WEBINAR ONLINE

ISO 42001

Requisiti Operativi e Sinergie con l'EU AI Act



Alessandro Pace

Ing. Lead Auditor ISO 42001

AS&C: certificazione e competenze

Audit Service & Certification (AS&C)

Organismo di certificazione Internazionale accreditato per il rilascio delle Certificazioni ISO.

01

Certificazione

Audit indipendenti per valutare
la conformità dei sistemi di gestione.

02

Formazione

Academy: competenze specialistiche
per professionisti e organizzazioni.

> La prospettiva di oggi: una governance dell'IA che si possa verificare.

Audit Service & Certification

Il percorso del webinar

01 **Scenario e responsabilità**
Dove l'IA incontra l'organizzazione

02 **Norma e regolamento**
ISO 42001, AI Act e valore strategico

03 **Rischi e controlli**
Requisiti ed evidenze operative

04 **Certificazione e formazione**
Preparazione dell'azienda e competenze

45

minuti

Poi, spazio alle domande.

Audit Service & Certification

L’IA entra nelle imprese

Italia · imprese con almeno 10 addetti che usano IA

8,2%

2024

16,4%

2025



L’utilizzo raddoppia in un anno.

53,1%

Grandi imprese italiane · 2025

20,0%

Imprese UE con almeno 10 addetti · 2025

Almeno una tecnologia di IA. Perimetro delle rispettive indagini sulle imprese.

Istat · Imprese e ICT 2025 / Eurostat · AI nelle imprese 2025

Audit
Service &
Certification

Ogni uso dell'IA richiede decisioni

Assistente per documenti
Quali informazioni può ricevere? Chi verifica le risposte?

Chatbot rivolto ai clienti
Come comunica i propri limiti? Quando interviene una persona?

Selezione del personale:
Quali criteri adopera? Come prevenire possibili discriminazioni?

IA integrata nei prodotti
quali prestazioni e condizioni di sicurezza occorre verificare?



Audit Service & Certification

Che cos’è la ISO/IEC 42001:2023

La ISO/IEC 42001:2023 definisce i requisiti per istituire, attuare, mantenere e migliorare un sistema di gestione dell’intelligenza artificiale (AIMS).

01 Si rivolge alle organizzazioni che sviluppano, forniscono o utilizzano prodotti e servizi basati sull’IA.

02 Collega politiche aziendali, responsabilità, rischi e controlli lungo il ciclo di vita dell’IA.

03 Si adatta al contesto, al ruolo e al perimetro dell’organizzazione.

04 Consente una valutazione indipendente del sistema di gestione attraverso la certificazione.

La certificazione riguarda il sistema di gestione entro il suo campo di applicazione. Non attesta l’infallibilità di ogni risultato dell’IA.

Audit Service & Certification

L’AI Act parte dal ruolo dell’azienda

EU AI Act: Regolamento (UE) 2024/1689 e successive modifiche

Fornitore

Sviluppa o fa sviluppare un sistema e lo immette sul mercato o in servizio con il proprio nome o marchio.

Sviluppo e immissione sul mercato

Deployer

Utilizza professionalmente un sistema di IA sotto la propria autorità.

Utilizzo nel proprio contesto

> Una stessa azienda può ricoprire più ruoli. Modifiche sostanziali possono cambiarne le responsabilità.

Audit Service & Certification

La classificazione europea del rischio

Pratiche vietate	l'azienda deve riconoscere gli usi proibiti ed escluderli, nei termini previsti dal regolamento.
Sistemi ad alto rischio	l'articolo 6 e gli allegati I e III individuano casi soggetti a requisiti specifici. *Esempio: determinati sistemi che selezionano o valutano candidati.*
Obblighi di trasparenza	determinati sistemi e contenuti richiedono informazioni o segnalazioni specifiche. *Esempio: interazione con un chatbot, secondo le condizioni dell'articolo 50.*
Altri sistemi	la valutazione considera comunque rischi aziendali e leggi applicabili, come la protezione dei dati.

La classificazione dipende dall'uso e dalle condizioni previste dalla legge. Gli obblighi di trasparenza possono aggiungersi ad altri requisiti.

Audit Service & Certification

Obblighi attuali e scadenze future

Già applicabili

02 FEB 2025

Applicazione delle prime pratiche vietate e delle disposizioni sull'alfabetizzazione in materia di IA, successivamente modificate.

02 AGO 2025

Applicazione delle regole sui modelli di IA per finalità generali, con disposizioni transitorie.

02 AGO 2026

Applicazione generale e avvio degli obblighi di trasparenza, salve specifiche transizioni.

Le prossime tappe dell'alto rischio

02 DIC 2027

Requisiti per i sistemi ad alto rischio dell'allegato III

02 AGO 2028

Requisiti per i sistemi ad alto rischio collegati ai prodotti regolamentati dell'allegato I, secondo il relativo perimetro.

Audit Service & Certification

La ISO 42001 come leva strategica

Un sistema di gestione dell'IA può aiutare l'organizzazione a:

01 **Decidere gli investimenti**

Valutare benefici attesi, vincoli e rischi prima di estendere gli utilizzi.

02 **Chiarire le responsabilità**

Stabilire chi autorizza gli usi e chi interviene in caso di problemi.

03 **Rendere verificabile la governance**

Rispondere alle richieste di clienti e partner con evidenze documentate.

04 **Integrare i processi**

Collegare l'IA ai sistemi qualità e sicurezza delle informazioni.

ISO 42001 e AI Act

AI Act

Definisce gli obblighi giuridici per ruoli, sistemi e utilizzi.

ISO 42001

Organizza responsabilità, rischi, controlli ed evidenze.

La certificazione ISO 42001 può sostenere il percorso di conformità. Occorrerà verificare gli obblighi specifici, comprese le procedure di valutazione della conformità e gli adempimenti previsti per il singolo caso.

Audit Service & Certification

La struttura della ISO/IEC 42001

4 · 5 · 6

Pianificare

Contesto e leadership
Rischi, impatti e obiettivi

7 · 8

Attuare

Risorse e competenze
Attività operative

9 · 10

Verificare e migliorare

Monitoraggi e audit
Riesame e azioni correttive

Allegato A	Controlli di riferimento	**Allegato B**	Guida all’attuazione

Audit Service & Certification

Perimetro chiaro e responsabilità definite

01	**Perimetro**	Sistemi, scopi d’uso e parti interessate.
02	**Direzione**	Politica per l’IA, priorità, risorse e responsabilità decisionali.
03	**IT e funzioni aziendali**	Dati, controlli tecnici e regole operative.
04	**Professionisti esterni**	Supporto al metodo e all’attuazione. La responsabilità resta all’azienda.

Audit Service & Certification

La gestione preventiva dei rischi dell'IA

01	**Criteri**	Come valutare e accettare i rischi.
02	**Scenari**	Errori, bias, dati divulgati, usi impropri e fornitori.
03	**Analisi e valutazione**	Conseguenze per azienda, persone e società. Probabilità quando applicabile.
04	**Trattamento**	Misure, responsabili, risorse e verifica dell'efficacia.
05	**Riesame**	Nuove valutazioni a intervalli pianificati e dopo cambiamenti significativi.

> *La direzione designata approva il piano di trattamento e accetta i rischi residui.*

Audit Service & Certification

Gli impatti sulle persone e sulla società

La valutazione degli impatti dell'IA esamina le possibili conseguenze degli utilizzi previsti e degli usi impropri prevedibili.

Quali **persone** o **gruppi** possono subire effetti?

Quali **conseguenze** possono riguardare diritti, sicurezza, accesso ai servizi o opportunità professionali?

Esistono gruppi particolarmente **vulnerabili**?

Quali **misure** riducono gli impatti e come se ne verifica l'efficacia?

Valutazioni da coordinare

Impatti ISO 42001 · DPIA GDPR · impatti sui diritti fondamentali
AI Act, art. 27: presupposti e contenuti specifici per ciascuna.

Audit Service & Certification

Dai rischi ai controlli applicabili

SoA

Dichiarazione di applicabilità

Scegliere

Identificare tutti i controlli necessari ai propri rischi.

Confrontare

Verificare l'allegato A e considerare controlli aggiuntivi.

Motivare

Documentare inclusioni ed esclusioni dei controlli.

> L'allegato A è il riferimento. La selezione dipende da rischi, ruolo e requisiti applicabili.

Audit Service & Certification

Bias e supervisione umana

Dati e criteri

Rappresentatività

Verificare i dati rispetto allo scopo.

Test pertinenti

Confrontare le prestazioni nei gruppi rilevanti, ove lecito.

Criteri di accettazione

Riesaminare gli scostamenti.

Supervisione umana

Competenza

Capire limiti e possibili errori.

Autorità

Poter intervenire e fermare l’uso quando necessario.

Verifica

Registrare gli interventi e valutarne gli effetti.

Audit Service & Certification

La data governance

01	**Provenienza**	Fonti, acquisizione e diritti di utilizzo.
02	**Qualità**	Pertinenza, accuratezza e rappresentatività.
03	**Preparazione**	Selezione, trasformazione e aggiornamento.
04	**Protezione**	Accessi, riservatezza e conservazione.
05	**Fornitori**	Informazioni disponibili e responsabilità contrattuali.

> Il livello di controllo cambia tra chi sviluppa il sistema e chi lo utilizza.

Audit Service & Certification

Trasparenza e tracciabilità

01

Trasparenza

Funzione, limiti e condizioni d’uso.
Segnalazione dell’IA nei casi previsti.

02

Tracciabilità

Versioni, eventi, verifiche
e interventi umani ricostruibili.

La documentazione deve corrispondere alle versioni realmente utilizzate.

> Evidenze: istruzioni aggiornate, log pertinenti e registrazioni delle decisioni.

Audit Service & Certification

Il controllo lungo il ciclo di vita

01

Prima dell'avvio

Requisiti, test e autorizzazioni.

02

Durante l'utilizzo

Monitoraggio, supervisione e fornitori.

03

Quando cambia

Rischi, impatti e verifiche aggiornati.

04

Alla dismissione

Accessi, dati e dipendenze operative.

Il supporto al sistema

Risorse · competenze · consapevolezza
Informazioni documentate accessibili e aggiornate

Audit Service & Certification

Misurare e migliorare

01	**Monitorare**	Misurare errori, anomalie, reclami e altri indicatori pertinenti.
02	**Verificare**	Audit interni obiettivi su conformità e attuazione.
03	**Decidere**	Riesame della direzione su risultati, cambiamenti e risorse.
04	**Correggere**	Gestire le cause delle non conformità e verificare le azioni.

> Il sistema deve restare efficace mentre cambiano tecnologie, fornitori e utilizzi.

Audit Service & Certification

Le sinergie operative

Tema AI Act	Riferimento ISO 42001	Evidenze utili
Rischio · art. 9	6.1.2–6.1.3 · 8.2–8.3	Valutazioni e trattamento
Dati · art. 10	A.7	Provenienza e qualità
Documenti e log · artt. 11–13	7.5 · A.6.2.7–8 · A.8	Istruzioni e registrazioni
Supervisione · artt. 14 e 26	5.3 · 7.2 · A.9–A.10	Ruoli e interventi
Sistema qualità · art. 17	Punti 4–10 · controlli pertinenti	Processi e verifiche
Monitoraggio · art. 72–73	Punti 8–10 · A.8.4	Segnalazioni e correzioni

Un’azienda software sviluppa con l’IA

Una software house usa un assistente IA per proporre codice e test.

Inquadramento	L’azienda usa un assistente IA per generare codice. Il ruolo ai sensi dell’AI Act dipende dal sistema usato e da ciò che offre sul mercato.
Rischi	Codice errato o vulnerabile, dati riservati nei prompt, licenze non chiare e modifiche accettate senza verifica.
Controlli	Strumenti approvati, dati ammessi, revisione umana del codice, test e scansioni di sicurezza prima del rilascio.
Evidenze	Regole d’uso, revisioni delle pull request, esiti dei test, versioni e modifiche registrate, gestione degli incidenti.

> Il codice proposto dall’IA entra nel ciclo di sviluppo come contributo da verificare.

Audit Service & Certification

Preparare l'azienda: la GAP Analysis

01	**Mappare**	Sistemi, utilizzi, ruoli e perimetro.
02	**Confrontare**	Processi, competenze e documenti rispetto ai requisiti.
03	**Individuare**	Carenze su rischi, impatti, controlli ed evidenze.
04	**Pianificare**	Priorità, responsabili e risorse per l'adeguamento.
05	**Verificare**	Attuazione, audit interno e riesame della direzione.

> Il risultato: un piano aziendale motivato e verificabile, con l'eventuale supporto di consulenti.

Competenze proporzionate al ruolo

01	**Dirigenti**	Scelte sull'IA, responsabilità e accettazione dei rischi.
02	**Responsabili IT**	Dati, test, monitoraggio, tracciabilità e fornitori.
03	**Utilizzatori**	Regole d'uso, limiti, supervisione e segnalazioni.
04	**Professionisti e auditor**	Requisiti, evidenze e verifica dei processi.

> Individuare le competenze necessarie e valutare l'efficacia delle azioni formative.

Audit Service & Certification

L’iter di certificazione

01 **Richiesta di certificazione**

Perimetro e caratteristiche dell’organizzazione.

02 **Pre-Audit (opzionale)**

Esamina del livello di preparazione del sistema.

03 **Stage 1**

Preparazione, documenti, audit interni e riesame.

04 **Stage 2**

Attuazione ed efficacia: interviste e campionamento.

05 **Mantenimento**

Sorveglianze e successivo rinnovo.

> Tempi e impegno dipendono da perimetro, complessità e preparazione dell’organizzazione.

Audit Service & Certification

Cosa verifica un auditor

Ambito	Evidenze	Errore da evitare
Responsabilità	Ruolo dell'organizzazione rispetto all'IA Ruoli conosciuti e usi censiti	Responsabilità soltanto formali
Rischi e impatti	Analisi degli utilizzi effettivi	Valutazioni generiche e statiche
Controlli	Test e motivazioni della SoA	Dichiarazioni senza prove
Competenze	Persone che applicano le regole	Sola registrazione delle presenze
Miglioramento	Audit, riesami e azioni verificate	Chiusure senza analisi delle cause

L'auditor cerca coerenza tra requisiti, processi dichiarati e attività effettive.

Audit Service & Certification

Academy

Corsi per i professionisti | Formazione per le aziende

ISO/IEC 42001	Intelligenza artificiale
ISO/IEC 27001	Sicurezza delle informazioni
ISO 9001	Gestione Qualità
ISO 14001	Gestione Ambientale
ISO 45001	Salute e sicurezza sul lavoro



Scopri i corsi

Audit Service & Certification

Domande e risposte

Le vostre domande

Ruoli e utilizzi

Rischi e controlli

Evidenze di audit

Percorsi e competenze

15 minuti di confronto