

5th Project Management Forum Lugano

Innovazione e Strategie nel Project Management

Applicazione della ISO/IEC 42001 alla gestione dei progetti e alla formazione di competenze in ambito IA nel Project Management

Maurilio Savoldi

October 13-14, 2025

Lead auditor per SV Certification, docente e consulente.

Svolgo il ruolo di DPO per diverse organizzazioni di medie/grandi dimensioni.

Da sempre mi occupo di miglioramento delle organizzazioni e delle persone



SV Cert. Group

www.svcertification.com



www.linkedin.com/in/maurilio-savoldi/

SV Certification Sagl
Pascolet 41b –
6537 Grono (GR) Switzerland



msavoldi@svcert.ch



+41 (0)76 812 13 09 (CH)



LA NORMA



I PROGETTI



5th Project Management Forum Lugano

Innovazione e Strategie nel Project Management

Che cos'è la ISO/IEC 42001 e la sua applicazione in un mondo che cambia

Maurilio Savoldi

October 13-14, 2025

Il mondo è cambiato velocemente





15 25 51

15 25 51

In che modo il mondo è cambiato?

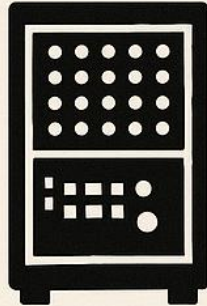


5th Project
Management Forum
Lugano
October 13-14, 2025



INVENTION
OF PRINTING

1450



BIRTH OF
COMPUTING

1940



BIRTH OF
PC

1980



BIRTH OF
INTERNET

2000



BIRTH
AI

2023

The image features a dark blue night sky filled with numerous small white stars. In the foreground, the silhouettes of several oil drilling rigs are visible against a bright orange and yellow horizon. The central rig is the most prominent, with a large, dark, stylized gusher of oil or gas erupting from its top, forming a fan-like shape. The text "I dati sono il nuovo petrolio" is written in white, sans-serif font across the lower portion of the image, centered horizontally.

I dati sono il nuovo petrolio



In questi anni è emersa l'esigenza
sempre più l'esigenza di normative,
regolamenti e legislazione
specifici.

(LPD/GDPR, Data Act, IA Act,
norme della famiglia ISO/IEC
27000)



1. Normativa volontaria (standard e framework)

- ISO/IEC 42001:2023 – AI Management System (AIMS): requisiti per istituire, mantenere e migliorare un sistema di gestione dell'IA (governance, risk & impact assessment, ciclo di vita, fornitori). Utile per dimostrare “state of the art” e allinearsi ai futuri standard armonizzati UE.
- ISO/IEC 23894:2023 – AI Risk Management (guidance): guida per integrare la gestione del rischio AI nel ciclo di vita, in coerenza con ISO 31000. Complementare a 42001.
- ISO/IEC 22989:2022 – Concetti e terminologia (+ emendamento su GenAI in sviluppo): tassonomia e definizioni comuni; emendamento su GenAI in fase draft.
- CEN/CENELEC JTC 21 (UE) – standard “armonizzati” per l'AI Act: programma di lavoro per standard su affidabilità, gestione rischio, QMS AI e conformity assessment che supporteranno la presunzione di conformità.
- NIST AI RMF 1.0 (USA) + Generative AI Profile (NIST.AI.600-1): quadro volontario per identificare/mitigare i rischi; profilo specifico GenAI (2024).
- IEEE 7000-series (etica, trasparenza, privacy, bias, fail-safe): famiglia di standard/linee guida per principi etici e requisiti tecnici (es. 7000, 7001, 7002, 7009).

2. Quadro legislativo – Unione Europea (UE)

- AI Act (Reg. UE 2024/1689): entrata in vigore 1 agosto 2024. Applicazione graduale: divieti/alfabetizzazione AI dal 2 febbraio 2025; obblighi per modelli GPAI e governance dal 2 agosto 2025; regole per sistemi ad alto rischio pienamente applicabili entro 2 agosto 2026 (con alcune estensioni fino al 2 agosto 2027). In parallelo sviluppo degli standard armonizzati CEN/CENELEC.
- Nuova Direttiva Prodotti Difettosi – PLD (Dir. (UE) 2024/2853): in vigore dall'8 dicembre 2024; gli Stati membri devono recepirla entro il 9 dicembre 2026. Modernizza la responsabilità oggettiva e copre anche prodotti digitali e AI.
- AI Liability Directive (proposta 2022): ritirata dal programma di lavoro 2025 della Commissione per mancanza di consenso.
- Trattati/Cooperazione: Convenzione quadro del Consiglio d'Europa sull'IA (aperta alla firma dal 5 settembre 2024) potenzialmente rilevante per il diritto UE e nazionale.



3. Quadro legislativo – Stati Uniti (federale)

- Legge federale orizzontale: non esiste ancora una normativa federale onnicomprensiva sull'IA.
- Policy federale: OMB M-24-10 (28 marzo 2024) stabilisce obblighi di governance e risk management dell'IA per le agenzie federali (con pratiche minime per usi ad impatto sui diritti/sicurezza).
- NIST: AI Risk Management Framework 1.0 e profilo Generative AI (2024) come riferimento tecnico volontario ampiamente adottato.
- Stati federati: quadro frammentato (privacy acts e leggi di settore); non ci sono obblighi federali equivalenti all'AI Act UE.



Diversi approccio

- UE: mappa i casi d'uso al rischio; implementa un AIMS conforme a ISO/IEC 42001; prepara QMS e documentazione tecnica; monitora gli standard armonizzati CEN/CENELEC.
- Svizzera: allinea governance e risk management a ISO/IEC 42001 e 23894; verifica impatti settoriali e requisiti LPD; monitora percorso di ratifica della Convenzione CoE.
- USA: adotta NIST AI RMF (e il profilo GenAI) come baseline di risk management; applica le linee OMB se lavori con agenzie federali; monitora sviluppi federali e statali; costruisci un AIMS ispirato a ISO 42001.

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Context of the organization	5
4.1 Understanding the organization and its context	5
4.2 Understanding the needs and expectations of interested parties	6
4.3 Determining the scope of the AI management system	6
4.4 AI management system	6
5 Leadership	7
5.1 Leadership and commitment	7
5.2 AI policy	7
5.3 Roles, responsibilities and authorities	8
6 Planning	8
6.1 Actions to address risks and opportunities	8
6.1.1 General	8
6.1.2 AI risk assessment	9
6.1.3 AI risk treatment	9
6.1.4 AI system impact assessment	10
6.2 AI objectives and planning to achieve them	10
6.3 Planning of changes	11
7 Support	11
7.1 Resources	11
7.2 Competence	11
7.3 Awareness	12
7.4 Communication	12
7.5 Documented information	12
7.5.1 General	12
7.5.2 Creating and updating documented information	12
7.5.3 Control of documented information	13
8 Operation	13
8.1 Operational planning and control	13
8.2 AI risk assessment	13
8.3 AI risk treatment	14
8.4 AI system impact assessment	14
9 Performance evaluation	14
9.1 Monitoring, measurement, analysis and evaluation	14
9.2 Internal audit	14
9.2.1 General	14
9.2.2 Internal audit programme	14
9.3 Management review	15
9.3.1 General	15
9.3.2 Management review inputs	15
9.3.3 Management review results	15
10 Improvement	15
10.1 Continual improvement	15
10.2 Nonconformity and corrective action	16

INTERNATIONAL
STANDARD

ISO/IEC
42001

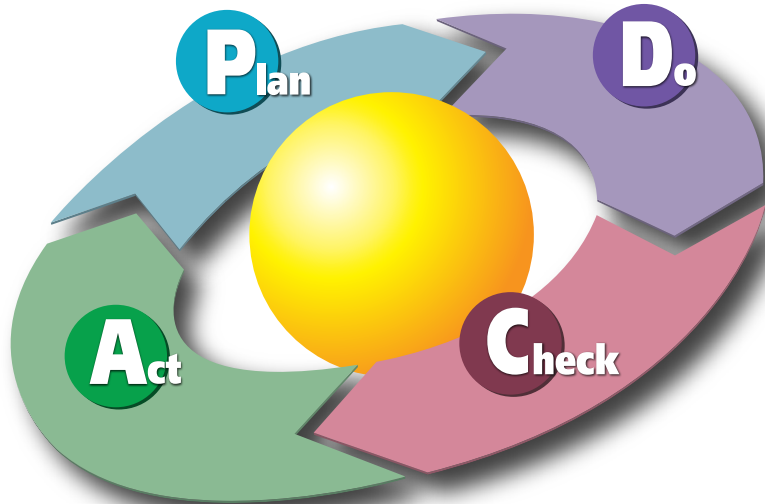
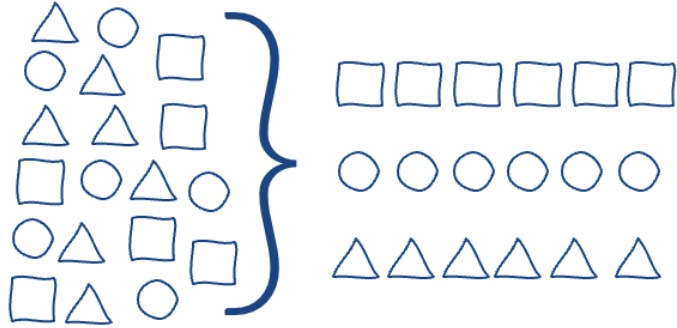
HIGH LEVEL
STRUCTURE
comme alle
norme ISO

First edition
2023-12

Information technology — Artificial
intelligence — Management system

*Technologies de l'information — Intelligence artificielle — Système
de management*

Che cosa è un sistema di gestione?



Un modello organizzativo che permette di dare un ordine ai significativo:

- ai flussi di attività,
- ai ruoli,
- agli strumenti,
- ai metodi,
- ai controlli,

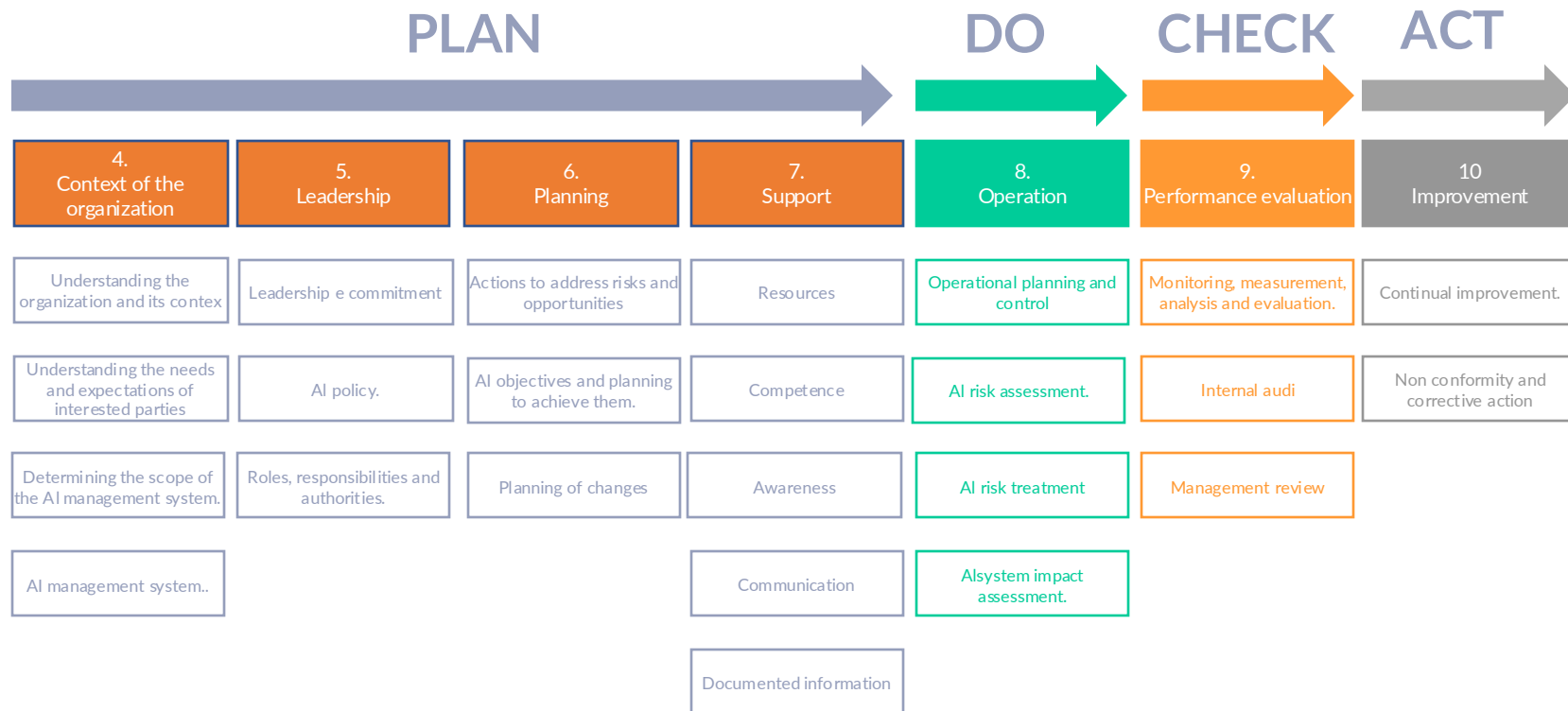
garantendo così da un lato il corretto funzionamento dell'organizzazione e

- il miglioramento continuo del del sistema

La visione del miglioramento continuo della ISO/IEC 42001:2023



5th Project
Management Forum
Lugano
October 13-14, 2025



A. Comprensione e Impegno

- Consapevolezza: Garantire che le parti interessate comprendano lo scopo e i benefici della ISO/IEC 42001.
- Impegno: Ottenere l'impegno della direzione nel implementare e mantenere un sistema di gestione dell'intelligenza artificiale.

B. Scopo

- Identificare le Attività di AI: Determinare quali processi, prodotti o servizi di intelligenza artificiale sono inclusi.
- Esclusioni: Definire chiaramente le aree escluse.

C. Leadership e Governance

- Nomina di una Persona Responsabile: Designare qualcuno che sovrintenda alla gestione dell'AI.
- Sviluppo delle Politiche: Creare una politica per la gestione dell'AI allineata con gli obiettivi organizzativi.

D. Valutazione dei Rischi e Identificazione delle Opportunità

- Valutare i Rischi: Identificare e valutare i rischi legati all'implementazione dell'AI.
- Identificare le Opportunità: Individuare possibilità di miglioramento dei processi di AI.

E. Implementazione e Operatività dell'AI

- Progettazione e Sviluppo: Implementare sistemi di AI seguendo linee guida stabilite.
- Gestione dei Dati: Garantire qualità, privacy e sicurezza dei dati.
- Test e Validazione: Validare modelli e algoritmi di AI.
- Implementazione: Distribuire le soluzioni di AI in modo controllato.

F. Monitoraggio e Misurazione

- Metriche di Prestazione: Definire metriche per valutare le prestazioni dell'AI.
- Monitoraggio: Monitorare continuamente i sistemi di AI per verificarne l'efficacia e la conformità.

G. Feedback e Miglioramento

- Ciclo di Feedback: Creare canali per raccogliere feedback da utenti, stakeholder e dipendenti.
- Azioni di Miglioramento: Riesaminare e migliorare regolarmente i processi di AI in base ai dati di performance e ai feedback ricevuti.

H. Documentazione e Registrazioni

- Controllo dei Documenti: Mantenere registri relativi alla gestione dell'AI.
- Materiali Formativi: Sviluppare materiali di formazione per il personale coinvolto nelle attività di AI.

I. Audit Interni e Riesami

- Audit Regolari: Condurre audit interni per verificare la conformità alla ISO/IEC 42001.
- Riesame della Direzione: Valutare periodicamente l'efficacia del sistema di gestione dell'AI.



J. Miglioramento Continuo

- Apprendere e Adattarsi: Imparare continuamente dalle esperienze e adattare le pratiche di AI.
- Rimanere Aggiornati: Tenersi informati sui progressi tecnologici e sulle migliori pratiche in materia di AI.

Il ruolo degli allegati



5th Project
Management Forum
Lugano
October 13-14, 2025



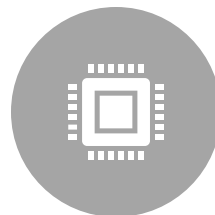
L'allegato A (normativo) contiene i controlli ovvero le misure da porre in atto per mantenere o modificare un rischio (analogamente a quanto prevede il corrispondente allegato A della ISO/IEC 27001:2022)



L'allegato B (normativo) riporta le linee guida per l'applicazione dei controlli definiti nell'allegato A (analogamente alla ISO/IEC 27002:2022 per quanto senza la componente degli attributi)



L'allegato C (informativo) delinea i potenziali obiettivi organizzativi, le fonti di rischio e le descrizioni che possono essere prese in considerazione nella gestione dei rischi legati all'uso dell'IA



L'allegato D (informativo) riguarda gli ambiti e i settori in cui può essere utilizzato un AIMS

La struttura dei controlli dell'allegato A

- **A.2 Politiche relative all' Intelligenza Artificiale** (comprende anche allineamento alle altre politiche dell'organizzazione e la revisione delle politiche di AI);
- **A.3 Organizzazione interna** (es. ruoli e responsabilità);
- **A.4 Risorse per i sistemi di Intelligenza Artificiale** (es. dati, strumenti, risorse umane);
- **A.5 Analisi dell'impatto dei sistemi di Intelligenza Artificiale** (es. su individui, gruppi e società e relativa documentazione);
- **A.6 Ciclo di vita del sistema di Intelligenza Artificiale;**
- **A.7 Dati per i sistemi di Intelligenza Artificiale** (es. acquisizione e preparazione dei dati);
- **A.8 Informazioni per le parti interessate ai sistemi di Intelligenza Artificiale** (es. comunicazione di incidenti);
- **A.9 Utilizzo dei sistemi di Intelligenza Artificiale** (es. uso responsabile ed uso previsto);
- **A.10 Rapporti con terze parti** (ad esempio: fornitori, clienti).

5th Project Management Forum Lugano

Innovazione e Strategie nel Project Management

Applicazione della ISO/IEC 42001 alla gestione dei progetti: la gestione del rischio

Maurilio Savoldi

October 13-14, 2025



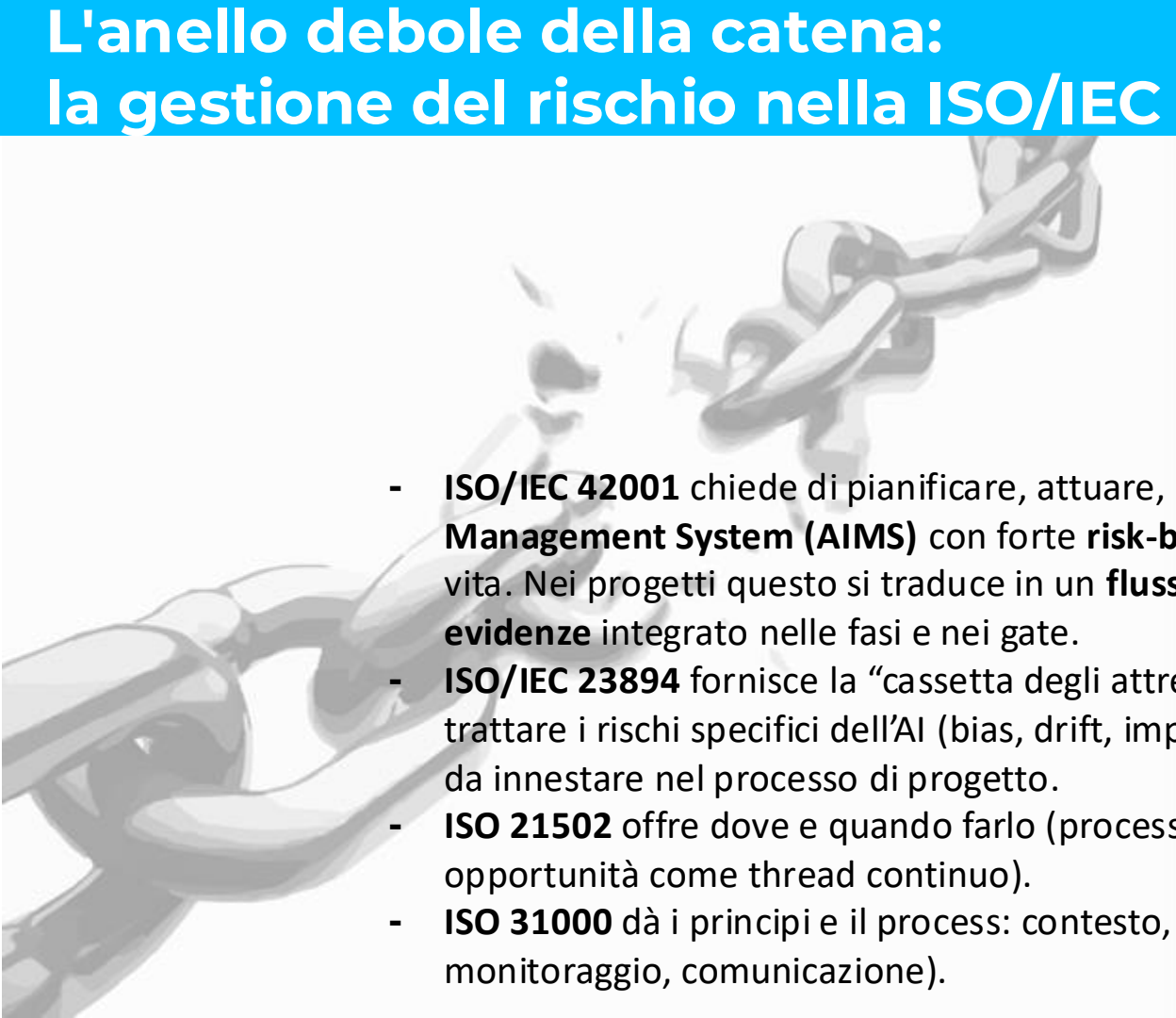
Le fonti rischio identificate nell'allegato C, e da tenere sotto controllo attraverso l'apparato dei controlli, sono dovute a:

- **complessità dell'ambiente**
- **mancaanza di trasparenza e condivisione**
- **livello di automazione**
- **componente di machine learning**
- **problemi hardware del sistema**
- **stato del sistema nel corso del suo "ciclo di vita"**
- **livello di maturità della tecnologia**

L'anello debole della catena: la gestione del rischio nella ISO/IEC 42001



5th Project
Management Forum
Lugano
October 13-14, 2025

- 
- **ISO/IEC 42001** chiede di pianificare, attuare, monitorare e migliorare un **AI Management System (AIMS)** con forte **risk-based thinking** lungo tutto il ciclo di vita. Nei progetti questo si traduce in un **flusso: rischio, obiettivi, controll ed evidenze** integrato nelle fasi e nei gate.
 - **ISO/IEC 23894** fornisce la “cassetta degli attrezzi” per identificare, valutare, trattare i rischi specifici dell’AI (bias, drift, impatti sociali, sicurezza, compliance), da innestare nel processo di progetto.
 - **ISO 21502** offre dove e quando farlo (processi e pratiche di PM, con rischi & opportunità come thread continuo).
 - **ISO 31000** dà i principi e il process: contesto, valutazione, trattamento, monitoraggio, comunicazione).

Gli elementi nella gestione del rischio



5th Project
Management Forum
Lugano
October 13-14, 2025

KEY RISKS

DESIGN RISK

DATA RISK

ALGORITHMIC RISK

PERFORMANCE RISK

TECHNOLOGY RISK

THIRD PART RISK

CONDUCT, COMPLIANCE
& LEGAL RISK

BUSINESS PROCESS RISK

PROCESS

CONSISTENCE AI
DEFINITION

MODEL RISK DEFINE

MODEL DOCUMENTATION
(TECNICAL DETAIL)

MODEL INVENTORY
FRAMEWORK

ETHICS & PRIVACY ASSESSMENT

LINES OF DEFENCE OPERATING
MODEL

ONGOING MONITORING & CONTROL

TECHNOLOGY

DATA & CLOUD

INFRASTRUCTURE

VENDOR TOOL MANAGEMENT

PEOPLE

LEADERSHIP

ROLE & RESPONSABILITY

TRAINING

PROLCY, PROCEDURE AND GUIDELINE

5th Project Management Forum Lugano

Innovazione e Strategie nel Project Management

Applicazione della ISO/IEC 42001 alla gestione dei progetti

Maurilio Savoldi

October 13-14, 2025

Alcuni esempi di applicazione dell'AI al PM



5th Project
Management Forum
Lugano
October 13-14, 2025

Processo / Area di conoscenza	Applicazione dell'IA	Tecnologia / Approccio IA	Benefici misurabili / Impatti
3. Pianificazione del progetto	Generazione automatica di WBS, Gantt, milestone	Generative AI (LLM), pianificazione automatizzata	Riduzione tempi di pianificazione del 40–60%, piani coerenti e completi
	Previsione di costi e tempi basata su dati storici	Regressione ML, reti neurali	Accuratezza delle previsioni $\pm 5\text{--}10\%$ rispetto a metodi tradizionali
	Pianificazione risorse e ottimizzazione del carico di lavoro	Algoritmi genetici, ottimizzazione multi-obiettivo	Uso efficiente delle risorse, riduzione straordinari e conflitti di carico
	Identificazione e classificazione automatica dei rischi	NLP + clustering + modelli predittivi	Maggiore copertura dei rischi, early warning automatico



In realtà, non lo sappiamo!!!!



Mappatura essenziale dei requisiti 42001 sul ciclo di progetto (ibrido stage-gate o iterativo):

- **Avvio / Concept:** Definire contesto, parti interessate, scopi e **criteri di rischio/impatti** per gli use case AI. Collegare obiettivi di progetto e **tolleranze** (risk criteria) → baseline.
- **Pianificazione:** Condurre **AI risk assessment** e **AI impact assessment** separati ma collegati; pianificare i **trattamenti** e gli **obiettivi di performance** (es. target su FPR/FNR, explainability). Integrare piani con qualità, sicurezza, privacy e compliance.
- **Esecuzione / Operatività:** Implementare controlli e **procedure operative** per sviluppo, validazione, rilascio, monitoraggio e incident handling dei sistemi AI (compresi fornitori/modelli terzi).
- **Monitoraggio & Valutazione:** Misurare e riesaminare performance/efficacia dei controlli e dei trattamenti; aggiornare rischi e impatti; **evidenze** per audit.
- **Miglioramento Continuo:** Gestire non conformità e azioni correttive/preventive, aggiornare metriche e criteri di rischio al mutare del contesto e dei dati.

5th Project Management Forum Lugano

Innovazione e Strategie nel Project Management

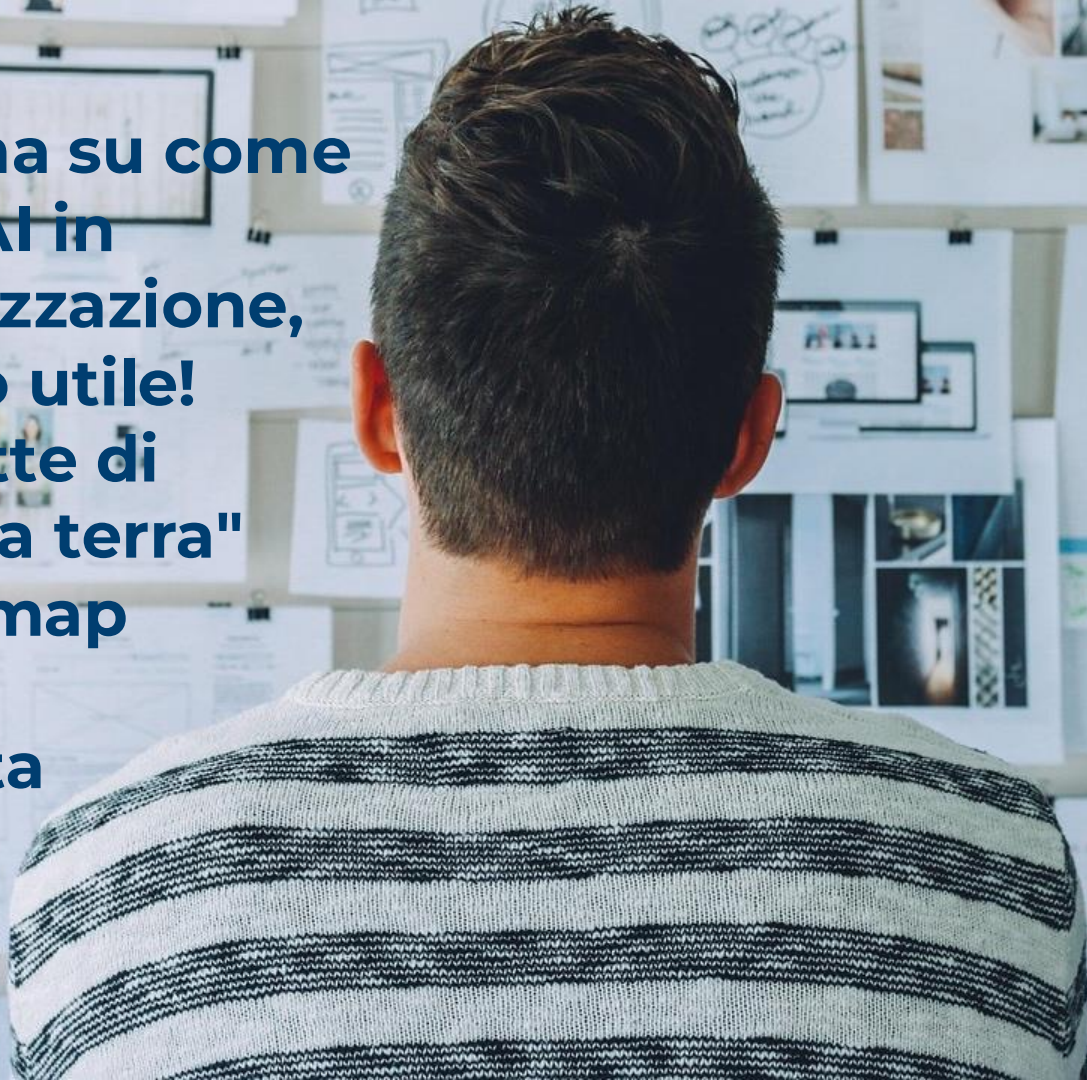
Applicazione della ISO/IEC 42001 alla formazione di competenze in ambito IA nel Project Management

Maurilio Savoldi

October 13-14, 2025



**Una norma su come
gestire l'AI in
un'organizzazione,
ci è molto utile!
Ci permette di
"mettere a terra"
una roadmap
definita e
strutturata**



In estrema sintesi, la norma ci aiuta a:



Punto	Descfizione requisito	Cosa fare
4.1	Comprendere l'organizzazione e il suo contesto	Analisi del contesto interno ed esterno, mappa degli stakeholder, documenti strategici
4.2	Comprendere le esigenze e le aspettative delle parti interessate	Elenco stakeholder, analisi requisiti legali e normativi, matrice di aspettative
4.3	Determinazione del campo di applicazione del sistema di gestione per l'IA	Documento di campo di applicazione, perimetro del sistema di gestione
4.4	Sistema di gestione per l'IA	Manuale AIMS, descrizione dei processi e interazioni



Capire in che contesto opera il progetto (o l'organizzazione, e quali sono le parti interessate, ci potrà guidare nel corso della prosecuzione del progetto, per esempio a capire le conformità legali, o etiche, a cui attenerci (per esempio nel trattamento di dati personali

In estrema sintesi, la norma ci aiuta a:



5th Project
Management Forum
Lugano
October 13-14, 2025

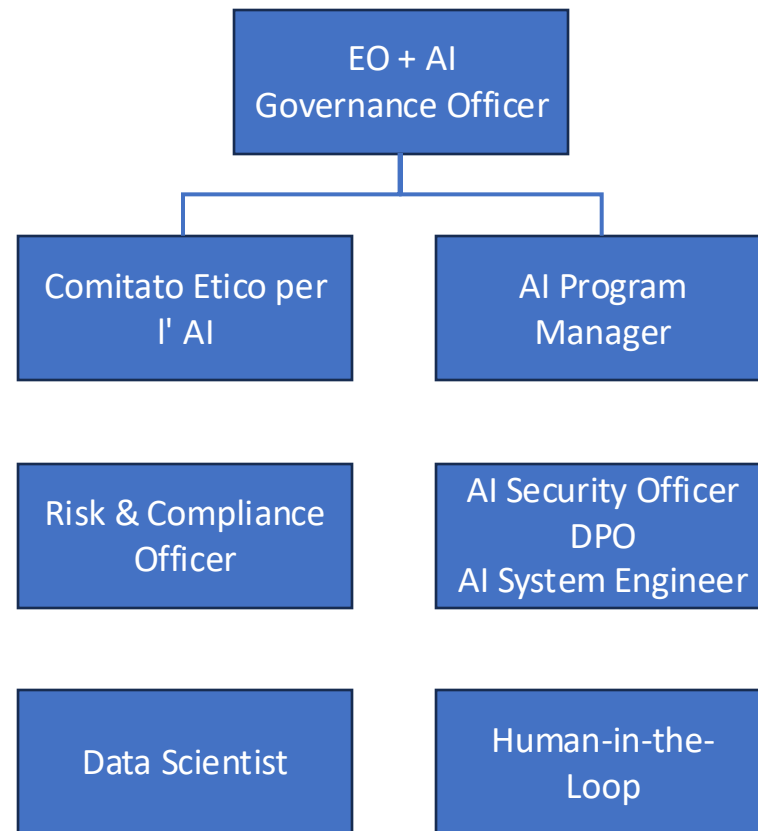
Punto	Descrizione requisito	Cosa fare
5.1	Leadership e impegno	Politica IA, verbali riunioni direzione, comunicazioni interne
5.2	Politica per l'IA	Politica formalmente approvata e diffusa, evidenza della revisione periodica
5.3	Ruoli, responsabilità e autorità nell'organizzazione	Organigramma IA, descrizione ruoli (AI Officer, Data Steward, ecc.)
6.1	Azioni per affrontare rischi e opportunità	Registro rischi/opportunità IA, criteri di trattamento

Struttura generale ed esempio di un organigramma AI



5th Project
Management Forum
Lugano
October 13-14, 2025

Livello	Funzione	Descrizione sintetica
Direzionale / Strategico	Governance e responsabilità legale	Definisce politiche IA, approva strategie e risorse
Tattico / Manageriale	Gestione del ciclo di vita dei sistemi IA	Coordina sviluppo, compliance, e rischio
Operativo / Tecnico	Sviluppo, validazione, monitoraggio	Implementa, testa e gestisce i modelli IA



In estrema sintesi, la norma ci aiuta a:

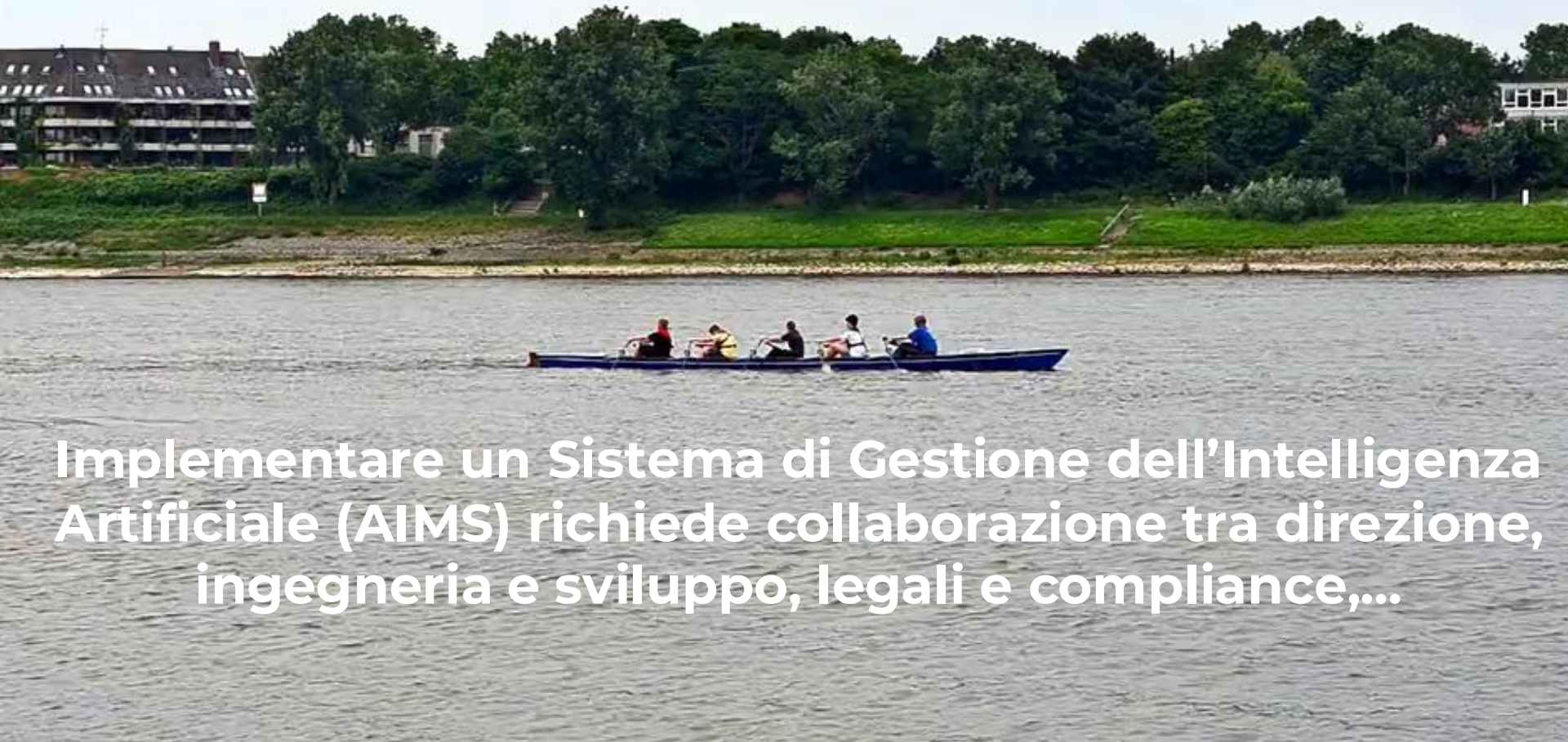


Punto	Descrizione requisito	Cosa fare
7.3	Consapevolezza	Comunicazioni interne, campagne di sensibilizzazione IA
7.4	Comunicazione	Piano comunicazione IA, registro comunicazioni interne/esterne
7.5	Informazioni documentate	Elenco documenti controllati, registro revisioni
8.1	Pianificazione e controllo operativi	Procedure IA, workflow, approvazioni modelli

Quali competenze nell'implementazione dell'AI



5th Project
Management Forum
Lugano
October 13-14, 2025



Implementare un Sistema di Gestione dell'Intelligenza Artificiale (AIMS) richiede collaborazione tra direzione, ingegneria e sviluppo, legali e compliance,...

Alcune competenze trasversali



Competenza trasversale	Descrizione sintetica	Livello atteso	Ruoli organizzativi più pertinenti
Pensiero critico e analitico	Capacità di analizzare dati, modelli e decisioni dell'IA in modo oggettivo, identificando bias, incoerenze e rischi etici o operativi.	Avanzato	AI Officer, Data Analyst, Risk Manager
Competenze etiche e responsabilità sociale	Conoscenza dei principi di equità, trasparenza, sicurezza e privacy nell'uso dell'IA; promozione di un approccio "Human-Centric AI".	Avanzato	Compliance Officer, HR Manager, AI Governance Lead
Comunicazione interdisciplinare	Capacità di tradurre concetti tecnici dell'IA in linguaggio comprensibile per stakeholder non tecnici; favorisce la collaborazione tra business, IT e compliance.	Intermedio	Project Manager, AI Specialist, Dirigente di funzione
Leadership adattiva e gestione del cambiamento	Guida dei processi di transizione organizzativa e culturale legati all'adozione dell'IA, gestendo resistenze e motivando i team.	Avanzato	Executive, AI Program Director, Change Manager
Collaborazione interfunzionale	Lavoro efficace in team multidisciplinari che uniscono competenze tecniche, legali e operative per sviluppare soluzioni IA sostenibili.	Intermedio	Data Scientist, Legal Counsel, Product Owner
Data literacy (alfabetizzazione ai dati)	Capacità di comprendere e utilizzare i dati in modo critico, riconoscendo limiti, qualità e rilevanza per i processi decisionali e predittivi.	Base → Intermedio	Tutti i dipendenti, Data Steward, Process Owner
Orientamento all'innovazione	Attitudine a sperimentare soluzioni IA, migliorare processi e servizi, e valorizzare il potenziale tecnologico in chiave sostenibile.	Intermedio	Innovation Manager, R&D Specialist, AI Engineer
Problem solving complesso	Identificazione e analisi di problemi aziendali complessi, selezionando soluzioni basate su IA con impatto misurabile e gestione dei trade-off.	Avanzato	AI Architect, Strategy Analyst, Process Engineer
Gestione dei rischi e conformità	Valutazione e mitigazione di rischi legali, reputazionali, tecnici e operativi associati ai sistemi IA, in coerenza con i requisiti ISO/IEC 42001 e AI Act.	Avanzato	AI Compliance Officer, Risk Manager, DPO
Mentalità data-driven	Predisposizione a decisioni basate su evidenze e indicatori misurabili, migliorando la trasparenza e la fiducia nei sistemi IA.	Intermedio	Dirigenti, Analisti, Responsabili di funzione

Alcune competenze tecniche



Competenza tecnica	Descrizione sintetica	Livello atteso	Ruoli organizzativi più pertinenti
Machine Learning e Deep Learning	Conoscenza delle principali tecniche di apprendimento automatico e profondo, inclusa la progettazione, addestramento, validazione e ottimizzazione dei modelli.	Avanzato	Data Scientist, AI Engineer, ML Specialist
Data Engineering e Data Management	Capacità di gestire l'intero ciclo di vita dei dati (raccolta, pulizia, integrazione, qualità, governance) a supporto delle applicazioni IA.	Avanzato	Data Engineer, Data Steward, Data Architect
MLOps e AI Lifecycle Management	Competenze su pipeline di sviluppo e deployment continuo (CI/CD), monitoraggio, versioning e auditing dei modelli IA.	Avanzato	AI Engineer, DevOps Engineer, AI Governance Lead
AI Risk & Security Management	Conoscenza delle vulnerabilità tipiche dell'IA (es. adversarial attacks, data poisoning) e applicazione dei controlli di sicurezza (AI Security by Design).	Intermedio/ Avanzato	AI Security Officer, Risk Manager, CISO
Explainable AI (XAI) e interpretabilità dei modelli	Capacità di utilizzare tecniche e strumenti per spiegare decisioni dei modelli e garantire trasparenza e accountability.	Intermedio	Data Scientist, Compliance Officer, AI Auditor
AI Governance e conformità normativa	Conoscenza delle norme ISO/IEC 42001, AI Act, GDPR e linee guida etiche; capacità di strutturare policy, controlli e audit sull'IA.	Avanzato	AI Governance Manager, DPO, Legal Officer
Data & Model Ethics Assessment	Valutazione dei bias nei dati e nei modelli, analisi di impatto etico e sociale (AI Impact Assessment, AIIA).	Intermedio	AI Compliance Officer, Ethics Committee Member
Cloud e Edge Computing per IA	Capacità di progettare e gestire architetture scalabili per il training e il deployment dei modelli IA in ambienti cloud, ibridi o edge.	Intermedio	Cloud Architect, AI Engineer, IT Infrastructure Manager
AI System Integration e API Management	Integrazione di modelli IA nei sistemi aziendali tramite API, microservizi e middleware, garantendo interoperabilità e sicurezza.	Intermedio	Solution Architect, Software Engineer, Integration Specialist
AI Performance & Quality Metrics	Definizione di KPI, metriche di accuratezza, robustezza, equità e affidabilità dei sistemi IA, in linea con i requisiti di monitoraggio ISO/IEC 42001 e 23894.	Intermedio/ Avanzato	AI Auditor, Quality Manager, AI Program Director

In estrema sintesi, la norma ci aiuta a:



Punto	Descrizione requisito	Cosa fare
8.2	Gestione dei sistemi di IA durante il ciclo di vita	Piano di sviluppo, test, validazione, monitoraggio dei modelli IA
8.3	Controllo dei processi esternalizzati	Contratti fornitori IA, SLA, audit fornitori
9.1	Monitoraggio, misurazione, analisi e valutazione	Indicatori di performance IA, risultati di monitoraggio
9.2	Audit interno	Piano audit, report di audit, azioni correttive

Alcuni indicatori per il monitoraggio dell'uso dell'AI in un progetto



5th Project
Management Forum
Lugano
October 13-14, 2025

Indicatore di performance (KPI)	Descrizione	Obiettivo di monitoraggio	Unità di misura / formula
Accuratezza dei modelli IA	Valuta la precisione delle previsioni, classificazioni o raccomandazioni generate dall'algoritmo.	Misurare l'efficacia tecnica del modello e il suo allineamento agli obiettivi di business.	% correttezza = (previsioni corrette / totale previsioni) × 100
Tasso di automazione efficace	Percentuale di processi o attività automatizzati dall'IA che raggiungono i risultati previsti senza intervento umano correttivo.	Valutare il livello di affidabilità operativa dell'IA.	% automazione = (processi automatizzati con successo / totale processi automatizzati) × 100
Tempo medio di decisione o di completamento attività	Misura la riduzione dei tempi decisionali o operativi grazie all'IA.	Valutare l'efficienza e la produttività introdotte dal sistema.	Δ tempo = (tempo medio pre-IA – tempo medio post-IA)
Indice di trasparenza e spiegabilità	Percentuale di modelli IA per i quali sono documentati i criteri decisionali e i log di output.	Garantire la conformità a principi etici, di accountability e governance (ISO/IEC 42001, Annex A.4 e A.6).	% modelli spiegabili = (modelli documentati / totale modelli) × 100
Tasso di incidenti o bias rilevati	Numero di anomalie, errori o discriminazioni rilevate nel funzionamento dei sistemi IA.	Monitorare la qualità, la sicurezza e l'equità del sistema IA.	(incidenti o bias rilevati / periodo)

In estrema sintesi, la norma ci aiuta a:



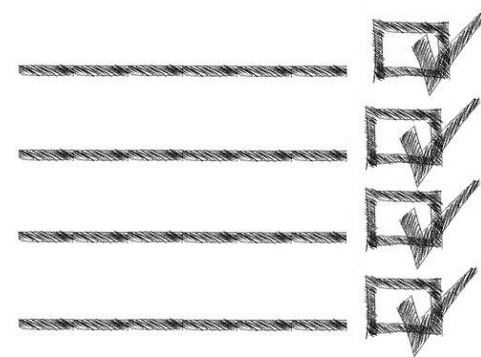
Punto	Descrizione requisito	Cosa fare
9.3	Riesame della direzione	Verbali riesame direzione, input e output documentati
10.1	Non conformità e azioni correttive	Registro non conformità IA, piani di azione
10.2	Miglioramento continuo	Evidenze di miglioramento, piani di revisione AIMS

In estrema sintesi, la norma ci aiuta a:



Punto	Descfizione requisito	Cosa fare
A.2	Governance dell'IA	Politiche di governance IA, comitato etico, framework di responsabilità
A.3	Gestione dei rischi dell'IA	Registro rischi IA, metodologie di valutazione, AIIA
A.4	Gestione del ciclo di vita dei sistemi di IA	Documentazione sul design, addestramento, validazione e monitoraggio dei modelli
A.5	Trasparenza e tracciabilità	Documentazione tracciabilità dati e modelli, report di explainability

- Politiche legate all'intelligenza artificiale
- Organizzazione interna sistema di intelligenza artificiale
- Risorse per i sistemi di intelligenza artificiale
- Valutazione degli impatti dei sistemi di intelligenza artificiale
- Ciclo di vita del sistema di intelligenza artificiale
- Dati per i sistemi di intelligenza artificiale
- Informazioni agli interessati
- Utilizzo dei sistemi di intelligenza artificiale
- Rapporti con terzi e clienti



La Gestione dei progetti AI è coerente con le altre politiche aziendali (privacy, sicurezza, qualità)?

Riferimento	Principio / Obiettivo	Policy IA Aziendale	Controlli / Misure Implementate	Evidenze	Stato	Azioni
ISO/IEC 42001 — Cl. 5.3	Ruoli e responsabilità nella governance dell'IA	§2.1 "Accountability e supervisione umana"	Nomina AI Officer, Comitato Etico, registro ruoli	Organigramma AI, verbali riunioni	✓	—
ISO/IEC 42001 — Cl. 6.1.2	Valutazione dei rischi IA	§3.2 "Gestione rischio algoritmico"	AIIA, framework ISO/IEC 23894, revisione trimestrale	Registro rischi IA, report mitigazioni	✓	—
AI Act — Art. 9	Gestione dei rischi dei sistemi ad alto rischio	§3.2 "Risk Management"	Risk matrix, validazione pre-produzione, test etico	Risk Register, risultati test bias	⚠	Aumentare frequenza riesami
AI Act — Art. 13	Trasparenza verso gli utenti	§4.1 "Comunicazione e trasparenza"	Banner informativo "Stai interagendo con un'IA"	Screenshot interfaccia, manuale utente	✓	—
AI Act — Art. 15	Accuratezza, robustezza e cybersicurezza	§5.4 "Robustezza tecnica"	Test di stress, monitoraggio drift, logging output	Report test, log performance	⚠	Implementare allerta automatica
ISO/IEC 42001 — Annex A.7.3	Protezione dei dati personali	§3.3 "Privacy by Design"	DPO review, pseudonimizzazione dataset	DPIA, registro trattamenti	✓	—
Codice Etico Aziendale	Equità e non discriminazione	§2.4 "Fairness & Bias"	Dataset bilanciati, analisi fairness trimestrale	Report bias testing	✓	—

In estrema sintesi, la norma ci aiuta a:



Punto	Descrizione requisito	Cosa fare
A.6	Affidabilità e robustezza	Test di robustezza, procedure di fallback, controlli di qualità
A.7	Protezione dei dati e sicurezza	Misure tecniche e organizzative, analisi privacy, controlli sicurezza IT
A.8	Imparzialità e mitigazione dei bias	Analisi bias nei dataset, validazione etica, revisione indipendente
A.9	Coinvolgimento umano e controllo	Procedure human-in-the-loop, criteri di intervento umano
A.10	Conformità legale e normativa	Registro normative applicabili, valutazioni di conformità legale

L'AI Impact Assessment (AIIA) - struttura



5th Project
Management Forum
Lugano
October 13-14, 2025

- A. Informazioni generali**
- B. Descrizione del sistema di IA**
- C. Analisi del contesto (riferimento ISO/IEC 42001 — Cl. 4)**
- D. Classificazione del rischio (AI Act — Allegato III)**
- E. Analisi dell'impatto etico e sociale**
- F. Analisi dell'impatto sui diritti fondamentali**
- G. Gestione dei rischi (ISO/IEC 23894 integrata in 42001 — Cl. 8.2)**
- H. Supervisione e governance**
- I. Decisione finale e approvazione**
- J. Allegati**

Un esempio di un AIIA

1. Informazioni generali	
Voce	Descrizione
Titolo del sistema IA	Assistente virtuale per il supporto clienti "SmartCare AI"
Versione / Data	v1.0 — Ottobre 2025
Organizzazione responsabile	XYZ Assicurazioni SA
Unità / Reparto	Customer Service / Digital Innovation
Referente del progetto IA	Ing. Laura Rossi — Responsabile AI Governance
Ambito di applicazione	Gestione automatizzata delle richieste clienti via chat e email
Categorie di dati trattati	Dati anagrafici, di contatto, contrattuali e in parte sensibili (stato di salute in polizze sanitarie)
Normativa e standard di riferimento	ISO/IEC 42001:2023, ISO/IEC 23894:2023, GDPR, AI Act UE, LPD CH
2. Descrizione del sistema di IA	
Elemento	Dettagli
Tipo di IA	Modello linguistico (LLM) addestrato su base proprietaria e fine-tuned su dataset assicurativi interni
Finalità del sistema	Automatizzare l'assistenza clienti, migliorando tempi di risposta e coerenza delle informazioni
Livello di autonomia	Semi-autonomo (intervento umano in caso di incertezza o richiesta complessa)
Output generati	Testo naturale, suggerimenti di risposta, sintesi di richieste
Destinatari degli output	Clienti finali e operatori umani del contact center

3. Analisi del contesto (riferimento ISO/IEC 42001 — CL 4)	
Fattore	Analisi
Stakeholder principali	Clienti, operatori, responsabili IT, DPO, compliance officer
Aspettative delle parti interessate	Affidabilità, trasparenza, rispetto della privacy, facilità d'uso
Requisiti legali e normativi	Conformità all'AI Act (UE) e GDPR (EU) per sistemi ad alto rischio; norme ISO/IEC 42001 e ISO/IEC 23894 per sistemi ad alto rischio; norme ISO/IEC 27001 e ISO/IEC 27701 per la privacy e la sicurezza dei dati.
Ambiente operativo	Cloud privato europeo con gestione centralizzata dei modelli e dei dati.
4. Classificazione del rischio (AI Act — Allegato III)	
Categoria	Valutazione
Tipo di rischio AI Act	Alto rischio per i consumatori e per la sicurezza pubblica
Motivo	Può influenzare diritti dei consumatori o discriminare
Livello stimato di rischio	Medio-Alto
Misure di mitigazione previste	Supervisione umana, audit dei dataset, explainability logica, canale di revisione umana

Esempio di un AIIA



5. Analisi dell'impatto etico e sociale		
Area	Impatti potenziali	Misure di mitigazione
Trasparenza	Rischio di non comprensione da parte dell'utente che interagisce con una IA	Avvisi chiari "Stai parlando con un assistente virtuale"
Bias / Discriminazione	Rischio di bias su genere o lingua	Revisione periodica dei dataset e fairness testing trimestrale
Autonomia e controllo umano	Possibile eccessiva fiducia nella macchina	Supervisione continua da parte di operatori formati
Privacy e protezione dati	Trattamento improprio di dati sensibili	Minimizzazione, anonimizzazione e DSR (Data Subject Request) integrato
Sicurezza informatica	Attacchi prompt injection o data poisoning	Hardening del modello e controlli SOC 2 / ISO 27001

6. Analisi dell'impatto sui diritti fondamentali			
Diritto	Rischio	Livello	Misure
Privacy	Accesso improprio ai dati	Alto	Logging, crittografia end-to-end
Non discriminazione	Output potenzialmente distorti	Medio	Dataset bilanciato, controlli bias
Accesso equo ai servizi	Possibile esclusione di utenti con disabilità	Medio	Interfaccia compatibile con screen reader
Libertà di espressione	Rischio di censura automatica	Basso	Revisione manuale in casi dubbi

7. Gestione dei rischi (ISO/IEC 23894 integrata in 42001 — Cl. 8.2)			
Fase	Descrizione	Responsabile	Stato
Identificazione rischio	Rilevati 8 rischi principali	Team AI Governance	Concluso
Valutazione	Analisi qualitativa e quantitativa	Risk Officer	Concluso
Trattamento	Implementazione controlli mitiganti	IT Security & Compliance	In corso
Monitoraggio	Riesame trimestrale	Comitato etico IA	Programmato

Esempio di un AIIA



8. Supervisione e governance

Aspetto	Dettagli
Ruolo umano nel ciclo di vita del sistema	Revisione output, validazione decisioni critiche, aggiornamento modello
Formazione operatori	Modulo obbligatorio "Uso etico dell'IA e gestione bias"
Audit e riesame	Annuale, con check ISO/IEC 42001 Annex A (A.4 – A.10)
Registro attività IA	Tutte le interazioni tracciate e revisionabili per 24 mesi

9. Decisione finale e approvazione

Elemento	Contenuto
Valutazione complessiva dell'impatto	Rischio medio , accettabile con mitigazioni operative
Autorizzazione alla messa in esercizio	Concessa dal Comitato AI Governance il 30/09/2025
Condizioni	Riesame trimestrale e aggiornamento AIIA in caso di modifiche al modello
Firma del responsabile	Ing. Laura Rossi — 01/10/2025

10. Allegati

- A. Registro dei rischi IA
- B. Report bias testing
- C. Piano di formazione etica
- D. Registro incidenti e misure correttive
- E. Check di conformità Annex A ISO/IEC 42001



Open Projects

-
-
-
-

**Come utilizzare la norma nell'ambito
del project management**

Come utilizzare la ISO/IEC 42001:2023 nell'ambito del PM

Titolo del controllo	Processo / Area PM (ISO 21502)	Come soddisfare il controllo	Cosa implementare
AI Policy	Contesto e avvio del progetto	Una politica AI formalmente approvata e applicata ai progetti	AI Policy, verbali approvazione, comunicazioni interne, evidenze formazione
Alignment with Other Organizational Policies	Governance strategica	La Gestione dei progetti AI è coerente con le altre politiche aziendali (privacy, sicurezza, qualità)	Matrice di allineamento policy, riferimenti interni, verbali comitato
AI Roles and Responsibilities	Esecuzione e governance	Definire ruoli e responsabilità per la supervisione, sviluppo e uso dell'AI nei progetti	Organigramma AI, RACI matrix, procedure di delega
AI System Impact Assessment Process	Avvio e pianificazione	Condurre un AI Impact Assessment (AIIA) prima dell'implementazione dei sistemi AI di progetto	Modulo AIIA compilato, risk assessment, verbali di approvazione

Come utilizzare la ISO/IEC 42001:2023 nell'ambito del PM

Titolo del controllo	Processo / Area PM (ISO 21502)	Come soddisfare il controllo	Cosa implementare
AI System Verification and Validation	Pianificazione ed esecuzione	I sistemi AI utilizzati sono verificati e validati prima dell'uso operativo	Report di test, risultati backtesting, metriche di accuratezza, validazione QA
Data Quality for AI Systems	Pianificazione e controllo	Sono stabiliti criteri di qualità dei dati utilizzati dai sistemi AI	Procedure di data quality, log di verifica, audit trail, report di pulizia dati
System Documentation and Information for User	Tutte le fasi del progetto	Sono fornite documentazioni e istruzioni chiare agli utenti sui limiti e sull'uso del sistema AI	Manuale utente, policy d'uso, linee guida interne
Communication of Incidents	Monitoraggio e controllo	Esistono procedure per comunicare incidenti o malfunzionamenti dei sistemi AI nei progetti	Registro incidenti, piano di comunicazione, notifiche interne

Come utilizzare la ISO/IEC 42001:2023 nell'ambito del PM



5th Project
Management Forum
Lugano
October 13-14, 2025

Titolo del controllo	Processo / Area PM (ISO 21502)	Come soddisfare il controllo	Cosa implementare
Processes for Responsible Use of AI Systems	Esecuzione e controllo	Sono stati implementati processi per garantire un uso responsabile e controllato dei sistemi AI	Procedure operative, training, audit trail decisioni
Suppliers	Miglioramento continuo / PMO	I fornitori di soluzioni AI sono valutati secondo criteri etici, tecnici e di conformità	Contratti, checklist di vendor assessment, audit dei fornitori

5th Project Management Forum Lugano

Innovazione e Strategie nel Project Management

Applicazione della ISO/IEC 42001 ambito IA nel Project Management CONCLUSIONI

Maurilio Savoldi

October 13-14, 2025



- La norma ISO/IEC 42001 deve essere una guida per le organizzazioni per sfruttare la potenza dell'Intelligenza Artificiale.
- Le organizzazioni potranno utilizzare, ma anche promuovere, buone pratiche di implementazione dell'intelligenza artificiale:
 - a. responsabili,
 - b. etiche ed efficaci
 - c. per un uso responsabile e sostenibile.

Il sistema è certificabile?



- Sistema di Gestione dell'Intelligenza Artificiale (AI Management System, AIMS) è certificabile secondo la ISO/IEC 42001:2023.
- Al momento **il processo di accreditamento formale ISO/IEC 42001** presso gli organismi di accreditamento nazionali è **in corso di sviluppo**.
- Tuttavia, è possibile avere certificazioni "fuori accreditamento"





- Il valore della norma sta nella sua capacità di essere una guida, semplice ed universale, utile per chi sta inserendo elementi di AI nei propri progetti e/o nelle proprie organizzazioni.

Via Pascolet 41b – 6537 GRONO (GR)

Switzerland

+41 (0)91 840 22 97

info@svgrouppcert.ch

www.svcertification.com

Maurilio Savoldi

+ 39 389 237 34 47

+41 (0)76 812 13 09

msavoldi@svcert.ch

www.linkedin.com/in/maurilio-savoldi



SV Cert. Group

Organismo di Certificazione accreditato

Numero 661 del Registro SNAS