

ISO 42001

Checklist di Conformità



Contenuti

Introduzione	03	Allegato A Controlli (Ampliato)	
Clausola 4 – Contesto dell’azienda	04	A.2 – Politiche relative all’IA	11
Clausola 5 – Leadership	05	A.3 – Organizzazione interna	12
Clausola 6 – Pianificazione	06	A.4 – Risorse per sistemi di IA	13
Clausola 7 – Supporto	07	A.5 – Valutazione degli impatti dei sistemi di IA	14
Clausola 8 – Operatività	08	A.6 – Ciclo di vita del sistema di IA	15
Clausola 9 – Valutazione delle prestazioni	09	A.7 – Dati per sistemi di IA	16
Clausola 10 – Miglioramento	10	A.8 – Informazioni per le parti interessate	17
		A.9 – Utilizzo dei sistemi di IA	18
		A.10 – Relazioni con terze parti e clienti	19
		I nostri servizi ISO 42001	20
		Perché lavorare con noi?	21

Utilizza la nostra checklist e scopri se sei sufficientemente preparato per la certificazione.



Questa checklist di conformità ISO 42001 è uno strumento prezioso per aiutarti a valutare il tuo Sistema di Gestione dell'Intelligenza Artificiale (AIMS) e identificare eventuali aree che potrebbero richiedere attenzione prima della tua certificazione o audit di transizione.

Strutturata attorno alle clausole principali dell'ISO 42001, questa lista di controllo ti aiuterà a valutare se il tuo AIMS è allineato con i requisiti dello standard e i principi chiave della governance dell'IA. Copre:

- Il contesto della tua azienda
- Leadership e governance
- Identificazione dei rischi e valutazione dell'impatto
- Controlli operativi e di gestione dei dati
- Ciclo di vita, trasparenza e relazioni con terze parti

Utilizzando questa lista di controllo, puoi rivedere ogni requisito e inserire le tue risposte direttamente. Questo supporterà una comprensione più completa

Clausola 4 – Contesto dell’azienda

Comprendere lo scopo della tua azienda, il contesto interno ed esterno e le aspettative delle parti interessate è essenziale per stabilire un AIMS efficace. Questo pone le basi per l’ambito, gli obiettivi e la governance dei sistemi di IA.

Hai identificato problemi interni ed esterni rilevanti per i tuoi sistemi di IA?

Hai determinato le esigenze e le aspettative delle parti interessate?

L’ambito del tuo AIMS è chiaramente definito?

Il tuo AIMS è stabilito, implementato, mantenuto e continuamente migliorato?

Commenti

Clausola 5 – Leadership

La leadership gioca un ruolo fondamentale nello stabilire e supportare il Sistema di Gestione dell'IA. Il top management deve dimostrare impegno, allineare l'AIMS con la direzione strategica dell'azienda e assegnare responsabilità chiare.

Il top management ha dimostrato leadership e impegno verso l'AIMS?

Esiste una politica di IA stabilita allineata con la direzione strategica dell'azienda?

I ruoli, le responsabilità e le autorità per la gestione dell'IA sono assegnati e comunicati?

Commenti

Clausola 6 – Pianificazione

Una pianificazione efficace garantisce che i rischi e le opportunità relativi all'IA siano gestiti in modo proattivo. Ciò include la definizione degli obiettivi e la definizione di come la tua azienda soddisferà i requisiti dell'ISO 42001.

Sono state determinate le azioni per affrontare rischi e opportunità?

Esiste un processo per la valutazione e il trattamento dei rischi di IA?

Vengono condotte valutazioni di impatto dei sistemi di IA?

La valutazione dei rischi di IA è informata e allineata con la politica di IA e gli obiettivi di IA?

Sono selezionate opzioni di trattamento del rischio appropriate?

Sono stabiliti obiettivi di IA e piani per raggiungerli?

Commenti

Clausola 7 – Supporto

Il supporto copre le risorse, la competenza, la comunicazione e la documentazione necessarie per operare e migliorare l'AIMS. Garantire che i tuoi team siano informati, equipaggiati e supportati è essenziale per un'implementazione coerente.

Sono fornite le risorse necessarie per l'AIMS?

Esiste un processo per garantire che il personale sia competente sulla base di istruzione, formazione o esperienza?

Le persone che lavorano sotto il controllo dell'azienda sono consapevoli della politica di IA e delle procedure pertinenti?

La comunicazione interna ed esterna è determinata e implementata?

Le informazioni documentate richieste dall'AIMS e dall'ISO 42001 sono controllate?

Commenti

Clausola 8 – Operatività

La pianificazione operativa garantisce che i tuoi sistemi di IA siano sviluppati e utilizzati in linea con i processi definiti. Ciò include la gestione dei cambiamenti, la valutazione degli impatti e l'applicazione di trattamenti del rischio durante tutto il ciclo di vita del sistema.

I processi necessari per il funzionamento dei sistemi di IA sono pianificati, implementati e controllati?

Le valutazioni e i trattamenti dei rischi di IA sono integrati nei processi operativi?

Le valutazioni di impatto dei sistemi di IA sono mantenute e aggiornate se necessario?

Commenti

Clausola 9 – Valutazione delle prestazioni

Valutare le prestazioni del tuo AIMS aiuta a confermare se i processi sono efficaci e i risultati vengono raggiunti. Gli audit interni e le revisioni della direzione sono strumenti essenziali per guidare il miglioramento continuo.

Vengono condotti monitoraggio, misurazione, analisi e valutazione dell'AIMS?

Gli audit interni vengono eseguiti a intervalli pianificati?

La direzione rivede l'AIMS dell'azienda a intervalli pianificati?

Commenti

Clausola 10 – Miglioramento

Le non conformità e gli incidenti possono verificarsi – ciò che conta è come la tua azienda li identifica, li corregge e impara da essi. Un solido processo di miglioramento garantisce fiducia e efficacia sostenute del tuo AIMS.

Le opportunità di miglioramento sono determinate e implementate?

Le non conformità e le azioni correttive sono gestite efficacemente?

Commenti

Allegato A Controlli (Ampliato)

A.2 – Politiche relative all'IA

Per fornire una direzione chiara e stabilire le basi per un uso responsabile dell'IA, la tua azienda dovrebbe definire una politica che guidi lo sviluppo, l'implementazione e la supervisione dei sistemi di IA. Questa politica dovrebbe essere rivista regolarmente e allinearsi con i tuoi obiettivi aziendali, la propensione al rischio e gli obblighi legali.

Una politica di IA formale è stata documentata e approvata dal Top Management

La politica include principi per l'uso responsabile dell'IA e il miglioramento continuo

La politica viene rivista regolarmente per idoneità ed efficacia

La politica di IA si allinea e fa riferimento ad altre politiche organizzative pertinenti

Commenti

A.3 – Organizzazione interna

Per garantire responsabilità e chiarezza in tutto il sistema di gestione dell'IA, la tua azienda deve definire e comunicare ruoli, responsabilità e processi di escalation che supportino l'uso responsabile dell'IA durante tutto il ciclo di vita.

I ruoli e le responsabilità per i sistemi di IA sono chiaramente definiti e assegnati

Esiste un processo per segnalare preoccupazioni relative all'uso o allo sviluppo dell'IA

Le segnalazioni possono essere inoltrate in modo riservato, con garanzie contro eventuali ritorsioni

Il meccanismo di segnalazione prevede adeguate misure di indagine e risoluzione

Commenti

A.4 – Risorse per sistemi di IA

Comprendere la gamma completa di risorse utilizzate per supportare i tuoi sistemi di IA è essenziale per gestire il rischio. Questo include l'infrastruttura tecnica, i set di dati, gli strumenti e le capacità umane necessarie in ogni fase del ciclo di vita del sistema.

È stato creato un registro di tutte le risorse relative all'IA, inclusi dati, strumenti, sistemi e persone

Gli strumenti e le risorse informatiche sono documentati e adeguati ai requisiti di sistema

La competenza e la capacità delle risorse umane coinvolte nello sviluppo e nella supervisione dell'IA sono valutate e registrate

Gli impatti ambientali o operativi dell'infrastruttura sono considerati ove applicabile

Commenti

A.5 – Valutazione degli impatti dei sistemi di IA

Per salvaguardare gli individui e la società, la tua azienda deve valutare e documentare i potenziali impatti dei tuoi sistemi di IA. Queste valutazioni dovrebbero essere condotte in momenti chiave durante il ciclo di vita e dovrebbero guidare le decisioni di progettazione e trattamento del rischio.

Vengono eseguite valutazioni d’impatto per valutare gli effetti su individui, gruppi o società

Il processo per condurre valutazioni d’impatto è documentato e ripetibile

Le valutazioni d’impatto dei sistemi di IA vengono aggiornate dopo cambiamenti significativi o a intervalli pianificati

I risultati delle valutazioni informano la progettazione, i controlli e la comunicazione con le parti interessate

Commenti

A.6 – Ciclo di vita del sistema di IA

L'intero ciclo di vita del sistema di IA, dalla progettazione alla dismissione, deve essere supportato da requisiti, specifiche, validazione e processi di monitoraggio chiaramente definiti. Questi aiutano a garantire affidabilità continua e allineamento con l'uso previsto.

Gli obiettivi per lo sviluppo responsabile sono definiti e documentati

I processi di verifica e convalida sono specificati e collegati agli obiettivi organizzativi

La documentazione tecnica è disponibile per utenti, partner e regolatori

I log degli eventi sono registrati e mantenuti, specialmente durante l'uso del sistema

Commenti

A.7 – Dati per sistemi di IA

Dati di alta qualità, ottenuti eticamente e adeguatamente documentati sono fondamentali per sistemi di IA sicuri ed efficaci. La tua azienda dovrebbe definire criteri per selezionare, preparare e valutare i dati in ogni fase del ciclo di vita dell'IA.

Esiste un processo documentato di gestione dei dati per lo sviluppo dell'IA

Le fonti dei dati sono chiaramente identificate, con indicazione della provenienza e dell'uso previsto

I requisiti di qualità dei dati sono definiti e rivisti regolarmente

I metodi per la preparazione dei dati sono documentati e giustificati

Commenti

A.8 – Informazioni per le parti interessate

Le parti interessate – inclusi gli utenti del sistema e i regolatori – devono essere dotate delle informazioni necessarie per comprendere, utilizzare e valutare i sistemi di IA che gestisci. Questo supporta trasparenza, responsabilità e fiducia.

Agli utenti e alle altre parti interessate viene fornita la documentazione necessaria relativa al sistema

Esiste una procedura per fare escalation e segnalare agli organi superiori gli incidenti relativi all'IA

I piani di comunicazione degli incidenti sono documentati e periodicamente rivisti

I requisiti per informare gli stakeholder sono definiti e rispettati

Commenti

A.9 – Utilizzo dei sistemi di IA

La tua azienda deve garantire che i sistemi di IA siano utilizzati in modi che si allineano con le tue politiche, obiettivi e impegni etici. Ciò include chiarire i limiti di utilizzo, le responsabilità e i risultati previsti.

Esiste un processo definito per l'uso responsabile dei sistemi di IA

Sono stati fissati obiettivi per garantire che i sistemi di IA siano utilizzati eticamente e appropriatamente

L'utilizzo è in linea con lo scopo previsto e le procedure documentate

L'uso improprio o le conseguenze non intenzionali sono monitorati e affrontati

Commenti

A.10 – Relazioni con terze parti e clienti

Quando terze parti sono coinvolte in qualsiasi fase del ciclo di vita del sistema di IA, è necessario stabilire ruoli chiari, responsabilità condivise e aspettative allineate per garantire responsabilità continua e conformità.

Le responsabilità relative al ciclo di vita dell'IA sono chiaramente definite con le terze parti

Esiste un processo per la selezione e la gestione dei fornitori coinvolti nei sistemi di IA

Le aspettative dei clienti vengono raccolte e prese in considerazione nella progettazione e nel funzionamento del sistema

I ruoli delle terze parti sono rivisti come parte della governance continua del sistema

Commenti

I nostri servizi ISO 42001



Formazione

Costruisci la tua conoscenza dell'ISO 42001 con una gamma di corsi progettati per diversi livelli di esperienza – forniti attraverso diversi stili di apprendimento.



Gap analysis

Un servizio opzionale in cui uno dei nostri auditor esperti ti aiuterà a identificare eventuali aree critiche, ad alto rischio o deboli del tuo sistema prima della certificazione.



Certificazione

Valutiamo il tuo AIMS in linea con i requisiti dell'ISO 42001 – con particolare attenzione ai controlli dell'Allegato A e a come impattano sul tuo sistema.



Valutazioni integrate

Se hai implementato più sistemi di gestione, potresti beneficiare di un programma di audit e sorveglianza integrato – un modo più efficiente ed economico per gestire il rischio.

Perché lavorare con noi?

In LRQA, aiutiamo le aziende a sviluppare programmi di gestione del rischio robusti e pronti per il futuro che consentono l'adozione sicura, responsabile ed efficace dell'IA e della tecnologia.

Dall'assicurare la conformità con le normative IA in evoluzione al rafforzamento della sicurezza dei dati e all'incorporamento delle migliori pratiche nella governance, forniamo la garanzia necessaria per guidare l'innovazione con fiducia – aiutando le aziende a integrare l'IA e la tecnologia gestendo proattivamente i rischi.

Competenza sul campo

Le nostre soluzioni sono fornite da un team globale di esperti specializzati in cybersecurity, conformità e gestione del rischio della catena di approvvigionamento, aiutandoti a navigare i rischi legati all'IA, soddisfare i requisiti normativi in evoluzione e integrare pratiche di IA responsabili nelle tue operazioni.

Garanzia continua

I rischi guidati dall'IA richiedono una supervisione continua. Il nostro approccio alla gestione del rischio in tempo reale consente la risoluzione proattiva dei problemi, riducendo l'interruzione del business e migliorando la resilienza. Il nostro portfolio connesso di soluzioni di gestione del rischio aiuta le aziende ad andare oltre i requisiti normativi e incorporare la gestione del rischio dell'IA nelle operazioni quotidiane.

Partnership basate su soluzioni

Non ci limitiamo a certificare – lavoriamo al tuo fianco per integrare la governance dell'IA nella tua più ampia strategia di rischio e conformità. Il nostro approccio su misura garantisce che l'IA e la tecnologia aiutino a guidare una crescita sostenibile soddisfacendo le aspettative legali ed etiche in evoluzione.

Processo decisionale basato sui dati

Sfruttiamo piattaforme digitali e analisi per fornire approfondimenti più profondi sui rischi dell'IA in tutta la tua azienda. La nostra intelligenza umana, potenziata da strumenti basati sui dati, aiuta le aziende a identificare vulnerabilità, prevedere rischi futuri e prendere decisioni informate con fiducia.



Su LRQA

LRQA è il principale partner globale di assurance, che riunisce decenni di esperienza ineguagliabile nei servizi di valutazione, supporto tecnico, ispezione e cybersecurity.

Le nostre partnership basate su soluzioni sono supportate da approfondimenti basati sui dati che aiutano i nostri clienti a risolvere le loro più grandi sfide aziendali. Operando in più di 150 paesi con un team di oltre 5.000 persone, i nostri specialisti premiati in conformità, catena di approvvigionamento, cybersecurity ed ESG aiutano più di 61.000 clienti in quasi tutti i settori ad anticipare, mitigare e gestire il rischio ovunque operino.

In tutto ciò che facciamo, siamo impegnati a plasmare un futuro migliore per la nostra gente, i nostri clienti, le nostre comunità e il nostro pianeta.

Contattaci

Visita lrqa.com/it-it per maggiori informazioni o invia un'email a certificazione@lrqa.com



LRQA
Milan
Viale Monza
259/265, Milan,
Italy 20126
+39 02 30551200