaminare le risultanze dell'audit a fronte dei relativi obiettivi e dei criteri di audit, classificare i rilievi, concordare le conclusioni dell'audit ed ogni azione conseguente necessaria.

- **Riunione finale:** Nella riunione di chiusura alla presenza del Gruppo d'Audit e della Direzione dell'Organizzazione e, ove appropriato, dei responsabili delle funzioni o dei processi sottoposti ad audit – il LA illustra la metodologia con cui è stato condotto l'audit e le relative conclusioni, comprese la raccomandazione riguardo alla certificazione e i possibili rilievi (vedere § Classificazione dei rilievi).

Al termine dell'audit viene redatto un rapporto di valutazione, denominato Rapporto d'Audit, di proprietà di ACM, che riporta una sintesi dell'attività svolta e le eventuali non conformità ed osservazioni riscontrate o i commenti per il miglioramento.

Il ciclo di certificazione ha durata triennale e prevede:

✓ **Audit di certificazione iniziale**, articolato in Stage 1 e Stage 2

La fase 1 prevede una valutazione documentale allo scopo di verificare la correttezza e completezza dei dati forniti, compreso lo scopo di certificazione, ed avere un quadro complessivo delle attività e dei siti/sedi da sottoporre a certificazione e della documentazione del Sistema di Gestione dell'Intelligenza Artificiale, al fine di determinare il grado di preparazione dell'Organizzazione per lo Stage 2.

Come riportato al precedente §.4 la valutazione documentale comprende la verifica della completezza, dell'aggiornamento e della chiarezza delle procedure relative ad esempio a:

- Uso previsto del sistema AI (Intended Use): verifica che il documento descriva in modo esaustivo l'uso previsto del sistema AI, evidenziando le finalità, le modalità operative e le eventuali limitazioni d'uso.
- Usi ragionevolmente prevedibili (Reasonable Foreseeable Misuses) e degli eventuali scenari di uso improprio: verifica dell'analisi dei rischi legati agli usi non intenzionali o impropri, con particolare attenzione all'identificazione delle possibili criticità e alle contromisure adottate per mitigare tali rischi.
- Robustezza, accuratezza e qualità dei dati (Trustworthiness dei Dati): esame della documentazione che attesta i controlli implementati per garantire la robustezza, l'accuratezza e la qualità dei dati. Questo include:
 - La presenza di meccanismi di monitoraggio continuo e validazione dei dati.
 - L'utilizzo di indicatori di performance e procedure di audit trail per rilevare eventuali anomalie o errori.
 - La documentazione relativa ad eventuali incidenti o problematiche riscontrate e le azioni correttive adottate.
- Verifica che l'elaborazione e l'aggiornamento continuo della valutazione del rischio AI siano documentati e integrati nel sistema di gestione aziendale

Al termine della fase 1 viene emesso un rapporto di audit riportante le risultanze emerse e le relative conclusioni per il proseguimento o meno alla fase 2. Il modulo Self Assessment, approfondito e discusso in sede Stage 1 con il Lead Auditor viene conservato come registrazione della fase 1.

La decisione se procedere o meno alla fase 2 è in capo a personale qualificato che non ha partecipato all'audit che ha il compito di riesaminare in modo indipendente il rapporto di Stage 1 e deliberare in merito al proseguimento dell'iter di certificazione.

L'intervallo di tempo tra l'audit di Stage 1 e l'audit di Stage 2 viene concordato in modo da consentire all'Organizzazione la possibilità di risolvere eventuali aree di debolezza identificate nell'audit di Fase 1, rispettando in ogni caso il termine massimo di 6 mesi dall'Audit di Stage 1. Superato tale termine è necessario precedere nuovamente con un nuovo iter, ripartendo dallo Stage 1.

Qualora emergessero situazioni che differiscono dalle informazioni trasmesse dall'Organizzazione nella fase di richiesta d'offerta e che richiedono un ampliamento delle attività previste, ACM si riserva di rivedere gli accordi contrattuali e i corrispettivi dovuti.

Lo Stage 2 è eseguito solo a seguito di esito positivo delle Stage 1 e ha lo scopo di valutare il grado di adeguatezza ed applicazione Sistema di Gestione dell'Intelligenza Artificiale dell'Organizzazione, previa verifica della presa in carico e risoluzione dei rilievi emersi durante lo Stage 1.

La verifica viene svolta presso il sito dell'Organizzazione nell'ambito del campo di applicazione definito per il Sistema di Gestione dell'Intelligenza Artificiale.

Al Team ispettivo deve essere garantito l'accesso alle aree, alla documentazione e alle registrazioni di interesse. La raccolta delle evidenze prevede l'esame della documentazione e delle registrazioni, le interviste con il personale, l'osservazione diretta delle attività e degli ambienti, la ecc.

Gli elementi da valutare comprendono (*si veda anche quanto indicato al §4. Documentazione richiesta*):

- il contesto, perimetro e scopo del Sistema di Gestione dell'Intelligenza Artificiale, parti interessate/loro aspettative
- la struttura organizzativa
- analisi dei rischi e valutazione degli impatti dell'AI
 - Revisione della metodologia e degli strumenti utilizzati: la documentazione che descrive il metodo adottato per l'identificazione, valutazione e gestione dei rischi connessi all'uso del sistema AI e la metodologia che include criteri

chiari per la valutazione del rischio in relazione all'uso previsto, agli usi ragionevolmente prevedibili e alla "trustworthiness" (robustezza, accuratezza, qualità dei dati).

- Esame dell'identificazione e valutazione dei rischi: se l'azienda ha svolto un'analisi approfondita delle potenziali minacce e vulnerabilità specifiche del sistema AI, compresi scenari di uso improprio (misuses), valutando i livelli di impatto e la probabilità che tali rischi possano materializzarsi, con evidenza di assegnazione delle priorità per la mitigazione.
- Verifica dei documenti e delle registrazioni: i report e il registro dei rischi devono contenere valutazioni aggiornate, azioni correttive e i relativi piani di mitigazione. Si verificherà l'esistenza di evidenze concrete (es. log, audit trail, report di monitoraggio) che attestino il monitoraggio continuo dei rischi identificati e delle misure adottate.
- Aggiornamenti e integrazione nel sistema di gestione: verifica del processo di revisione periodica dell'analisi del rischio, per rispondere a eventuali cambiamenti normativi, tecnologici o nuove criticità. Le revisioni devono essere documentate e deve esserci una procedura di aggiornamento che includa le lezioni apprese da incidenti o anomalie.
- Interviste e osservazioni pratiche: per verificare la comprensione e la corretta applicazione della metodologia adottata, possibilmente anche attraverso simulazioni o test pratici che dimostrino l'efficacia delle misure di controllo e la capacità del sistema di rilevare e rispondere a situazioni di rischio.
- politica e obiettivi
- risorse umane e formazione
- tenuta sotto controllo dei documenti e conformità ai documenti legislativi di riferimento. La documentazione è essenziale per dimostrare la conformità del sistema ai requisiti dell'AI Act e deve essere mantenuta aggiornata e disponibile per le autorità competenti. I contenuti principali richiesti nell'Allegato IV includono:
 1. Descrizione generale del sistema IA: funzionalità previste, scopo previsto e contesto di utilizzo.
 2. Architettura del sistema: componenti hardware e software, nonché le interfacce con altri sistemi.
 3. Dati utilizzati: origine, natura e modalità di raccolta dei dati per addestramento, validazione e test del sistema.
 4. Processi di sviluppo: metodologie di addestramento del sistema, inclusi algoritmi e tecniche di ML impiegate.
 5. Valutazione dei rischi: identificazione e analisi dei rischi associati all'utilizzo del sistema e misure adottate per mitigarli.
 6. Misure di controllo e monitoraggio: procedure per garantire qualità, robustezza e sicurezza lungo tutto il ciclo di vita.
- pianificazione ed esecuzione degli audit interni e del riesame di direzione
- altre registrazioni richieste per fornire evidenza del rispetto dei requisiti della ISO/IEC 42001, compresi i controlli Allegato A
- l'uso del Marchio ACM e dell'Ente di Accreditamento (per sorveglianze e rinnovi)

Il personale ispettivo valuta le risultanze della verifica e redige il Rapporto di Audit che riporta le risultanze della verifica in cui sono formalizzati gli eventuali rilievi evidenziati, classificati secondo i criteri indicati al §7 e la proposta/raccomandazione sull'esito della verifica per il Comitato di Certificazione. Il Rapporto di Audit viene presentato all'Organizzazione nel corso della riunione finale con la Direzione e sottoposto al riesame da parte del Comitato di Certificazione di ACM per la decisione finale in merito alla Certificazione.

- ✓ **Audit di sorveglianza:** si tratta di verifiche periodiche di mantenimento, con cadenza annuale, il cui scopo è verificare nel tempo l'applicazione conforme della ISO/IEC 42001 e la risoluzione di rilievi emersi nel corso di audit precedenti.

In particolare:

- 1° Audit di sorveglianza, successivo alla certificazione iniziale o Rinnovo, entro 12 mesi dalla data decisione sulla certificazione;
- 2° Audit di Sorveglianza entro 24 mesi dalla data decisione della certificazione.

L'Organizzazione si impegna a comunicare le variazioni/aggiornamenti dei dati con riferimento a:

- elenco sedi/siti operativi
- variazioni n° addetti, turni di lavoro, fatturato
- modifiche di scopo
- modifiche di figure chiave nell'Organizzazione
- altre modifiche significative dell'organizzazione e/o del Sistema di Gestione dell'Intelligenza Artificiale tali da influenzare negativamente la certificazione rilasciata

- ✓ **Audit di rinnovo,** ha lo scopo di confermare la continua conformità ed efficacia del Sistema di Gestione dell'Intelligenza Artificiale. È richiesta la presentazione di una nuova domanda di certificazione e revisione degli accordi contrattuali, in previsione di un ulteriore triennio di certificazione.

L'audit di rinnovo deve essere effettuato entro la data di scadenza del certificato e con anticipo sufficiente in modo da consentire il completamento della verifica di attuazione/ efficacia delle azioni correttive implementate a fronte di NC e garantire la continuità del certificato. Il rinnovo può essere approvato solo a completamento positivo di tale attività (prima della data di scadenza del certificato).

L'Audit di Rinnovo può essere eseguito anche oltre la data di scadenza della certificazione, entro 6 mesi massimo. In tal caso durante tale intervallo temporale la validità del certificato risulta scaduta: sul certificato rimesso verrà indicato chiaramente il periodo in cui la certificazione è stata inattiva.

Qualora non sia possibile eseguire del tutto l'Audit di Rinnovo o verificare trattamenti/ Azioni correttive per ogni NC entro i tempi previsti, non sarà possibile rinnovare la certificazione né sarà possibile prorogare la validità del certificato.

L'Organizzazione che desideri nuovamente ottenere la Certificazione dovrà riattivare l'iter effettuando un nuovo Audit Iniziale.

Nel corso del ciclo di certificazione possono essere svolti **audit speciali**, non previsti dal programma di sorveglianza, quali:

- audit di estensione del campo di applicazione del certificato;
- audit con breve preavviso;
- audit ravvicinati.

Si rimanda per ulteriori informazioni e approfondimenti al Regolamento Generale di Certificazione RG CE.01

6. CLASSIFICAZIONE DEI RILIEVI

I rilievi sono classificati secondo il criterio: Non Conformità, Osservazione, Commento.

Eventuali rilievi che dovessero emergere al termine dell'Audit devono essere presi in carico dall'Organizzazione per l'analisi della causa radice applicando un metodologia strutturata, definizione di trattamento, azioni correttive e relative tempistiche.

Il piano di gestione deve essere comunicato ad ACM, per l'approvazione da parte del Lead Auditor, prima di proseguire con le successive fasi del processo di Certificazione utilizzando la modulistica di ACM.

Una volta concluse con esito positivo le attività di verifica da parte del Gruppo d'Audit e risolte eventuali NC, il Rapporto d'Audit ed eventuale documentazione integrativa, viene trasmesso al Comitato di Certificazione, per il proseguimento dell'iter certificativo.

Rilievo	Descrizione	Azioni richieste
Non Conformità	una Non-Conformità che influenza la capacità del Sistema di Gestione IA di raggiungere i risultati attesi e che segnala la presenza di una deviazione/mancanza che: a) mette a rischio l'affidabilità dei risultati/prestazioni/servizi prodotti dall'organizzazione; b) induce al dubbio significativo circa l'efficacia dei processi di controllo in atto, o che i prodotti o servizi non soddisfino i requisiti specifici; c) inficia la capacità del sistema di gestione IA di mantenere il livello qualitativo stabilito delle prestazioni o indica un blocco nel funzionamento del SGIA; d) minaccia la credibilità della procedura di certificazione o dell'integrità/onestà di ACM; e) deriva dal reiterato mancato efficace superamento di un'Osservazione precedentemente formalizzata all'Organizzazione o dalla presenza di un certo numero di non conformità minori associato al medesimo requisito o aspetto (potrebbero dar prova di una criticità sistemica e dunque costituire una non conformità maggiore) f) evidenzia il mancato rispetto di requisiti cogenti applicabili.	È sempre richiesta l'apertura di un trattamento e azione correttiva, con l'evidenza della verifica della chiusura prima della delibera del Comitato di Certificazione. Tempi: - per notificare la proposta di gestione ad ACM: 15 gg dalla data dell'audit - per attuazione e chiusura della proposta: 90 gg dalla data dell'audit Le NC sono ostative al proseguimento dell'iter certificativo. Il Comitato di Certificazione può emettere una delibera positiva, solo a seguito della verifica della positiva dell'attuazione dell'Azione Correttiva, previa valutazione documentale o verifica supplementare in campo, a seconda dei casi, al fine di assicurare che le azioni correttive siano state effettivamente attuate
Osservazione	Rilievo il cui risultato non influenza la capacità del sistema di gestione IA di conseguire i risultati attesi e non inficia o non è suscettibile d'inficiare direttamente o immediatamente la qualità delle prestazioni e dei risultati dell'organizzazione. Un'osservazione non chiusa alla verifica periodica successiva viene riclassificata come Non Conformità.	Notifica della proposta di trattamento/azione correttiva entro 15 gg dalla data di audit Apertura di un trattamento e azione correttiva entro un definito periodo temporale Verifica di attuazione dell'azione correttiva nel corso della verifica successiva oppure valutazione su base documentale.
Commento	Un rilievo viene classificato come commento quando non è conseguente al riscontro di una situazione oggettiva di mancato soddisfacimento di un requisito, ma è finalizzato a prevenire che tale situazione si verifichi (in quanto potenzialmente realizzabile) e/o a fornire indicazioni per il miglioramento dei documenti e/o delle modalità operative dell'organizzazione.	Non è richiesto un immediato e formale riscontro a fronte di un commento, tuttavia il grado di recepimento delle indicazioni fornite verrà verificato in occasione della prima verifica utile.

7. RILASCIO DEL CERTIFICATO

Il rilascio all'Organizzazione del Certificato di conformità è vincolato al parere positivo espresso dal Comitato di Certificazione di ACM che riesamina in modo indipendente la documentazione di audit e le relative risultanze e prende la decisione finale.

È compito del Comitato di Certificazione decidere se:

- confermare senza riserve la proposta del gruppo di audit;
- richiedere integrazioni e chiarimenti al gruppo di audit in merito alle evidenze oggettive e a supporto del parere espresso;
- richiedere una verifica supplementare presso l'Organizzazione, qualora le evidenze non siano considerate sufficienti.

Il Certificato riporta le seguenti informazioni:

- l'identificazione univoca del certificato
- il nome e l'indirizzo di ACM
- il nome e l'indirizzo della sede legale dell'Organizzazione e di tutti i siti compresi nel campo di applicazione ISO/IEC 42001
- il campo di applicazione della certificazione
- il riferimento alla norma di riferimento ISO/IEC 42001
- il riferimento alla dichiarazione di applicabilità, SoA
- la data di prima emissione, di emissione corrente e di scadenza del certificato
- il marchio di riferimento di ACM in abbinamento al marchio dell'Ente di accreditamento Accredia

La certificazione ha durata triennale dalla data di emissione e mantiene la propria validità a seguito dell'esito positivo degli audit di sorveglianza periodica e di rinnovo.

Durante il periodo di validità del Certificato è possibile modificare il campo di applicazione della certificazione, dandone comunicazione scritta ad ACM che valuterà sulla base delle informazioni ricevute se sia necessaria l'esecuzione di audit supplementari e la rivalutazione delle condizioni economiche.

Eventuali periodi di non validità del certificato verranno esplicitati sul certificato (*periodo di non validità del certificato dal /al*).

Si chiarisce che il rilascio del certificato è subordinato al pagamento della relativa fattura. In ogni caso il pagamento dei corrispettivi per l'attività svolta è dovuto, indipendentemente dall'esito della verifica.

8. DIRITTI E DOVERI DELL'ORGANIZZAZIONE

L'Organizzazione che abbia ottenuto la certificazione del Sistema di Gestione dell'Intelligenza Artificiale può farne riferimento nella documentazione pubblicitaria in relazione alle attività, siti e scopo indicati nel certificato stesso, solamente per indicare che il proprio Sistema di Gestione dell'AI è conforme alla norma di riferimento e nel pieno rispetto delle regole di utilizzo del marchio ACM e dell'Ente di accreditamento.

Non è consentito l'utilizzo del Certificato o delle informazioni in esso contenute in modo da trarre in inganno i destinatari d'uso dell'informazione, facendo intendere che un prodotto o servizio è approvato da ACM, o tale da danneggiare l'immagine e la reputazione di ACM, o qualora siano in atto altre inadempienze (es. provvedimenti di revoca, mancato pagamento dei corrispettivi).

L'Organizzazione si impegna a garantire la veridicità delle informazioni e dei documenti messi a disposizione del personale ispettivo di ACM, a cooperare con il Gruppo di Audit consentendo l'accesso alle aree di valutazione, anche di eventuali osservatori e/o valutatori dell'Organismo di Accreditamento, alla documentazione e alle registrazioni pertinenti, compresi i rapporti degli audit interni. Si assume inoltre piena responsabilità delle proprie attività, delle scelte tecniche, del rispetto dei requisiti di legge applicabili e degli obblighi contrattuali verso i propri clienti, anche in riferimento a garanzie di sicurezza, prestazioni e/o difetti dei prodotti immessi sul mercato.

L'Organizzazione si impegna ad identificare e tenere sotto controllo i requisiti richiesti, compresi quelli cogenti, ad attuare, mantenere ed implementare un efficace Sistema di Gestione dell'Intelligenza Artificiale. Si impegna inoltre a mantenere una registrazione di tutti i reclami ricevuti dalle parti interessate rispetto ai temi che rientrano nello scopo del certificato e fornire evidenza delle azioni correttive intraprese, a formulare le proposte di azioni correttive per risolvere le carenze evidenziate e a segnalare tempestivamente ad ACM eventuali notifiche da parte delle Autorità competenti in merito a violazioni etiche/diritti umani o violazione della legislazione applicabile.

Si impegna inoltre a cessare qualsiasi riferimento alla certificazione del Sistema di Gestione dell'Intelligenza Artificiale in caso di revoca della stessa, cessando l'utilizzo del materiale pubblicitario che abbia riferimenti ad essa.

È dovere dell'Organizzazione comunicare ad ACM le modifiche anagrafiche, di carattere organizzativo o tecnico, intervenute successivamente a quanto indicato in fase di definizione degli accordi contrattuali con riferimento a:

- campo di applicazione del sistema di gestione dell'Intelligenza Artificiale
- sedi/siti/unità operative e processi produttivi
- numero di addetti coinvolti
- cessione a terzi di fasi di produzione (core) o di un ramo dell'Organizzazione titolare dell'attestato, fusione, scissione, ecc.
- modifiche sostanziali dei processi produttivi/servizi oggetto della certificazione o nelle figure chiave coinvolte nel Sistema di Gestione dell'Intelligenza Artificiale
- altri elementi che potrebbero influenzare la certificazione già emessa

In relazione alla tipologia ed entità delle modifiche ACM si riserva di richiedere ulteriore documentazione e/o di prevedere nuove verifiche presso l'Organizzazione o di iniziare un nuovo iter di certificazione, valutando se sia necessario un aggiornamento delle condizioni economiche e delle condizioni di erogazione del servizio. In particolare, ACM valuterà se le informazioni ricevute dall'Organizzazione possano influenzare la validità di una certificazione già emessa definendo i provvedimenti opportuni per poter emettere una revisione.

A seguito del mancato rispetto degli impegni sopra citati, ACM valuterà le azioni del caso, in relazione alla gravità ed entità degli eventi.

È facoltà dell'Organizzazione rinunciare volontariamente alla Certificazione, qualora non intenda uniformarsi a nuovi requisiti o alle condizioni del servizio, dandone comunicazione scritta ad ACM a mezzo PEC secondo le clausole contrattuali.

Si rimanda al Regolamento Generale di Certificazione RG CE.01 per maggiori informazioni sulle verifiche in accompagnamento e verifiche di market surveillance dell'Organismo di Accreditamento.

9. RESPONSABILITA' DI ACM

Il personale incaricato da ACM ha la responsabilità di verificare che l'Organizzazione, presso i siti comunicati e compresi nel campo di applicazione del Sistema di Gestione dell'Intelligenza Artificiale, gestisca e mantenga un sistema documentale e di registrazioni conforme ai requisiti della ISO/IEC 42001.

ACM si impegna a comunicare alle Organizzazioni certificate o in fase di valutazione (accordi contrattuali già stipulati) le modifiche nelle condizioni di rilascio della certificazione e/o le modifiche dei requisiti della prassi di riferimento, con indicazione dei tempi di adeguamento.

In funzione della significatività delle nuove prescrizioni, ACM valuta l'impatto sui certificati in validità definendo le modalità ed i tempi di transizione ai nuovi requisiti (es. esigenza di nuova valutazione o verifica coincidente con attività di sorveglianza).

È responsabilità di ACM mantenere aggiornati i propri registri, le banche dati dell'Ente di Accreditamento e le rendicontazioni richieste in relazione alle certificazioni rilasciate e al loro stato di validità.