Massimiliano Bellavista

AI COMPLIANCE E CERTIFICAZIONE

La norma ISO 42001:2023 e i vantaggi della certificazione dell'AI compliance

FrancoAngeli

Massimiliano Bellavista

AI COMPLIANCE E CERTIFICAZIONE

La norma ISO 42001:2023 e i vantaggi della certificazione dell'AI compliance

FrancoAngeli

ISBN: 9788835183129

Indice

Prefazione

di *Alessandro Ventimiglia*

È con grande piacere e sincero riconoscimento del valore di questo lavoro che introduco il presente volume dedicato alla norma UNI CEI ISO/IEC 42001:2024, un punto di svolta nel panorama della normazione internazionale. L'intelligenza artificiale (IA) non è più soltanto una tecnologia abilitante ma è una componente critica dell'infrastruttura organizzativa e decisionale di aziende, enti pubblici e istituzioni. La sua pervasività ha superato i confini della ricerca e dell'innovazione per entrare, in modo profondo e spesso silenzioso, nei meccanismi quotidiani della società e dell'economia.

Le applicazioni dell'IA oggi spaziano dalla sanità alla finanza, dalla pubblica amministrazione alla produzione industriale, dalla mobilità urbana ai servizi educativi e culturali. Questo diffuso radicamento dell'IA solleva interrogativi cruciali in termini di responsabilità, trasparenza, sicurezza, protezione dei dati, sostenibilità e impatti sulle persone e sull'ambiente. È dunque evidente la necessità, non più rinviabile, di un quadro sistemico che consenta alle organizzazioni di gestire l'IA in modo strutturato, documentato e verificabile.

In tale contesto, la norma ISO/IEC 42001 rappresenta il primo tentativo compiuto, su scala globale, di costruire un Sistema di Gestione per l'Intelligenza Artificiale (AIMS). Pur collocandosi nel filone delle norme basate sulla High Level Structure (HLS), essa ne amplia significativamente l'impianto attraverso l'introduzione di strumenti specifici e innovativi. Gli allegati A, B e D forniscono un livello di dettaglio applicativo senza precedenti: il primo identifica obiettivi e controlli specifici per l'IA; il secondo ne guida l'implementazione pratica; il terzo classifica le aree tecniche in cui l'IA può essere adottata, offrendo così un modello scalabile, modulare e adattabile a diversi contesti organizzativi.

Il volume che avete tra le mani nasce da un'esperienza concreta, alimentata dalla conoscenza profonda dell'autore e dalla sua capacità di tradurre i requisiti della norma in indicazioni operative chiare, pratiche e contestualizzate. Si rivolge a una platea ampia: responsabili IT, progettisti, data scientist, auditor, consulenti, formatori e decisori strategici. Chiunque sia coinvolto nella progettazione, sviluppo, valutazione o governo dei sistemi IA potrà trovare in questo testo una guida affidabile e autorevole.

La capacità dell'autore di accompagnare il lettore nei passaggi più critici dell'AIMS è particolarmente rilevante oggi, quando molte organizzazioni si interrogano su come affrontare l'adozione della norma in modo efficace e sostenibile. La scelta di concentrare l'implementazione iniziale sugli ambiti applicativi più critici, dal punto di vista normativo, etico, economico o reputazionale, rappresenta una raccomandazione strategica, utile per evitare approcci dispersivi, progetti eccessivamente onerosi o implementazioni inefficaci.

Attualmente sono disponibili numerose pubblicazioni dedicate all'intelligenza artificiale, molte delle quali analizzano gli aspetti tecnici, etici o normativi del fenomeno. Tuttavia, questo libro si distingue perché nasce dall'esperienza diretta di chi ha un ruolo attivo nell'implementazione e nella verifica dei sistemi di gestione per l'intelligenza artificiale. Oltre a colmare un vuoto nell'attuale letteratura tecnica, contribuisce in modo significativo alla crescita della maturità organizzativa nel campo dell'IA, legittima la norma stessa, ne evidenzia la portata e l'utilità, e mette a disposizione strumenti concreti per affrontare il cambiamento in corso con competenza e consapevolezza.

Buona lettura.

I.
Analisi ragionata della norma e degli aspetti salienti

1.1. Una premessa

Quanto segue è un commento dello Standard UNI CEI ISO/IEC 42001:2024, che si contraddistingue per i seguenti aspetti salienti, la seguente struttura (e le collegate avvertenze):

1. a fronte di quel che la Norma di riferimento riporta, si forniscono indicazioni di carattere pratico, ovvero esattamente quelle con cui ci si è confrontati durante la creazione di un Sistema conforme a ISO 42001.Tali indicazioni non pretendono di essere esaustive, ma sono certamente il frutto di prime concrete e sostanzialmente efficaci esperienze applicative;
2. si raccomanda in ogni caso di acquistare e leggere attentamente lo Standard, perché è ricchissimo di note e suggerimenti su cui è prezioso ragionare durante l'implementazione del Sistema; questo manuale va letto avendo sempre disponibile il riferimento al testo ufficiale dello Standard;
3. in tutta l'analisi e anche nella seconda parte, quella legata all'analisi dell'Appendice 'A', si è cercato di mettere in rilievo le interrelazioni tra i vari punti in cui lo Standard è articolato, di evidenziare come metterne al meglio a frutto le potenzialità e, attraverso dei semplici schemi, si sono voluti mettere in evidenza tutti quei documenti fondamentali da produrre che consentono di strutturare il sistema. In ultimo, si è cercato di collegare lo Standard con i requisiti e i documenti di riferimento caratteristici dei Sistemi basati su ISO 27001:2022 e 9001:2015, poiché chi scrive ritiene che la norma ISO 42001 possa

fornire le sue migliori prestazioni nell'ambito di un sistema integrato di questo tipo (almeno con ISO 27001);

4. il caso che completa il volume è il primo caso applicativo in Italia che è giunto fino al completamento della fase certificativa. Come tale è una assoluta primizia e costituisce un valido e prezioso riferimento per tutti coloro che saranno intenzionati ad applicare lo Standard ISO 42001.

1.2. Analisi della sezione 4: contesto dell'organizzazione

Cosa dice la norma

I punti da considerare sono i seguenti:

- 4.1. Comprendere l'organizzazione e il suo contesto

L'organizzazione deve in sostanza individuare e mappare tutti quei fattori esterni e interni al suo perimetro organizzativo che sono rilevanti per le sue finalità e che possano influire significativamente sulla sua capacità di raggiungere gli stessi scopi che si è prefissa implementando il proprio sistema di gestione dell'IA.

- 4.2. Comprendere le esigenze e le aspettative delle parti interessate

L'organizzazione deve individuare gli *stakeholder* rilevanti per il sistema di gestione dell'IA e quali siano le regole di ingaggio e gestione dei rapporti con gli stessi.

- 4.3. Determinazione del campo di applicazione del sistema di gestione dell'IA

L'organizzazione deve determinare in modo puntuale il perimetro e il campo di applicazione del proprio Sistema di gestione.

- 4.4. Sistema di gestione dell'IA

Lo Standard stabilisce che l'organizzazione deve impegnarsi concretamente a gestire, controllare, migliorare in modo continuo e documentare il sistema di gestione dell'IA, ivi compresi i suoi processi.

Indicazioni pratiche

Questo insieme di punti nasconde le insidie iniziali più rilevanti.

Comprendere quali siano esattamente le motivazioni e le finalità di implementazione di un sistema di gestione come quello per l'IA non è scontato.

Esattamente con non esiste in letteratura (e anche in ambito normativo, basti vedere le differenze a riguardo tra le varie normative internazionali) una definizione unica di AI, non può esistere un approccio unico alla definizione di un Sistema di gestione per l'IA basato sullo Standard ISO 42001.

Da un lato vi possono essere l'input e la criticità di una o più esigenze progettuali immediate, da un altro l'esigenza di gestire e regolamentare in un medio periodo e in un'ottica strategica l'approccio all'AI da parte delle proprie risorse e collaboratori.

Non è quindi solo un problema di definizione dell'ambiente e del contesto competitivo in cui si situa l'uso dell'AI, ma in primis, la definizione del proprio ruolo e posizionamento in relazione a questa componente. Date le difficoltà di carattere tecnico e tecnologico e gli investimenti in gioco, non può che trattarsi di un'analisi di contesto orientata almeno sul medio periodo. L'organizzazione può a seconda dei casi giocare uno o più tra questi ruoli:

- integratore di componenti AI;
- cliente/utente di sistemi AI;
- produttrice/sviluppatrice di soluzioni AI;
- fornitrice di dati.

In relazione al proprio o ai propri ruoli, vi sono accurate indagini da fare per definire il contesto.

Ovvio e scontato che il proprio contesto interno, fatto di componenti di governance, organizzative e infrastrutturali, è pesantemente influenzato da variabili esterne che sono solo parzialmente sotto il controllo dell'azienda. È infatti possibile compiere scelte di carattere tecnologico, procedurale e infrastrutturale che ricadono sotto il proprio controllo, ma vi sono aspetti di carattere macroeconomico e normativo cui invece si può solo adattarsi.

Vi sono quindi nel contesto AI, molte variabili da considerare su alcune specifiche categorie di stakeholder tra cui, eminentemente:

- fornitori;
- clienti;
- shareholder;
- autorità di controllo.

Si consiglia un approccio strutturato e supportato da una univoca metodologia (es. redigere preliminarmente un'accurata SWOT ANALYSIS) all'analisi di contesto, un approccio non meramente descrittivo ma analitico e propositivo, che consenta di fissare con attenzione gli aspetti di forza e debolezza, le opportunità e i rischi almeno nei seguenti ambiti:

- normativo/regolamentare (generale e di settore);
- contrattuale;
- tecnologico;
- finanziario;
- valoriale e reputazionale.

Cercando con questo sforzo di comprendere:

- l'atteggiamento degli stakeholder,
- il comportamento dei competitor;
- le aspettative dei portatori d'interesse;
- le modalità più favorevoli di ingaggio, consultazione e comunicazione con gli stessi.

Per quanto riguarda i fornitori, occorre un'attenta analisi del loro posizionamento riguardo all'IA (non solo tecnologico, ma proprio di approccio anche valoriale al tema, onde valutarne la compatibilità col proprio), e un'accurata analisi dei rapporti contrattuali vigenti/da integrare. È chiaro che servono uno screening e una valutazione specifici e accurati, non essendo sufficienti quelli richiesti dagli altri Standard.

Per i clienti, i cui dati potrebbero essere messi a rischio da una non efficace gestione dell'IA, è necessario comprenderne le aspettative, i valori e anche le percezioni rispetto ad un tema ancora così poco conosciuto e approfondito come quello dell'AI. Questo spinge quasi inevitabilmente verso la creazione di rapporti solidi, trasparenti e di medio/lungo periodo, necessari per mettere in luce, anche su un piano formativo e 'culturale' i vantaggi derivanti dall'IA, e dall'altro lato razionalizzare e relativizzare le percezioni dei rischi intrinsechi. Possono essere utili in tal senso anche delle *survey* preliminari presso campioni di clienti opportunamente selezionati.

Gli azionisti dovranno essere opportunamente informati e tenuti in considerazione con trasparenza per gli impatti che un posizionamento deciso dell'organizzazione in tema di intelligenza artificiale potrebbe

avere sui loro investimenti, ma anche e reciprocamente, per valutare le connessioni e sovrapposizioni ed evitare difformità con le strategie adottate parallelamente o in passato nell'ambito del loro portafoglio di investimenti.

Il monitoraggio costante delle attività e il contatto con le autorità di controllo e più in generale gli attori del contesto regolamentare, in un periodo di intensa e a tratti anche compulsiva attività di emissione di normative e regolamenti in tema IA, sono fondamentali per gestire gli impatti di autorizzazioni, accreditamenti e attività di audit e ispezione.

In ultimo, utile considerare il comportamento dei competitor e le loro scelte di posizionamento riguardo al tema in esame. Imparare da casi di successo ed eventualmente errori precedenti può essere utile. L'impressione generale infatti è che in questa fase sia quanto mai necessario un modello progettuale (e organizzativo) resiliente, cioè basato su metodologie e infrastrutture in grado di poter modificare anche rapidamente l'approccio a determinate soluzioni tecnologiche in ragione del rapidissimo sviluppo delle prestazioni dei Sistemi di IA.

Quanto allo scopo certificativo, valgono in sostanza le considerazioni che si fanno abitualmente in sede di implementazione di un sistema di gestione. Lo scopo può quindi essere complessivo, ovvero comprendere l'intera organizzazione, o invece messo in rapporto:

- a singoli processi e *business unit*;
- a singoli servizi;
- a specifiche sedi.

Tuttavia, dati la pervasività della tecnologia basata sull'IA e i costi iniziali connessi all'implementazione di un Sistema di gestione fondato su ISO 42001, è consigliabile non parcellizzare troppo l'ambito di applicazione, o comunque arrivare gradualmente a comprendere l'intero contesto aziendale.

Una nota importante merita il percorso e il posizionamento valoriale in tema di IA che l'organizzazione deve compiere implementando il Sistema di Gestione. I valori da soli non bastano, vanno tradotti in requisiti concreti. Si rimanda ad esempio a quanto ottimamente elaborato dal *Gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale* istituito dalla Commissione europea nel giugno 2018 (cfr. documento *Orientamenti etici per un'IA affidabile*).

I principi elaborati dal Gruppo, ovvero:

i) rispetto dell'autonomia umana;
ii) prevenzione dei danni;
iii) equità;
iv) esplicabilità;

e la loro traduzione in requisiti e cioè:

1. *Intervento e sorveglianza umani* – Inclusi i diritti fondamentali, l'intervento umano e la sorveglianza umana.
2. *Robustezza tecnica e sicurezza* – Inclusi la resilienza agli attacchi e la sicurezza, il piano di emergenza e la sicurezza generale, la precisione, l'affidabilità e la riproducibilità.
3. *Riservatezza e governance dei dati* – Inclusi il rispetto della riservatezza, la qualità e l'integrità dei dati e l'accesso ai dati.
4. *Trasparenza* – Incluse la tracciabilità, la spiegabilità e la comunicazione.
5. *Diversità, non discriminazione ed equità* – Incluse la prevenzione di distorsioni inique, l'accessibilità e la progettazione universale, e la partecipazione dei portatori di interessi.
6. *Benessere sociale e ambientale* – Inclusi la sostenibilità e il rispetto ambientale, l'impatto sociale, la società e la democrazia.
7. *Accountability* – Inclusi la verificabilità, la riduzione al minimo degli effetti negativi e la loro segnalazione, i compromessi e i ricorsi.

Dovrebbero costituire le basi per la composizione e personalizzazione del/ei propri orientamenti valoriali e animare tutto il ciclo di vita (vedi punti successivi 6.1.3 e 8.1).

Utile che l'organizzazione e il suo management si confrontino al loro interno e con i portatori di interesse esterni e che studino bene le fonti più autorevoli in tema di etica dell'IA ed etica d'impresa. La gestione di una Sistema di IA si basa sicuramente su un posizionamento etico altrettanto forte di quello tecnologico.

Giova riflettere su alcuni elementi. Il primo è proprio il contesto in cui questi orientamenti sopra riepilogati (e che costituiscono il substrato su cui è maturato l'*AI Act*, il Regolamento europeo sull'IA, che è entrato in vigore nell'agosto 2024) sono maturati. Il concetto di *trustworthness* viene, anche giustamente, tradotto in italiano con il concetto di 'affida-

bilità'. Questo concetto tuttavia rischia di ridurre la portata della parola ad un aspetto tecnico e un po' meccanico, quando in realtà dietro vi è molto di più. Attiene alla capacità da parte della progettualità aziendale, di *generare fiducia* presso tutti gli stakeholder, attraverso un serio e robusto posizionamento etico e il rispetto rigoroso e comprovabile delle prescrizioni etiche, a cominciare naturalmente dal GDPR e dall'*AI Act*.

Un altro elemento che è trasversale a tutti i principi e portatori di interesse e che dovrebbe pertanto animare gli sforzi aziendali data la sua importanza è il partire sempre dalla *centralità della persona.*

Significa in pratica che ogni azione, ogni principio in tema di IA in caso di dubbio o conflitto (è possibile infatti che i principi sopra esposti generino tensioni e conflitti al confine tra aspetti di business, scelte economiche e strategiche e richieste e interessi specifici degli stakeholder) debba sempre ricadere nella scelta che massimizza l'idea che tale tecnologia rappresenta un mezzo e non un fine, un mezzo che rimane al servizio dell'uomo e della collettività umana, Come tale, non deve arrecare danno ma beneficio, e deve favorire la giustizia sociale, l'equità di trattamento e l'inclusione, ed essere sostenibile e spiegabile/comprensibile (per quanto possibile) ai propri utenti e anche a chi ne può essere impattato indirettamente.

È bene tenere in mente che i sistemi di cui trattiamo possono provocare anche gravi danni, e non sempre di facile lettura e immediata interpretabilità.

1.3. Analisi della sezione 5: leadership

Cosa dice la norma

I punti in gioco sono i seguenti:

- 5.1. Leadership e impegno

Questo punto descrive accuratamente l'impegno e la capacità di *leadership* che l'alta direzione deve dimostrare a riguardo del sistema di gestione dell'IA.

- 5.2. Politica

Come in ogni Sistema di gestione l'alta direzione deve stabilire una politica di IA formalmente documentata, solida, efficace da comunicare alle parti interessate, appropriata alla finalità per cui si implementa il Sistema e improntata al miglioramento.

• 5.3. Ruoli, responsabilità e autorità

Il management dell'organizzazione deve assicurare che le responsabilità e le autorità relative ai ruoli rilevanti entro il Sistema di gestione siano puntualmente assegnate e comunicate.

Indicazioni pratiche

Quanto alla leadership le parole chiave sono almeno due:

- promozione;
- sensibilizzazione.

Quindi è necessario che le attività inerenti siano ben documentate e suffragate da appositi piani di approccio. In pratica occorre stabilire cosa e come:

- il management comunica all'interno della propria organizzazione riguardo all'importanza e la rilevanza dei requisiti dello Standard;
- con quali strumenti e procedure documentate questo avviene (informazione/formazione, ad esempio attraverso momenti anche informali ma comunque pianificati/strutturati di condivisione con le risorse interne e i collaboratori). È del tutto evidente quanto questo requisito sia importante, se solo si riflette sulle crescenti responsabilità che gravano sul management in merito ad un cattivo uso dell'AI e al sostanziale vuoto regolamentare in merito (ad un livello elementare ma già fonte di notevoli danni reputazionali ed economici per alcune imprese si pensi al tema dell'impiego dell'AI nella redazione di documenti, relazioni e altro). Utile insomma poter documentare come ci si è proposti di regolamentare l'uso degli strumenti di AI e come ci si è accertati che i valori e le soluzioni proposte siano state adeguatamente condivisi con tutti gli interessati. E da essi compresi.

La politica (o meglio le politiche) di un Sistema di gestione dell'IA dovrebbero rispondere a criteri di buon senso ed efficacia che sono comuni a tutti gli Standard ISO.

In particolare i seguenti:

- appropriatezza. La Politica dovrebbe riflettere il sistema e il contesto valoriale dell'organizzazione, e farvi esplicito riferimento. Non deve

risultare un corpo estraneo alla cultura dell'organizzazione né tantomeno un testo-standard, magari desunto da altri contesti senza un più che adeguato grado di personalizzazione;
- leggibilità (comunicabilità). Si tratta di un documento per sua natura estremamente diffuso a tutte le categorie di stakeholder. Quindi in ultima analisi dovrebbe essere redatto da figure, interne o esterne all'aziende, consapevoli delle regole e delle tecniche base di comunicazione;
- credibilità. Questo punto attiene alla chiara indicazione di concreti obiettivi attinenti al Sistema di Gestione per l'IA o perlomeno ad una consistente descrizione delle modalità di come e chi all'interno dell'organizzazione definisce, implementa, monitora e documenta gli obiettivi di gestione e di miglioramento (e con quali logiche e strumenti);
- accessibilità. La politica dovrebbe essere un documento ben diffuso e facilmente reperibile attraverso i canali istituzionali aziendali (web, social, etc);
- progettazione in modalità, per così dire, '*stakeholder by design'*. È fondamentale, infatti, che a priori il management abbia individuato chi sono i portatori di interesse che si intendono coinvolgere nel Sistema di Gestione, perché occorre tener conto del loro contesto per definire e indirizzare i contenuti della Politica in modo comprensibile e efficace.

Utile che sia l'organizzazione stessa a stabilire senza preconcetti se:

- formulare una sola politica;
- formulare un set di politiche collegate tra di loro (ad esempio sul ciclo di vita, sulle attività di *testing* e/o di gestione dei dati, etc);
- integrare o meno la politica in merito all'IA con politiche già presenti in azienda (es le politiche in ambito ISO 27001:2022 o ISO 22301:2019 o ISO 9001:2015).

Dovendo dare un suggerimento legato alle prime esperienze, l'opzione di redigere un corpo di politiche piuttosto che una sola, omnicomprensiva, sembra essere una scelta efficace anche sul piano della comunicazione interna.

In merito alla definizione ruoli e alle responsabilità in seno ad un Sistema ISO 42001, si rilevano almeno tre piani di lettura cui il management dovrebbe prestare debita attenzione:

- quello inerente alla formulazione e la formalizzazione (tramite apposite nomine posizionali, cioè legate automaticamente all'occupare determinati ruoli organizzativi o invece ad personam cioè nominative) di opportuni organigrammi, funzionigrammi e mansionari che inquadrino dettagliatamente i ruoli specificatamente connessi ai processi IA, come ad esempio la figura del Responsabile per la Gestione e i suoi eventuali collaboratori;
- quello assai più complesso delle figure che, pur non avendo responsabilità dirette, sono fortemente collegati ai processi di gestione e monitoraggio del Sistema e in relazione ai quali si potrebbero dover opportunamente integrare le *job description* e/o le linee di reporting già presenti in azienda, quali ad esempio:
  1. gli *owner* di particolari categorie di dati e informazioni;
  2. gli *owner* di specifici processi e *tool* (ad esempio in ambito ICT, HR, amministrazione, *procurement*);
  3. i *project manager* dei progetti impattati dall'IA;
  4. i *risk manager*;
  5. gli *asset owner* (dove la parola include anche gli asset immateriali);
- per ultimo il piano inerente ruoli e responsabilità attribuiti all'esterno (fornitori, outsourcer, collaboratori, esperti) la cui definizione attiene ad una attenta integrazione dei dispositivi contrattuali già eventualmente disponibili.

Scrivere una efficace politica del Sistema di Gestione ISO 42001 dovrebbe implicare la redazione di un documento comprensivo almeno dei seguenti punti e avvertenza pratiche:

- la dichiarazione del campo di applicazione e impegno in relazione allo scopo certificativo;
- l'esposizione sintetica del contesto e della visione aziendale in termini di AI, il suo posizionamento attuale e a tendere;
- l'enunciazione (chiara) dell'impegno del top management sul tema. Questa parola, 'impegno' è una delle più banalizzate e fraintese del linguaggio della qualità, ma per essere seriamente applicata non dovrebbe corrispondere solo a frasi che iniziano con verbi 'crediamo', 'riteniamo' o 'pensiamo', ma piuttosto a frasi che esprimano, con riferimenti a fatti, linee guida e investimenti materiali o immateriali le concrete azioni intraprese e da realizzare nel medio e breve periodo,

nonché specifiche linee d'indirizzo e 'messaggi' a tutti gli stakeholder impattati.
- l'affermazione di valori e principi, di alto livello e generale, ma ben collegata anche da altri documenti aziendali come carta dei valori, codice etico, ecc. e/o il collegamento a riferimenti costituiti da linee guida internazionali, nazionali ed eventualmente di settore di particolare impatto per l'organizzazione;
- il raccordo con le tematiche ESG, visto ad esempio il ruolo duale dell'intelligenza artificiale, da un lato come agevolatrice di soluzioni innovative, dall'altro come strumento energivoro, stante l'elevato consumo di risorse energetiche e materiali richieste da queste tecnologie;
- le regole e le responsabilità per la sua diffusione, comunicazione e periodica revisione. Quanto mai opportuno mettere in atto concretamente questo punto a parere di chi scrive: visto e considerato che si è in presenza di un settore in rapidissima evoluzione una politica statica e immodificata per più di un anno pare davvero assai poco credibile.

1.4. Analisi della sezione 6: pianificazione

Cosa dice la norma

I punti in esame sono i seguenti:

- 6.1. Azioni per affrontare rischi e opportunità
- *6.1.1. Generalità*

L'organizzazione deve impostare un consistente progetto di analisi e mappatura dei rischi e stabilire adeguati criteri in relazione all'IA che le indichino chiaramente la distinzione tra rischi accettabili e rischi non accettabili. Deve inoltre poter impostare correttamente le fasi di valutazione, trattamento e valutazione degli impatti del rischio.

- *6.1.2. Valutazione del rischio dell'IA*

L'organizzazione deve in sostanza operare con coerenza individuando un sistema di valutazione del rischio efficace, in grado di fornire risultati coerenti, validi e comparabili. Sulla base di questi risultati le deve poi essere possibile confrontare e comparare gli impatti e stabilire le priorità di mitigazione dei rischi. I risultati di questo processo devono essere sempre adeguatamente documentati.