



UNIMORE

UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

**Università degli Studi di Modena e Reggio Emilia
Dipartimento di Scienze e Metodi dell'Ingegneria**

**Corso di Laurea Magistrale in
Ingegneria Gestionale**

A.A. 2025/2026

**Dalla conformità normativa all'AI governance:
sviluppo e applicazione di un modello operativo
per l'adeguamento all'AI Act**

Relatore:
Prof. Franco Francia

Laureando:
Giuseppe Raucci
Matricola n. 206339

*«Nel cuore dell'inverno,
imparavo finalmente che vi era in me
un'estate invincibile.»*

ALBERT CAMUS

Indice

Elenco delle figure	iv
Elenco delle tabelle	v
Sommario	vi
Introduzione	1
1 Dall'AI Act all'AI governance aziendale	3
1.1 L'intelligenza artificiale nel contesto organizzativo	3
1.2 Il quadro normativo europeo sull'intelligenza artificiale	5
1.3 L'approccio basato sul rischio	7
1.4 Ruoli regolatori e scenari applicativi	10
1.5 Gli obblighi lungo il ciclo di vita dei sistemi di IA	12
1.6 AI risk management e AI governance	15
1.7 Standard e framework di riferimento	17
1.8 Dalla conformità normativa al modello operativo	19
2 Progettazione del modello operativo di AI governance	21
2.1 Dalla normativa ai requisiti operativi	22
2.2 Censimento e identificazione dei sistemi di IA	24
2.3 Classificazione del rischio e determinazione del ruolo regolatorio .	26
2.4 L'AI Lifecycle: fasi, attività e responsabilità	29
2.5 Progettazione del modello organizzativo di AI governance	32
2.5.1 Ruoli, responsabilità e organi di governance	33
2.5.2 La governance a livello di gruppo	37
2.5.3 Confronto qualitativo delle configurazioni organizzative . .	38
2.5.4 Il modello ibrido come configurazione in valutazione	40
2.5.5 Coordinamento tra livello centrale e realtà estere	41
2.6 Integrazione delle componenti nel modello operativo	43
3 Implementazione operativa del modello di AI governance e sviluppo degli strumenti di valutazione	46
3.1 Dall'architettura del modello alla sua implementazione operativa .	47
3.2 Formalizzazione dell'AI Lifecycle	48
3.2.1 Obiettivi e funzione della procedura	48
3.2.2 Fasi comuni: dal bisogno al registro e alla selezione dei controlli	48
3.2.3 Differenziazione dei percorsi per rischio e ruolo regolatorio	49
3.2.4 Percorso dei sistemi ad alto rischio in qualità di fornitore .	51
3.2.5 Percorso dei sistemi ad alto rischio utilizzati in qualità di deployer	52
3.2.6 Attività tecniche e di monitoraggio lungo il ciclo di vita . .	53

3.3	Sviluppo e aggiornamento dell'AI Policy e raccordo con il modello operativo	54
3.3.1	Finalità, perimetro e natura evolutiva	54
3.3.2	Principi generali e regole di utilizzo	55
3.3.3	Gestione dei nuovi casi d'uso e collegamento con l'AI Lifecycle	56
3.3.4	Ruoli, monitoraggio e aggiornamento	56
3.4	Sviluppo del TAF e del sistema dei controlli	57
3.4.1	Finalità e architettura del framework	57
3.4.2	Applicabilità dei controlli in funzione di rischio e ruolo . .	59
3.4.3	Dal requisito al controllo verificabile	60
3.4.4	Valutazione dello stato di attuazione	61
3.4.5	Affinamento del framework attraverso l'applicazione	61
3.5	Formalizzazione documentale degli adempimenti	62
3.5.1	La documentazione come componente del controllo	62
3.5.2	Documentazione dei sistemi ad alto rischio in qualità di fornitore	62
3.5.3	Documentazione dei sistemi ad alto rischio utilizzati in qualità di deployer	63
3.6	Analisi degli scostamenti e avvio delle azioni di adeguamento . . .	64
3.6.1	Dall'autovalutazione all'individuazione degli scostamenti .	64
3.6.2	Qualificazione dello scostamento	64
3.6.3	Definizione delle azioni di adeguamento	65
3.6.4	Primo ciclo di applicazione e stato di avanzamento	65
3.6.5	Monitoraggio delle azioni nel tempo	66
3.7	Predisposizione del Risk Assessment per i sistemi di IA ad alto rischio	67
3.7.1	Finalità, perimetro e collegamento con il sistema di gestione del rischio	67
3.7.2	Definizione dei pillar e delle minacce	69
3.7.3	Questionario e valutazione del rischio intrinseco	69
3.7.4	Valutazione delle misure compensative	70
3.7.5	Determinazione del rischio residuo	71
3.7.6	Trattamento del rischio e monitoraggio	72
3.7.7	Ruoli, strumento operativo e stato di avanzamento	73
3.8	Predisposizione della metodologia per la FRIA	74
3.8.1	Finalità e perimetro di applicazione	74
3.8.2	Governance della valutazione	75
3.8.3	Definizione dell'insieme dei diritti fondamentali	76
3.8.4	Contestualizzazione del sistema	76
3.8.5	Identificazione dei diritti potenzialmente interessati	77
3.8.6	Valutazione delle misure e dei fattori di rischio	77
3.8.7	Determinazione del livello di rischio FRIA e integrazione con il Risk Assessment	78
3.8.8	Azioni, valutazione finale e aggiornamento	79
3.8.9	Strumento operativo e stato di avanzamento	80
3.9	Integrazione degli strumenti e stato di avanzamento del modello .	82

4	Sviluppo di una soluzione sperimentale per il monitoraggio dei piani di adeguamento	83
4.1	Obiettivi e impostazione della sperimentazione	83
4.2	Costruzione della base informativa sperimentale	84
4.3	Architettura della soluzione e trasformazione dei dati	88
4.3.1	Architettura e acquisizione delle fonti	88
4.3.2	Trasformazione e organizzazione dei dati in Power Query .	89
4.4	Modello semantico e logiche di calcolo	92
4.5	Progettazione della vista di sintesi	96
4.5.1	Impostazione generale e filtri	96
4.5.2	Indicatori e visualizzazioni aggregate	97
4.5.3	Dettaglio delle azioni	97
4.6	Verifica funzionale della soluzione sperimentale	98
4.7	Limiti e possibili sviluppi	100
4.7.1	Limiti della sperimentazione	100
4.7.2	Evoluzioni architetturali e del modello dati	100
4.7.3	Sviluppi della reportistica e considerazioni conclusive . . .	101
	Conclusioni	102
	Bibliografia e sitografia	104

Elenco delle figure

1.1	Rappresentazione sintetica dell’approccio basato sul rischio dell’AI Act (elaborazione da [11])	10
2.1	Fac-simile semplificato dell’inventario dei sistemi di IA (dati fittizi)	25
2.2	Struttura dell’AI Lifecycle nel modello operativo	32
2.3	Articolazione dei ruoli nel modello organizzativo di AI governance	37
2.4	Configurazione ibrida in valutazione per il coordinamento tra livello centrale e realtà estere	42
2.5	Integrazione delle principali componenti del modello operativo di AI governance	44
3.1	Workflow operativo per sistemi di IA ad alto rischio in qualità di fornitore	52
3.2	Workflow operativo per sistemi di IA ad alto rischio utilizzati in qualità di deployer	53
3.3	Principi di riferimento dell’AI Policy per un utilizzo responsabile dell’IA	55
3.4	Fac-simile semplificato dello strumento Excel del TAF (dati fittizi)	58
3.5	Fac-simile semplificato del file Excel per il monitoraggio dei piani di adeguamento e flusso di verifica delle azioni (dati fittizi)	66
3.6	Matrice per la determinazione del rischio residuo nella metodologia di Risk Assessment	71
3.7	Fac-simile semplificato dello strumento Excel per il Risk Assessment (dati fittizi)	74
3.8	Fac-simile semplificato dello strumento Excel per la FRIA (dati fittizi)	81
4.1	Fac-simile di un foglio di monitoraggio del file <code>Experimental_Monitoring_BU_01.xlsx</code> (dati sintetici)	87
4.2	Architettura logica della soluzione sperimentale di monitoraggio .	89
4.3	Rappresentazione grafica della dashboard implementata per il monitoraggio dei piani di adeguamento	98

Elenco delle tabelle

1.1	Sintesi della rappresentazione dell'approccio basato sul rischio proposta dalla Commissione europea	8
1.2	Principali ruoli regolatori previsti dall'AI Act	11
1.3	Sintesi degli obblighi e delle principali attività lungo il ciclo di vita di un sistema di IA	14
1.4	Principali riferimenti per l'AI governance	18
2.1	Dimensioni utilizzate nella traduzione dei requisiti normativi	23
2.2	Scenari regolatori utilizzati nel modello operativo	28
2.3	Struttura di sintesi dell'AI Lifecycle nel modello operativo	31
2.4	Ruoli principali nel modello organizzativo di AI governance	36
2.5	Confronto tra le configurazioni organizzative considerate per la governance di gruppo	39
3.1	Sintesi dei percorsi dell'AI Lifecycle in funzione del rischio e del ruolo regolatorio	50
3.2	Rapporto tra AI Policy e AI Lifecycle nel modello operativo	57
3.3	Principali dimensioni presidiate dal TAF	60
3.4	Tipologie di scostamento considerate nell'analisi	65
3.5	Struttura logica della metodologia di Risk Assessment	68
3.6	Tracciabilità delle principali scelte della metodologia di Risk Assessment	72
3.7	Fattori utilizzati nella valutazione FRIA	78
4.1	Requisiti della soluzione sperimentale di monitoraggio	84
4.2	Configurazione dei file Excel utilizzati nella sperimentazione	86
4.3	Campi principali della tabella Remediation_Source	92
4.4	Principali indicatori implementati nel modello semantico	96
4.5	Casi principali di verifica funzionale del prototipo	99

Sommario

Il presente lavoro riguarda la progettazione e la progressiva implementazione di un modello operativo di AI governance finalizzato a tradurre i requisiti introdotti dal Regolamento (UE) 2024/1689 sull'intelligenza artificiale (AI Act) in processi, responsabilità, controlli e strumenti applicabili al contesto aziendale. Il lavoro è stato sviluppato nell'ambito di un progetto di consulenza svolto durante il tirocinio presso KPMG per un'azienda cliente. I requisiti applicabili sono stati tradotti in flussi operativi, politiche, procedure, checklist, template e strumenti di supporto.

Il modello sviluppato supporta il censimento e la classificazione dei sistemi di IA, la determinazione del ruolo regolatorio e la loro gestione lungo il ciclo di vita. Un ruolo centrale è svolto dal Trusted AI Framework (TAF), utilizzato per organizzare i controlli applicabili, valutarne il livello di copertura e individuare eventuali scostamenti. Il lavoro ha inoltre riguardato la definizione della governance a livello di gruppo e il coordinamento con le società estere, nonché la predisposizione delle metodologie e degli strumenti di Risk Assessment e Fundamental Rights Impact Assessment (FRIA) per i sistemi classificati ad alto rischio.

Le prime attività di applicazione hanno consentito di avviare la definizione dei piani di adeguamento per una parte dei sistemi in perimetro. A completamento del lavoro è stata infine progettata e sperimentata una dashboard interattiva in Power BI per il monitoraggio trasversale di tali piani.

Introduzione

La crescente diffusione dei sistemi di intelligenza artificiale sta trasformando il funzionamento delle organizzazioni, incidendo sui processi operativi, sulla gestione delle informazioni e sui meccanismi di supporto alle decisioni. A tali opportunità si accompagnano nuovi rischi e la necessità di definire modalità strutturate per governare i sistemi lungo il loro intero ciclo di vita. In questo contesto, l'AI Act introduce un quadro regolatorio armonizzato fondato su un approccio basato sul rischio e differenzia gli obblighi in funzione delle caratteristiche dei sistemi e del ruolo assunto dagli operatori coinvolti [1]. Per le organizzazioni la questione non consiste quindi soltanto nell'individuare i requisiti applicabili ma anche nel tradurli in processi, responsabilità, controlli ed evidenze concretamente integrabili nel funzionamento aziendale.

Il problema affrontato nella tesi nasce da questa esigenza di traduzione dalla norma all'operatività. AI governance, gestione del rischio, standard e framework di riferimento offrono principi e criteri utili ma non definiscono un'unica configurazione applicabile indistintamente a ogni organizzazione. È necessario costruire un modello coerente con i processi, le responsabilità e le caratteristiche dello specifico contesto aziendale mantenendo al tempo stesso la tracciabilità rispetto ai requisiti normativi e metodologici da cui le singole scelte derivano.

Il lavoro è stato sviluppato durante il tirocinio svolto presso KPMG nell'ambito di un progetto di consulenza finalizzato all'adeguamento di un'azienda cliente all'AI Act. Per esigenze di riservatezza l'organizzazione è mantenuta anonima e le informazioni sono presentate in modo da non consentirne l'identificazione, neppure indirettamente. Il contesto considerato presenta una particolare complessità poiché l'organizzazione può, a seconda dello scenario, sviluppare, acquistare, utilizzare, integrare o commercializzare sistemi di IA, assumendo ruoli regolatori differenti e, conseguentemente, obblighi diversi.

L'attività ha riguardato la progettazione e la progressiva implementazione di un modello operativo di AI governance capace di collegare classificazione, ruolo regolatorio, ciclo di vita, responsabilità, controlli, documentazione e monitoraggio. In tale percorso sono stati sviluppati e progressivamente affinati gli strumenti per il censimento e la classificazione dei sistemi, il modello del ciclo di vita dei sistemi di IA, il modello organizzativo di governance, il Trusted AI Framework (TAF), gli strumenti per l'analisi degli scostamenti e il monitoraggio dei piani di adeguamento. Per i sistemi ad alto rischio sono state inoltre sviluppate le metodologie e i relativi strumenti operativi di Risk Assessment e Fundamental Rights Impact Assessment (FRIA). Un ulteriore ambito di lavoro ha riguardato la definizione delle modalità di coordinamento con le società estere del gruppo, per le quali sono state considerate differenti configurazioni organizzative. Al momento della redazione, l'ipotesi di un assetto ibrido costituisce una possibile direzione progettuale e non una scelta definitivamente formalizzata.

Dal punto di vista metodologico, il lavoro ha seguito un approccio progettuale, applicativo e iterativo. L'analisi dell'AI Act, degli standard e degli altri riferimenti

tecnici e metodologici ha costituito la base per individuare i requisiti da tradurre in processi, responsabilità, controlli e strumenti. Le diverse componenti sono state sviluppate in parte parallelamente e progressivamente affinate attraverso il confronto con le funzioni coinvolte e le prime attività di applicazione. Il percorso non è stato quindi lineare: le scelte assunte su una componente hanno richiesto, in più occasioni, il riesame di altre parti del modello secondo successivi cicli di progettazione, formalizzazione e revisione.

Lo stato di avanzamento delle diverse componenti non è omogeneo. Il TAF è già stato applicato in una prima fase e, per una parte dei sistemi in perimetro, sono state avviate le conseguenti attività di definizione e monitoraggio dei piani di adeguamento. Le metodologie e i relativi strumenti di Risk Assessment e FRIA sono stati invece completati nella loro impostazione metodologica e operativa, mentre le valutazioni sistema-specifiche non risultano ancora avviate alla data di redazione. Le attività di adeguamento sono tuttora in corso e la governance delle società estere rimane in progressiva definizione. A completamento del percorso è stata inoltre sviluppata una soluzione sperimentale in Power BI, verificata funzionalmente su dati sintetici, con l'obiettivo di consolidare e monitorare in modo trasversale le azioni di adeguamento registrate negli strumenti operativi.

La tesi è articolata in quattro capitoli. Il primo presenta il quadro normativo e concettuale di riferimento, con particolare attenzione all'approccio basato sul rischio, ai ruoli regolatori, all'AI governance e ai principali standard e framework. Il secondo approfondisce la progettazione del modello operativo, dal censimento e dalla classificazione dei sistemi fino alla definizione del ciclo di vita dei sistemi e della governance organizzativa e di gruppo. Il terzo descrive l'implementazione operativa del modello, il TAF, l'analisi degli scostamenti, i piani di adeguamento e gli strumenti di valutazione predisposti per i sistemi ad alto rischio. Il quarto è dedicato allo sviluppo e alla verifica funzionale della soluzione sperimentale di monitoraggio. Le conclusioni sintetizzano i principali risultati, i limiti del lavoro e i possibili sviluppi futuri.

CAPITOLO 1

Dall'AI Act all'AI governance aziendale

Il presente capitolo introduce il quadro concettuale e normativo necessario per comprendere il problema affrontato nel lavoro. In primo luogo viene analizzato il ruolo dell'intelligenza artificiale nelle organizzazioni. Successivamente vengono esaminati l'AI Act, l'approccio basato sul rischio e i principali ruoli regolatori previsti dalla normativa. L'analisi prosegue con gli obblighi applicabili lungo il ciclo di vita dei sistemi di IA e con il rapporto tra AI risk management e AI governance, richiamando i principali standard e framework di riferimento. Infine, viene approfondito il passaggio dalla conformità normativa alla definizione di un modello operativo di governance, che costituisce il punto di partenza per i capitoli successivi.

1.1 L'intelligenza artificiale nel contesto organizzativo

Negli ultimi anni l'intelligenza artificiale ha assunto un ruolo sempre più rilevante all'interno delle organizzazioni, trovando progressivamente applicazione non soltanto in contesti sperimentali ma anche in processi, prodotti e servizi. Le applicazioni possono riguardare attività molto eterogenee tra cui l'automazione di operazioni ripetitive, l'analisi di grandi quantità di dati, il supporto ai processi decisionali, la gestione delle interazioni con clienti e utenti e lo sviluppo di nuove funzionalità digitali. L'adozione dell'intelligenza artificiale non rappresenta quindi soltanto una scelta tecnologica ma può incidere sull'organizzazione del lavoro, sulle responsabilità decisionali e sulle modalità con cui vengono progettati e gestiti i processi aziendali.

La diffusione dell'intelligenza artificiale nelle imprese rimane tuttavia eterogenea. La sua adozione non dipende soltanto dalla disponibilità della tecnologia ma anche dal grado di preparazione dell'organizzazione. In particolare, un'analisi condotta dall'Organisation for Economic Co-operation and Development (OECD), Boston Consulting Group e INSEAD evidenzia il ruolo della maturità nella gestione dei dati, della disponibilità di competenze adeguate e della capacità di individuare casi d'uso coerenti con gli obiettivi aziendali [2]. L'introduzione di sistemi di IA può infatti richiedere adeguamenti che coinvolgono processi, competenze, assetti organizzativi e cultura aziendale, andando oltre la dimensione puramente tecnologica.

A fronte delle opportunità offerte dall'IA emergono anche rischi legati sia alle caratteristiche tecniche dei sistemi sia alle modalità con cui essi vengono sviluppati, utilizzati e integrati nei processi organizzativi. La qualità e la rappresentatività dei dati possono influenzare i risultati prodotti e l'opacità o la complessità dei modelli

possono limitarne la trasparenza, la spiegabilità e l'interpretabilità. L'impiego dell'IA nei processi decisionali richiede inoltre una chiara definizione dei ruoli umani e delle responsabilità di supervisione. A questi aspetti si aggiungono rischi relativi alla privacy, alla sicurezza, alla robustezza e alla presenza di bias dannosi nonché la possibilità che errori o comportamenti inattesi producano conseguenze negative per persone e organizzazioni [3].

Il tema assume quindi una dimensione sociotecnica: il rischio non dipende esclusivamente dalle caratteristiche dell'algoritmo ma anche dal contesto nel quale il sistema viene impiegato, dai dati utilizzati, dalle modalità di interazione con gli utenti, dal livello di autonomia attribuito al sistema e dai processi organizzativi che ne governano l'utilizzo. La stessa soluzione tecnica può pertanto presentare profili di rischio differenti se utilizzata per finalità diverse o inserita in processi con conseguenze differenti per le persone coinvolte.

Queste caratteristiche rendono insufficiente una gestione dell'IA limitata alla sola dimensione tecnica. Quando i sistemi vengono inseriti nei processi aziendali e utilizzati da funzioni differenti diventa necessario chiarire chi sia responsabile delle decisioni che li riguardano, quali informazioni debbano essere raccolte e mantenute, quali verifiche debbano essere svolte e come debba essere gestita l'evoluzione del sistema nel tempo. La letteratura sull'AI governance sottolinea, in questa prospettiva, la necessità di integrare la gestione dell'intelligenza artificiale nella più ampia struttura di governance dell'organizzazione, collegandola ad ambiti già consolidati quali corporate governance, IT governance e data governance [4].

La natura articolata del tema emerge anche da una recente revisione sistematica della letteratura. Batool, Zowghi e Bano organizzano l'analisi dell'AI governance attorno a quattro domande fondamentali: chi esercita la governance, che cosa viene governato, in quale fase del ciclo di vita essa interviene e attraverso quali strumenti viene attuata [5]. La prospettiva evidenzia come la governance non possa essere ricondotta a un singolo controllo o a una specifica funzione aziendale ma richieda il coordinamento di soggetti, responsabilità, processi decisionali e strumenti diversi.

A questo livello è sufficiente osservare che la gestione organizzativa dell'IA assume una natura necessariamente trasversale. Lo stesso sistema può coinvolgere, in momenti diversi del proprio ciclo di vita, funzioni tecniche, di business, legali, di gestione del rischio, sicurezza e conformità. Diventa quindi necessario predisporre meccanismi di coordinamento che consentano di integrare competenze differenti e di assumere decisioni secondo criteri condivisi. Le modalità attraverso cui tali responsabilità vengono strutturate e messe in relazione con la gestione del rischio saranno approfondite nelle sezioni successive.

Nel contesto europeo, questa esigenza organizzativa si inserisce inoltre in un quadro normativo specificamente dedicato all'intelligenza artificiale. Il Regolamento (UE) 2024/1689, comunemente noto come AI Act, rappresenta il principale riferimento in tale ambito e introduce una disciplina differenziata in funzione delle caratteristiche dei sistemi, dei rischi associati e del ruolo assunto dai soggetti coinvolti. Prima di analizzare nel dettaglio tali elementi è quindi necessario ricostruire il percorso che ha condotto all'adozione dell'AI Act, le sue finalità generali e il relativo ambito di applicazione.

1.2 Il quadro normativo europeo sull'intelligenza artificiale

L'AI Act rappresenta l'esito di un percorso europeo avviato diversi anni prima della sua adozione. Nel 2019 il gruppo di esperti ad alto livello sull'intelligenza artificiale istituito dalla Commissione europea aveva pubblicato le *Ethics Guidelines for Trustworthy AI*, proponendo una visione dell'IA affidabile fondata su tre caratteristiche fondamentali: liceità, eticità e robustezza [6]. Le linee guida individuavano inoltre sette requisiti per un'IA affidabile:

- supervisione e intervento umano;
- robustezza tecnica e sicurezza;
- privacy e governance dei dati;
- trasparenza;
- diversità, non discriminazione ed equità;
- benessere sociale e ambientale;
- responsabilità.

Pur non avendo natura vincolante, tali orientamenti hanno contribuito a consolidare un approccio europeo all'intelligenza artificiale incentrato sulla tutela delle persone e dei diritti fondamentali.

Nel febbraio 2020 la Commissione europea ha pubblicato il *White Paper on Artificial Intelligence – A European approach to excellence and trust*, delineando un approccio volto a promuovere lo sviluppo e l'adozione dell'IA e, al tempo stesso, a costruire un quadro capace di tutelare sicurezza, diritti fondamentali e fiducia [7]. In continuità con tale percorso, il 21 aprile 2021 è stata presentata la proposta di regolamento europeo sull'intelligenza artificiale, impostata fin dall'origine secondo una logica basata sul rischio [8]. Il percorso legislativo si è quindi concluso con l'adozione del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 [1].

L'AI Act combina due esigenze principali, chiaramente riconoscibili nelle finalità indicate dall'articolo 1 del Regolamento. Da un lato, mira a migliorare il funzionamento del mercato interno attraverso un quadro armonizzato per lo sviluppo, l'immissione sul mercato, la messa in servizio e l'utilizzo dei sistemi di IA nell'Unione, promuovendo al contempo l'innovazione. Dall'altro, intende favorire lo sviluppo e l'impiego di un'intelligenza artificiale antropocentrica e affidabile, assicurando un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali. Il Regolamento si propone quindi di conciliare la diffusione dell'innovazione con l'esigenza di stabilire condizioni comuni per uno sviluppo e un utilizzo dell'IA coerenti con il quadro europeo di tutela [1].

Per comprendere quali soluzioni possano rientrare nel campo di applicazione della normativa è innanzitutto necessario richiamare la definizione di sistema di

IA. L'articolo 3, punto 1, dell'AI Act definisce il «sistema di IA» come un «sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali» [1]. La definizione costituisce il primo riferimento per stabilire se una determinata soluzione debba essere considerata ai fini dell'AI Act. Le valutazioni relative al rischio, al ruolo dei soggetti coinvolti e agli obblighi applicabili intervengono soltanto in un momento successivo.

L'applicabilità del Regolamento non dipende tuttavia soltanto dalle caratteristiche della soluzione. L'AI Act definisce infatti un ambito di applicazione ampio che tiene conto anche dei soggetti coinvolti, del contesto territoriale e della finalità per cui il sistema viene sviluppato, messo a disposizione o utilizzato. In determinate circostanze la disciplina si applica anche a soggetti stabiliti al di fuori dell'Unione europea, ad esempio quando un sistema di IA viene immesso sul mercato o messo in servizio nell'Unione oppure quando l'output prodotto dal sistema è utilizzato al suo interno. Il Regolamento prevede al tempo stesso specifiche esclusioni e condizioni di applicabilità che ne delimitano il perimetro in funzione dello scenario considerato [1]. Per le organizzazioni presenti in più Paesi ciò rende necessario valutare il sistema nel suo contesto complessivo e non soltanto in base al luogo in cui è stato sviluppato.

L'AI Act si inserisce inoltre in un quadro normativo già articolato e non sostituisce le altre discipline che possono applicarsi allo stesso sistema o allo stesso processo. A seconda dello scenario, la gestione di un sistema di IA può quindi richiedere di considerare congiuntamente, oltre all'AI Act, norme in materia di protezione dei dati personali, sicurezza dei prodotti, tutela dei consumatori, cibersicurezza e tutela dei lavoratori. Uno stesso sistema può pertanto essere soggetto contemporaneamente a più fonti normative, ciascuna riferita a profili differenti. Dal punto di vista organizzativo, l'adeguamento all'AI Act deve quindi essere integrato con i processi e i presidi di conformità già esistenti, evitando di trattare la gestione dell'IA come un ambito completamente separato.

L'AI Act è entrato in vigore il 1° agosto 2024 e ha previsto un'applicazione progressiva delle proprie disposizioni. Dal 2 agosto 2026 il Regolamento è generalmente applicabile. Il calendario di alcune disposizioni è stato successivamente modificato dal Regolamento (UE) 2026/1744 [9]. In particolare, sono state rinviate le date di applicazione delle sezioni 1, 2 e 3 del Capo III, relative alla classificazione, ai requisiti e agli obblighi dei sistemi ad alto rischio. Tali disposizioni si applicheranno dal 2 dicembre 2027 ai sistemi individuati ai sensi dell'articolo 6, paragrafo 2, e dell'allegato III e dal 2 agosto 2028 ai sistemi individuati ai sensi dell'articolo 6, paragrafo 1, e dell'allegato I [9]. Gli obblighi di trasparenza previsti dall'articolo 50 sono invece applicabili dal 2 agosto 2026. La Commissione europea ha inoltre pubblicato specifici orientamenti per supportarne l'applicazione [10].

La presenza di scadenze differenziate non riduce la necessità di preparare per tempo le attività di adeguamento. Le organizzazioni devono infatti identificare i sistemi interessati, comprenderne la classificazione e il ruolo regolatorio e definire gli obblighi applicabili prima delle relative date di applicazione. Lo stesso vale

per la predisposizione di processi, documentazione e controlli che richiede tempi di progettazione e implementazione non sempre compatibili con interventi avviati a ridosso delle scadenze. L'adeguamento assume quindi la forma di un percorso progressivo nel quale metodologie e strumenti vengono costruiti e affinati in anticipo rispetto all'applicazione dei singoli requisiti.

1.3 L'approccio basato sul rischio

L'AI Act adotta un approccio basato sul rischio. La disciplina applicabile varia infatti in funzione delle caratteristiche del sistema, del suo utilizzo e dei potenziali impatti che ne possono derivare. Il Regolamento definisce il rischio come la combinazione tra la probabilità che si verifichi un danno e la gravità del danno stesso [1]. Questa impostazione si traduce in regimi differenti. Alcune pratiche sono vietate, i sistemi ad alto rischio sono soggetti a requisiti specifici e per determinati sistemi, utilizzi o contenuti sono previsti obblighi di trasparenza.

Per facilitarne la comprensione, la Commissione europea rappresenta l'approccio basato sul rischio attraverso quattro livelli principali: rischio inaccettabile, alto rischio, rischio limitato, associato in particolare a specifici obblighi di trasparenza, e rischio minimo o nullo [11]. Questa rappresentazione costituisce una chiave di lettura utile dell'impostazione dell'AI Act e consente di ricondurre i diversi scenari a regimi regolatori differenti. Non si tratta tuttavia di quattro categorie giuridiche definite in modo uniforme dal Regolamento. I sistemi ad alto rischio sono individuati secondo i criteri previsti dall'articolo 6 e dagli allegati I e III, mentre gli obblighi di trasparenza dell'articolo 50 riguardano specifici sistemi, utilizzi o contenuti e possono applicarsi anche in assenza di una classificazione ad alto rischio. Il rischio minimo o nullo indica infine, in termini generali, i sistemi che non ricadono nei regimi più stringenti previsti dal Regolamento, ferma restando l'eventuale applicabilità di altre disposizioni. La Tabella 1.1 sintetizza questa rappresentazione e le principali conseguenze regolatorie associate ai diversi livelli.

Tabella 1.1: Sintesi della rappresentazione dell'approccio basato sul rischio proposta dalla Commissione europea

Livello	Inquadramento	Conseguenza regolatoria principale
Rischio inaccettabile	Pratiche vietate nei casi individuati dall'articolo 5	Divieto delle pratiche previste dalla norma, salvo le specifiche eccezioni applicabili
Alto rischio	Sistemi che soddisfano le condizioni previste dall'articolo 6 e dagli allegati I o III	Requisiti specifici per il sistema e obblighi differenziati in funzione del ruolo degli operatori coinvolti
Rischio limitato / di trasparenza	Sistemi, utilizzi o contenuti per i quali il Regolamento prevede specifiche esigenze di trasparenza	Obblighi di informazione, identificabilità o marcatura nei casi previsti dall'articolo 50
Rischio minimo o nullo	Sistemi che non ricadono nei regimi più stringenti previsti dall'AI Act	Assenza di obblighi specifici comparabili a quelli previsti per i sistemi ad alto rischio, ferma restando l'applicabilità di altre disposizioni

La rappresentazione sintetizzata nella Tabella 1.1 consente di distinguere regimi che rispondono a logiche differenti. Il caso più restrittivo è quello delle pratiche vietate dall'articolo 5. Vi rientrano, tra le altre, alcune forme di manipolazione o sfruttamento delle vulnerabilità, determinate pratiche di social scoring, specifici utilizzi della categorizzazione biometrica e del riconoscimento delle emozioni e alcuni casi di identificazione biometrica remota in tempo reale. In questi scenari il Regolamento non richiede semplicemente l'adozione di misure aggiuntive ma vieta le pratiche individuate dal legislatore, fatte salve le eccezioni espressamente previste [1]. Il Regolamento (UE) 2026/1744 ha inoltre ampliato l'articolo 5 introducendo ulteriori divieti relativi alla generazione o manipolazione non consensuale di determinati contenuti intimi o sessualmente espliciti. Tali disposizioni si applicheranno dal 2 dicembre 2026 [9].

Una logica diversa riguarda i sistemi ad alto rischio, per i quali l'AI Act prevede requisiti e obblighi specifici. L'articolo 6 individua due principali modalità di classificazione. La prima riguarda i sistemi di IA destinati a essere utilizzati come componente di sicurezza di un prodotto oppure che costituiscono essi stessi un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I e, nei casi previsti, soggetto a una valutazione della conformità da parte di terzi. La seconda riguarda i sistemi di IA ricompresi nei casi d'uso elencati nell'allegato III [1]. Tra le aree considerate figurano, a titolo esemplificativo, biometria, infrastrutture critiche, istruzione, occupazione, accesso a determinati servizi essenziali, attività di contrasto, migrazione e controllo delle frontiere, amministrazione della giustizia e processi democratici. Il Regolamento (UE) 2026/1744 ha inoltre precisato il concetto di componente di sicurezza. I sistemi

utilizzati esclusivamente per finalità non connesse alla sicurezza non rientrano in tale nozione, salvo il caso in cui un loro guasto o malfunzionamento possa mettere a rischio la salute o la sicurezza [9].

Per i sistemi ricompresi nell'allegato III, l'appartenenza a una delle aree individuate dal Regolamento non determina sempre in modo automatico la classificazione ad alto rischio. L'articolo 6 prevede che un sistema possa non essere considerato ad alto rischio quando non presenti un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali e non influenzi materialmente il risultato di un processo decisionale, purché ricorrano le condizioni previste dalla norma. La deroga non opera quando il sistema effettua profilazione di persone fisiche [1]. Il fornitore che conclude che un sistema ricompreso nell'allegato III non debba essere classificato ad alto rischio deve inoltre documentare la propria valutazione prima dell'immissione sul mercato o della messa in servizio. La classificazione richiede quindi di considerare la finalità, le funzionalità, il contesto d'uso e l'impatto concreto del sistema, mantenendo traccia delle motivazioni alla base della decisione.

Accanto a questi regimi, l'articolo 50 introduce specifici obblighi di trasparenza che possono applicarsi anche a sistemi non classificati ad alto rischio. Rientrano, tra gli altri, i sistemi destinati a interagire direttamente con persone fisiche, quelli che generano o manipolano contenuti sintetici, i sistemi di riconoscimento delle emozioni o di categorizzazione biometrica e la diffusione di deepfake o di determinati testi generati o manipolati dall'IA nei casi previsti dalla norma [1]. La finalità è rendere riconoscibile sia l'interazione con un sistema di IA sia l'origine artificiale o manipolata di determinati contenuti. La Commissione europea collega tali misure alla necessità di ridurre rischi di inganno, manipolazione e disinformazione e di consentire alle persone di comprendere quando sono esposte a contenuti o interazioni generati dall'IA [10].

Separatamente dalla classificazione dei sistemi per rischio, l'AI Act prevede un regime specifico per i modelli di IA per finalità generali (General-Purpose AI, GPAI). Questi modelli non costituiscono quindi un ulteriore livello della rappresentazione precedente. Il Capo V introduce obblighi specifici per i loro fornitori, tra cui requisiti relativi alla documentazione e alla disponibilità di informazioni per i soggetti a valle. Per i modelli di IA per finalità generali con rischio sistemico sono inoltre previsti obblighi aggiuntivi relativi, tra l'altro, alla valutazione del modello, alla gestione dei rischi sistemici, alla segnalazione degli incidenti gravi e alla cibersecurity [1]. Un modello per finalità generali può essere integrato in sistemi destinati a usi specifici. Diventa quindi necessario distinguere le responsabilità dei diversi soggetti lungo la catena del valore.

Nel complesso, l'approccio basato sul rischio richiede una valutazione che vada oltre la sola tecnologia impiegata. Per individuare correttamente il regime applicabile occorre considerare la finalità del sistema, il contesto in cui viene utilizzato, il livello di rischio e il ruolo assunto dall'organizzazione. Da questa esigenza deriva la necessità di un processo strutturato di identificazione e classificazione, capace di ricondurre ogni sistema a uno scenario normativo coerente e di documentare le decisioni assunte. La Figura 1.1 sintetizza graficamente i principali livelli attraverso cui la Commissione europea rappresenta l'approccio

basato sul rischio dell'AI Act.

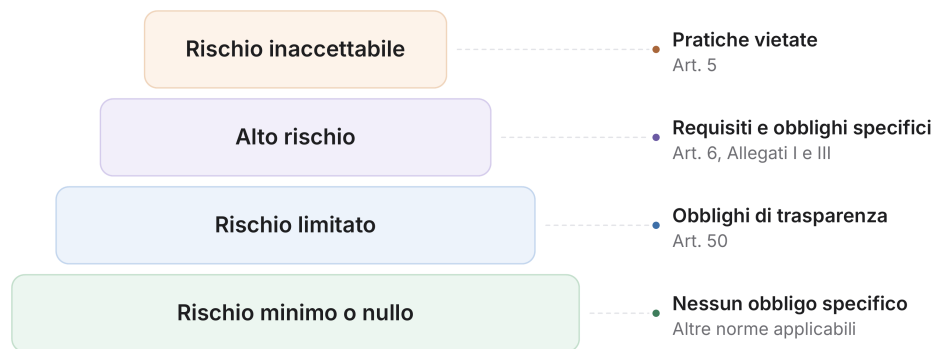


Figura 1.1: Rappresentazione sintetica dell'approccio basato sul rischio dell'AI Act (elaborazione da [11])

1.4 Ruoli regolatori e scenari applicativi

Accanto alla classificazione del rischio, la determinazione degli obblighi applicabili richiede di individuare il ruolo assunto dall'organizzazione rispetto al sistema. L'AI Act distingue infatti diverse figure in base alle attività svolte e alla posizione assunta rispetto allo sviluppo, all'immissione sul mercato e all'utilizzo del sistema. A ciascuna di esse sono associati obblighi differenti [1].

Tra i principali ruoli previsti dal Regolamento rientrano il fornitore, il deployer, l'importatore, il distributore e il rappresentante autorizzato. Il termine *operatore* è utilizzato come definizione generale che ricomprende queste figure insieme al fabbricante del prodotto [1]. Ai fini del presente lavoro assumono particolare rilevanza i ruoli di fornitore e deployer poiché corrispondono agli scenari effettivamente riscontrati nel perimetro analizzato. Alla data di redazione della tesi non sono infatti emersi casi d'uso riconducibili agli ulteriori ruoli previsti dal Regolamento. Il modello operativo è stato pertanto sviluppato con riferimento ai percorsi relativi a fornitore e deployer, ferma restando la rilevanza degli altri ruoli ai fini dell'inquadramento complessivo della catena del valore e di eventuali scenari futuri.

Il fornitore è il soggetto che sviluppa o fa sviluppare un sistema di IA o un modello di IA per finalità generali e lo immette sul mercato oppure mette in servizio il sistema sotto il proprio nome o marchio. Il deployer è invece il soggetto che utilizza un sistema di IA sotto la propria autorità, fatta eccezione per l'uso personale e non professionale [1]. La distinzione assume particolare rilievo per i sistemi ad alto rischio. Al fornitore sono attribuiti gli obblighi connessi alla conformità del sistema mentre il deployer è responsabile del rispetto degli obblighi relativi al suo utilizzo nel contesto concreto.

La Tabella 1.2 sintetizza i principali ruoli regolatori e le relative implicazioni organizzative.

Tabella 1.2: Principali ruoli regolatori previsti dall'AI Act

Ruolo	Criterio essenziale	Implicazione organizzativa
Fornitore	Sviluppa o fa sviluppare il sistema e lo immette sul mercato o lo mette in servizio sotto il proprio nome o marchio	È destinatario degli obblighi di conformità attribuiti al fornitore nei casi applicabili
Deployer	Utilizza un sistema di IA sotto la propria autorità, fatta eccezione per l'uso personale e non professionale	Governa l'utilizzo del sistema nel contesto concreto e, ove applicabile, adotta le misure organizzative e di sorveglianza previste
Importatore	Immette sul mercato dell'Unione un sistema recante il nome o marchio di un soggetto stabilito in un Paese terzo	Verifica gli elementi di conformità previsti prima dell'immissione sul mercato
Distributore	Rende disponibile sul mercato dell'Unione un sistema senza essere fornitore o importatore	Svolge le verifiche previste e gestisce eventuali condizioni di non conformità
Rappresentante autorizzato	Opera nell'Unione sulla base di un mandato scritto conferito da un fornitore non stabilito nell'Unione	Svolge i compiti attribuiti dal mandato e quelli previsti dal Regolamento

I ruoli appena descritti non sono attribuiti all'organizzazione in modo univoco ma devono essere determinati con riferimento al singolo sistema e allo specifico scenario in cui essa opera. Una stessa impresa può quindi essere fornitore per un sistema che sviluppa o fa sviluppare e che immette sul mercato o mette in servizio sotto il proprio nome o marchio, e deployer per una soluzione acquistata da un soggetto terzo e utilizzata sotto la propria autorità. All'interno di gruppi complessi, inoltre, società differenti possono assumere ruoli diversi rispetto allo stesso ecosistema tecnologico. La determinazione del ruolo deve pertanto essere effettuata caso per caso considerando le attività concretamente svolte, le modalità di sviluppo, immissione sul mercato o utilizzo del sistema e le relazioni tra i soggetti coinvolti.

Il ruolo può inoltre mutare a seguito di determinate attività svolte lungo la catena del valore. L'articolo 25 prevede che, per i sistemi ad alto rischio, un distributore, un importatore, un deployer o un altro soggetto terzo sia considerato fornitore quando appone il proprio nome o marchio su un sistema già immesso sul mercato o messo in servizio, quando apporta una modifica sostanziale mantenendo il sistema ad alto rischio oppure quando modifica la finalità prevista di un sistema in modo tale da renderlo ad alto rischio [1]. Modifiche, personalizzazioni o integrazioni devono quindi essere valutate anche sotto il profilo regolatorio per verificare se producano uno degli effetti previsti dall'articolo 25.

In questo quadro assume particolare rilievo la nozione di finalità prevista, definita dal Regolamento come l'uso al quale il sistema è destinato dal fornitore, compresi il contesto e le condizioni d'uso specifici indicati nelle istruzioni per l'uso, nel materiale promozionale o di vendita, nelle dichiarazioni e nella documentazione

tecnica [1]. La finalità prevista incide sulla classificazione del rischio e sull'individuazione delle responsabilità degli operatori. Una sua modifica o un cambiamento delle condizioni di utilizzo rilevanti ai fini della normativa può pertanto richiedere una nuova valutazione dell'inquadramento regolatorio del sistema.

L'AI Act attribuisce inoltre rilievo ai rapporti tra i soggetti della catena del valore. Nei casi previsti, il fornitore di un sistema ad alto rischio e i soggetti che forniscono sistemi di IA, modelli di IA, strumenti, servizi, componenti o processi utilizzati o integrati nel sistema devono disciplinare mediante accordo scritto le informazioni, le capacità tecniche, gli accessi e l'assistenza necessari affinché il fornitore possa adempiere agli obblighi applicabili [1, 9]. La gestione della conformità richiede quindi anche una circolazione adeguata delle informazioni tra gli attori che contribuiscono allo sviluppo, alla distribuzione e all'utilizzo del sistema.

Da un punto di vista operativo, la determinazione del ruolo richiede quindi una lettura dello scenario complessivo: chi sviluppa il sistema, sotto quale nome o marchio viene immesso sul mercato o messo in servizio, chi ne controlla l'utilizzo, quali modifiche vengono apportate, come viene integrato in prodotti o servizi, quale sia la finalità prevista e quale sia il concreto contesto di utilizzo. Questa analisi costituisce un passaggio preliminare indispensabile per associare correttamente gli obblighi e definire responsabilità interne coerenti.

1.5 Gli obblighi lungo il ciclo di vita dei sistemi di IA

L'AI Act non concentra gli obblighi in un singolo momento ma distribuisce responsabilità e requisiti lungo il ciclo di vita dei sistemi. Questa logica è particolarmente evidente per i sistemi ad alto rischio, per i quali il Regolamento combina requisiti di progettazione, obblighi documentali, valutazioni preventive, controlli durante l'utilizzo e attività di monitoraggio successive alla messa in servizio [1].

Per ciclo di vita di un sistema di IA si intende l'insieme delle fasi che accompagnano il sistema dalla sua individuazione e progettazione fino all'utilizzo, al monitoraggio e all'eventuale modifica o dismissione. A seconda dello scenario, il percorso può comprendere attività di sviluppo interno oppure di acquisizione da soggetti terzi, seguite dalla preparazione alla messa in servizio, dall'utilizzo operativo e dal monitoraggio nel tempo. Le diverse fasi non devono essere intese come una sequenza rigida e identica per ogni sistema ma come momenti logici nei quali possono emergere responsabilità, requisiti e decisioni differenti.

Prima degli obblighi specifici connessi alle categorie di rischio, il Regolamento introduce anche alcuni requisiti di carattere trasversale. Tra questi rientra l'articolo 4 sull'alfabetizzazione in materia di IA, che, nella formulazione modificata dal Regolamento (UE) 2026/1744, richiede a fornitori e deployer di adottare misure volte a sostenere lo sviluppo dell'alfabetizzazione del personale e delle altre persone che operano per loro conto nell'ambito del funzionamento e dell'utilizzo dei sistemi. La disposizione evidenzia come la conformità non dipenda soltanto dall'esistenza di controlli tecnici ma anche dalla capacità dell'organizzazione di mettere i soggetti

coinvolti nelle condizioni di comprendere caratteristiche, opportunità e rischi dei sistemi utilizzati [1, 9].

Per i sistemi ad alto rischio, gli articoli da 9 a 15 definiscono un insieme di requisiti che incidono direttamente sul modo in cui il sistema deve essere progettato e gestito. L'articolo 9 prevede un sistema di gestione del rischio continuo e iterativo lungo l'intero ciclo di vita mentre l'articolo 10 disciplina i dati e la relativa governance. Gli articoli 11 e 12 riguardano rispettivamente la documentazione tecnica e la registrazione automatica degli eventi attraverso log. Gli articoli 13, 14 e 15 disciplinano infine la trasparenza e le informazioni da fornire ai deployer, la sorveglianza umana e i requisiti di accuratezza, robustezza e cibersicurezza [1].

Questi requisiti mostrano come la gestione del rischio debba iniziare fin dalla progettazione del sistema. La documentazione tecnica, la qualità dei dati, la sorveglianza umana e i requisiti di robustezza non possono essere considerati soltanto al termine del processo ma devono essere integrati nelle attività di sviluppo, test e preparazione al rilascio. La conformità deve quindi essere costruita progressivamente nelle diverse fasi del ciclo di vita del sistema.

A tali requisiti si affiancano specifici obblighi organizzativi del fornitore. Tra questi rientrano l'adozione di un sistema di gestione della qualità, la conservazione della documentazione, la gestione dei log quando sono sotto il proprio controllo e l'adozione di azioni correttive in presenza di non conformità. Prima dell'immissione sul mercato o della messa in servizio il sistema deve inoltre essere sottoposto alla procedura di valutazione della conformità applicabile. Nei casi previsti devono essere predisposte la dichiarazione UE di conformità, la marcatura CE e la registrazione nelle banche dati pertinenti [1].

Il ciclo di conformità non si conclude con il rilascio. Il Regolamento prevede attività di monitoraggio successive all'immissione sul mercato attraverso le quali il fornitore deve raccogliere e analizzare in modo sistematico le informazioni relative alle prestazioni del sistema durante il suo utilizzo. Sono inoltre previsti obblighi di gestione e segnalazione degli incidenti gravi nei casi applicabili. Il profilo di rischio di un sistema non può quindi essere considerato statico. Condizioni d'uso, dati, prestazioni e contesto possono cambiare e richiedere interventi successivi alla messa in servizio.

Anche il deployer di un sistema ad alto rischio è destinatario di obblighi specifici. L'articolo 26 richiede l'adozione di misure tecniche e organizzative appropriate per utilizzare il sistema conformemente alle istruzioni fornite dal fornitore e l'assegnazione della sorveglianza umana a persone dotate delle necessarie competenze, formazione e autorità. Il deployer deve inoltre gestire i dati di input quando questi sono sotto il proprio controllo, monitorare il funzionamento del sistema sulla base delle istruzioni d'uso, conservare i log nei casi previsti e adottare le misure necessarie qualora emergano rischi o malfunzionamenti [1].

Per alcuni deployer e specifici casi d'uso, l'articolo 27 introduce inoltre la valutazione d'impatto sui diritti fondamentali (*Fundamental Rights Impact Assessment*, FRIA), finalizzata a valutare l'impatto che l'utilizzo del sistema ad alto rischio può produrre sui diritti fondamentali delle persone interessate. La valutazione considera i processi nei quali il sistema è utilizzato, il periodo e la frequenza

d'uso, le categorie di persone interessate, i rischi specifici di danno, le misure di sorveglianza umana e le azioni previste qualora tali rischi si concretizzino [1]. La FRIA costituisce un esempio particolarmente chiaro di come la conformità richieda di mettere in relazione le caratteristiche del sistema con il contesto organizzativo di utilizzo.

Su questa base, la gestione lungo il ciclo di vita può essere sintetizzata distinguendo alcune macrofasi logiche. Nelle fasi iniziali assumono rilievo l'identificazione del sistema, la definizione della finalità, la classificazione del rischio e l'individuazione del ruolo regolatorio. Le fasi di sviluppo o acquisizione e di preparazione al rilascio richiedono l'implementazione dei requisiti tecnici e organizzativi, la produzione della documentazione e, per il fornitore, le verifiche di conformità previste. Durante l'utilizzo diventano centrali la sorveglianza umana, il monitoraggio, la gestione degli incidenti e la raccolta delle evidenze. Modifiche sostanziali, variazioni della finalità prevista o evoluzioni del sistema possono infine richiedere una nuova valutazione dello scenario regolatorio. La Tabella 1.3 sintetizza, per ciascuna fase, i temi principali e le evidenze organizzative tipiche.

Tabella 1.3: Sintesi degli obblighi e delle principali attività lungo il ciclo di vita di un sistema di IA

Fase	Temi principali	Evidenze organizzative tipiche
Identificazione e classificazione	Appartenenza al perimetro dell'IA, finalità prevista, rischio, ruolo regolatorio, soggetti coinvolti	Registro dei sistemi, valutazione di classificazione, motivazioni della classificazione e del ruolo
Sviluppo o acquisizione	Requisiti applicabili, dati, gestione del rischio, robustezza, sicurezza e sorveglianza umana	Requisiti di progetto o acquisizione, controlli, documentazione tecnica e informazioni del fornitore
Preparazione al rilascio o alla messa in servizio	Verifiche, approvazioni, conformità, registrazioni e condizioni d'uso	Liste di controllo, valutazioni, approvazioni, dichiarazioni e registrazioni ove previste
Utilizzo e monitoraggio	Uso conforme, sorveglianza umana, registrazione degli eventi, prestazioni e incidenti	Log, evidenze di monitoraggio, segnalazioni, report e azioni correttive
Modifica e dismissione	Modifiche sostanziali, variazioni della finalità prevista, aggiornamento del rischio e cessazione dell'uso	Rivalutazioni, aggiornamenti documentali, decisioni di modifica o dismissione

Questa lettura per ciclo di vita è particolarmente utile dal punto di vista aziendale perché consente di trasformare obblighi distribuiti in numerosi articoli in un insieme ordinato di momenti decisionali e attività. La conformità diventa così un processo continuo: non è sufficiente verificare un sistema una sola volta

ma occorre mantenere nel tempo la coerenza tra classificazione, utilizzo, controlli, documentazione e rischio effettivo.

Alla data di redazione della tesi una parte degli obblighi specificamente riferiti ai sistemi ad alto rischio presenta, come già evidenziato, date di applicazione differite. Ciò non impedisce tuttavia di utilizzarne la struttura come riferimento per la preparazione dei processi di governance. Per organizzazioni complesse predisporre inventari, responsabilità, procedure, strumenti di valutazione e meccanismi di monitoraggio richiede infatti tempi incompatibili con un approccio concentrato esclusivamente sulla data formale di applicazione.

1.6 AI risk management e AI governance

La gestione del rischio costituisce una componente centrale della gestione dei sistemi di IA ma non coincide con l'intero concetto di AI governance. Il risk management riguarda principalmente il processo attraverso cui i rischi vengono identificati, analizzati, valutati, trattati e monitorati. La governance definisce invece il quadro di responsabilità, autorità, processi e meccanismi decisionali entro cui tali attività vengono svolte. In altri termini, il risk management definisce come gestire il rischio mentre la governance chiarisce chi deve farlo, quando, con quali informazioni e secondo quali regole organizzative.

La gestione dei rischi connessi ai sistemi di IA presenta alcune specificità rispetto a forme di rischio tecnologico più tradizionali. Le prestazioni di un sistema possono dipendere fortemente dai dati e variare quando cambia il contesto di utilizzo. Alcuni modelli possono essere difficili da interpretare e gli output possono interagire con decisioni umane. Le dipendenze da fornitori o componenti esterne possono inoltre ridurre la capacità dell'organizzazione di controllare direttamente tutti gli elementi della soluzione. A questi fattori si aggiungono rischi relativi a bias, privacy, sicurezza, affidabilità, uso improprio e possibili impatti sui diritti fondamentali.

L'AI Act incorpora questa logica imponendo, per i sistemi ad alto rischio, un processo di gestione del rischio continuo, iterativo e riferito all'intero ciclo di vita [1]. La normativa richiede di identificare e analizzare i rischi noti e ragionevolmente prevedibili, valutare quelli che possono emergere quando il sistema viene utilizzato conformemente alla finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile e adottare misure di gestione proporzionate. Questa impostazione supera quindi una visione del rischio come valutazione una tantum svolta prima del rilascio.

La stessa prospettiva è rintracciabile nell'*Artificial Intelligence Risk Management Framework* (AI RMF 1.0) del National Institute of Standards and Technology (NIST), pubblicato nel 2023 come framework volontario e adattabile a organizzazioni differenti [3]. Il framework organizza le attività di gestione del rischio in quattro funzioni: *Govern*, *Map*, *Measure* e *Manage*. La funzione *Govern* è trasversale e riguarda cultura, responsabilità, politiche e meccanismi di responsabilizzazione. *Map* è orientata alla comprensione del contesto, delle finalità, degli attori e dei rischi. *Measure* riguarda l'analisi e la valutazione mentre *Manage* riguarda la prioritizzazione e il trattamento dei rischi. La natura interconnessa delle funzioni

e il carattere continuo della gestione del rischio riflettono la necessità di aggiornare le valutazioni quando cambiano il sistema, i dati o il contesto.

Il NIST AI RMF associa inoltre la gestione del rischio alla costruzione di sistemi affidabili. Tra le caratteristiche considerate rientrano validità e affidabilità, sicurezza, resilienza, responsabilizzazione e trasparenza, spiegabilità e interpretabilità, tutela della privacy e gestione dei bias dannosi [3]. Questi elementi mostrano come il rischio connesso ai sistemi di IA non possa essere ridotto a una singola metrica ma richieda una valutazione multidimensionale.

La governance interviene per rendere tali principi concretamente applicabili. La definizione di un modello di AI governance richiede, ad esempio, di stabilire chi possa richiedere l'introduzione di un nuovo sistema, chi ne verifichi la classificazione, quali funzioni debbano approvare gli scenari più critici, chi sia responsabile della documentazione e dei controlli e quali eventi richiedano il coinvolgimento di livelli decisionali superiori. La letteratura sull'AI governance a livello organizzativo sottolinea proprio la necessità di integrare tali responsabilità con le strutture di governance già esistenti, evitando di creare processi paralleli non coordinati [4].

La revisione sistematica di Batool, Zowghi e Bano conferma questa natura multidimensionale mostrando come la governance possa operare a livello di team, di organizzazione, di settore, nazionale e internazionale, e come i relativi meccanismi possano assumere la forma di framework, strumenti, politiche o modelli organizzativi [5]. Per una singola organizzazione, il problema diventa quindi quello di selezionare e combinare tali meccanismi in modo coerente con il proprio profilo di rischio e con la propria struttura interna.

Ai fini del presente lavoro, una governance efficace può essere letta attraverso quattro dimensioni complementari:

- **dimensione decisionale**, relativa alla definizione di ruoli, autorità e momenti di approvazione;
- **dimensione metodologica**, riferita ai criteri utilizzati per identificare, classificare e valutare i sistemi;
- **dimensione di controllo**, che traduce i requisiti in verifiche e misure concretamente applicabili;
- **dimensione informativa**, finalizzata ad assicurare la disponibilità di dati, evidenze e documentazione necessari per rendere tracciabili le decisioni e monitorare l'evoluzione del rischio.

Il rapporto tra risk management e governance è quindi continuo e reciprocamente influente. Il processo di gestione del rischio produce informazioni che alimentano le decisioni di governance. Le decisioni di governance determinano a loro volta priorità, responsabilità e azioni di trattamento. Il monitoraggio verifica nel tempo l'adequatezza delle misure e può determinare una nuova valutazione. Questo meccanismo è particolarmente rilevante per sistemi soggetti a frequenti aggiornamenti o per scenari nei quali il contesto di utilizzo evolve nel tempo.

1.7 Standard e framework di riferimento

La normativa definisce il risultato di conformità atteso e individua specifici obblighi ma non esaurisce necessariamente le modalità con cui un'organizzazione può strutturare il proprio sistema di gestione. Standard e framework internazionali rappresentano quindi un riferimento utile per tradurre principi e requisiti in processi ripetibili, responsabilità, controlli e meccanismi di miglioramento continuo.

Tra gli standard maggiormente rilevanti rientra ISO/IEC 42001:2023, *Information technology – Artificial intelligence – Management system*. Lo standard definisce requisiti per istituire, implementare, mantenere e migliorare continuamente un Artificial Intelligence Management System (AIMS) [12]. La logica non riguarda il singolo algoritmo ma il sistema organizzativo attraverso cui l'impresa governa lo sviluppo, la fornitura o l'utilizzo dell'IA. In questo senso, ISO/IEC 42001 fornisce una struttura utile per integrare politiche, ruoli, pianificazione, supporto, attività operative, valutazione delle prestazioni e miglioramento continuo.

Il riferimento a un sistema di gestione è particolarmente significativo perché porta il tema dell'IA oltre la sola dimensione progettuale. Un sistema di gestione richiede che obiettivi, responsabilità e processi siano formalizzati, monitorati e riesaminati. Richiede inoltre che la gestione dell'IA venga collegata al contesto dell'organizzazione e alle esigenze delle parti interessate. La logica di miglioramento continuo consente così di trattare la governance come un processo evolutivo nel quale politiche e controlli vengono aggiornati quando emergono nuove tecnologie, rischi, evidenze o requisiti.

Un secondo riferimento è ISO/IEC 23894:2023, *Information technology – Artificial intelligence – Guidance on risk management*. Lo standard fornisce indicazioni per organizzazioni che sviluppino, producano, distribuiscono o utilizzano prodotti, sistemi e servizi basati sull'IA e mira a integrare la gestione del rischio nelle attività e nelle funzioni legate all'intelligenza artificiale [13]. Il suo valore risiede soprattutto nell'adattamento dei principi generali di gestione del rischio alle peculiarità dei sistemi di IA e nella possibilità di modulare l'approccio in funzione del contesto dell'organizzazione.

Il NIST AI RMF 1.0 costituisce invece un framework volontario sviluppato dal National Institute of Standards and Technology statunitense. Come già evidenziato, le funzioni Govern, Map, Measure e Manage permettono di organizzare in modo strutturato il processo di gestione del rischio e di collegarlo alle caratteristiche di affidabilità del sistema [3]. Alla data di redazione della presente tesi, il NIST ha avviato un processo di revisione della versione 1.0 [14]. Il framework deve quindi essere considerato un riferimento evolutivo da utilizzare tenendo conto degli aggiornamenti pubblicati dall'istituto.

Accanto a standard e framework di gestione del rischio, gli orientamenti europei sull'IA affidabile continuano a rappresentare un utile riferimento concettuale. Le *Ethics Guidelines for Trustworthy AI* del 2019 avevano già proposto una lettura dell'affidabilità fondata su supervisione umana, robustezza tecnica e sicurezza, privacy e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità [6]. L'importanza di tali principi non risiede soltanto nella loro dimensione etica. Molti di essi si ritrovano

successivamente tradotti, con diversa forza giuridica, in requisiti e obblighi del quadro normativo europeo. La Tabella 1.4 sintetizza i principali riferimenti richiamati e il contributo che ciascuno di essi offre alla costruzione di un modello di AI governance.

Tabella 1.4: Principali riferimenti per l’AI governance

Riferimento	Natura	Contributo principale
AI Act	Regolamento dell’Unione europea	Obblighi giuridici differenziati in funzione del rischio, del ruolo e dello scenario di utilizzo
ISO/IEC 42001:2023	Standard internazionale per sistemi di gestione	Struttura organizzativa per governare e migliorare continuamente la gestione dell’IA
ISO/IEC 23894:2023	Linea guida internazionale sulla gestione del rischio	Indicazioni per integrare la gestione del rischio connesso all’IA nelle attività dell’organizzazione
NIST AI RMF 1.0	Framework volontario	Funzioni Govern, Map, Measure e Manage per la gestione dei rischi e delle caratteristiche di affidabilità
Ethics Guidelines for Trustworthy AI	Orientamento non vincolante	Principi e requisiti per un’IA lecita, etica e robusta

L’utilizzo degli standard e dei framework richiamati non determina di per sé la conformità all’AI Act. Il Regolamento attribuisce uno specifico valore alle norme armonizzate. Ai sensi dell’articolo 40, i sistemi o modelli conformi alle norme armonizzate i cui riferimenti siano stati pubblicati nella Gazzetta ufficiale dell’Unione europea beneficiano, per i requisiti coperti, di una presunzione di conformità [1]. Standard internazionali come ISO/IEC 42001 e ISO/IEC 23894 e framework come il NIST AI RMF rappresentano invece riferimenti metodologici e organizzativi utili ma la loro adozione non equivale automaticamente alla conformità al Regolamento. È quindi necessario verificare la copertura degli obblighi applicabili e costruire un collegamento esplicito tra requisiti normativi, processi e controlli.

Da un punto di vista operativo, la combinazione tra fonti normative, standard e framework consente di affrontare il problema da prospettive complementari. L’AI Act definisce ciò che deve essere rispettato. Gli standard relativi ai sistemi di gestione aiutano a strutturare il sistema organizzativo necessario. I framework di gestione del rischio supportano l’identificazione e la gestione dei rischi. Gli orientamenti sull’IA affidabile forniscono principi utili per interpretare il comportamento atteso dell’organizzazione. La sfida consiste nel ricondurre tali riferimenti a un unico modello coerente, evitando sovrapposizioni e frammentazione.

1.8 Dalla conformità normativa al modello operativo

L'analisi svolta nelle sezioni precedenti mostra come l'adeguamento all'AI Act non possa essere ridotto alla sola lettura degli articoli del Regolamento o alla produzione di singoli documenti. La normativa definisce criteri di classificazione, ruoli, requisiti e obblighi ma l'organizzazione deve tradurre tali elementi in un sistema capace di funzionare nella pratica. È quindi necessario stabilire come identificare i sistemi, chi debba valutarli, quali criteri utilizzare, quali funzioni coinvolgere, quali evidenze conservare e come monitorare nel tempo la conformità.

Il primo elemento di un modello operativo è la conoscenza del perimetro. Senza un inventario attendibile dei sistemi di IA non è possibile applicare in modo sistematico la normativa. Il censimento deve consentire di raccogliere informazioni sufficienti a comprendere la finalità, le caratteristiche del sistema, i soggetti coinvolti, le modalità di sviluppo o acquisizione e il contesto d'uso. Tali informazioni alimentano i passaggi successivi di classificazione del rischio e determinazione del ruolo regolatorio.

Il secondo elemento è rappresentato da una metodologia decisionale ripetibile. La classificazione non può dipendere esclusivamente dalla valutazione occasionale del singolo soggetto coinvolto ma deve essere supportata da criteri, domande, evidenze e responsabilità definite. Questo vale sia per stabilire se una soluzione rientri nella definizione di sistema di IA sia per determinarne il livello di rischio, il ruolo assunto dall'organizzazione e gli obblighi conseguenti. La standardizzazione del processo consente inoltre di rendere confrontabili le valutazioni e di conservarne nel tempo le motivazioni.

Il terzo elemento riguarda la gestione lungo il ciclo di vita del sistema. Gli obblighi devono essere associati ai momenti nei quali possono essere effettivamente attuati. Alcuni requisiti devono essere considerati in fase di progettazione o acquisizione, altri prima del rilascio e altri ancora durante l'utilizzo o il monitoraggio. Un modello operativo deve quindi integrare la conformità nei processi esistenti di sviluppo, acquisizione, gestione delle modifiche, gestione del rischio e monitoraggio, evitando che la verifica normativa intervenga soltanto alla fine del processo.

Il quarto elemento è il sistema dei controlli. Tradurre un requisito in un controllo significa definire quale comportamento o quale evidenza consenta di dimostrare che il requisito sia stato effettivamente considerato. Un sistema strutturato permette di collegare requisito normativo, rischio, responsabilità, attività di controllo ed evidenza attesa. In questo modo la conformità diventa verificabile e può essere utilizzata come base per l'analisi degli scostamenti e per la definizione delle successive azioni di adeguamento.

Il quinto elemento è la governance organizzativa. Poiché l'IA coinvolge competenze differenti, il modello deve chiarire responsabilità operative, responsabilità di controllo, meccanismi di coinvolgimento decisionale e organi decisionali. È necessario definire chi sia responsabile del sistema, chi supporti la classificazione, chi verifichi gli aspetti legali e di rischio, chi approvi gli scenari più critici e come vengano gestite le responsabilità quando il sistema coinvolge più società o funzioni.

La governance deve quindi garantire una chiara attribuzione delle responsabilità e un adeguato coordinamento.

A questi elementi si aggiunge la necessità di formalizzazione. Politiche, procedure, flussi operativi, liste di controllo e modelli documentali costituiscono gli strumenti attraverso cui il modello viene reso utilizzabile dalle funzioni aziendali. La loro funzione non è soltanto documentale. Tali strumenti traducono criteri astratti in attività ripetibili, rendono più omogenee le valutazioni e consentono di conservare le evidenze delle decisioni assunte.

Infine, il modello deve prevedere un meccanismo di monitoraggio e miglioramento. Nuovi sistemi entrano nel perimetro di governance, sistemi esistenti vengono modificati, cambiano i fornitori e possono cambiare sia la normativa sia gli standard di riferimento. Inventario, classificazioni, controlli e documentazione devono quindi poter essere aggiornati. Le eventuali non conformità devono essere tradotte in azioni con responsabilità, priorità, scadenze e stato di avanzamento, in modo da rendere il percorso di adeguamento governabile nel tempo.

Il passaggio dalla norma al modello operativo può quindi essere ricondotto a sei questioni fondamentali:

- quali sistemi rientrano nel perimetro;
- quale classificazione di rischio si applica;
- quale ruolo assume l'organizzazione;
- quali obblighi ne derivano;
- quali controlli ed evidenze ne consentono la gestione;
- quali soggetti sono responsabili delle decisioni e del monitoraggio.

Affrontare tali questioni richiede strumenti metodologici e organizzativi tra loro integrati. Il valore dell'AI governance risiede proprio in questa capacità di integrazione. Normativa, gestione del rischio, ciclo di vita, controlli e struttura organizzativa non devono essere trattati come componenti indipendenti ma come parti di un unico sistema. L'inventario alimenta la classificazione che, a sua volta, determina requisiti e controlli. I controlli consentono di individuare eventuali scostamenti e di definire le relative azioni di adeguamento. Il monitoraggio delle azioni e l'evoluzione dei sistemi possono infine rendere necessarie nuove valutazioni. La governance coordina l'intero processo e assicura la tracciabilità delle decisioni.

Su queste basi, il capitolo successivo approfondisce la progettazione del modello operativo di AI governance sviluppato nel corso del lavoro e oggetto della tesi. L'attenzione si sposta dal quadro generale alla sua traduzione in processi e strumenti concreti, con particolare riferimento al censimento dei sistemi, alla classificazione del rischio e del ruolo regolatorio, alla definizione del ciclo di vita dei sistemi e alla costruzione del modello organizzativo di governance.

CAPITOLO 2

Progettazione del modello operativo di AI governance

Il passaggio dal quadro normativo descritto nel capitolo precedente a un modello effettivamente utilizzabile in azienda richiede un'attività di progettazione che non può essere ricondotta alla semplice applicazione delle singole disposizioni dell'AI Act. Il Regolamento individua obblighi, responsabilità e condizioni di applicabilità ma non definisce in modo puntuale come tali elementi debbano essere incorporati nei processi decisionali, nei flussi informativi e nelle responsabilità di una specifica organizzazione. Il problema affrontato è stato quindi quello di costruire un'architettura operativa capace di collegare ciascun requisito normativo al momento del ciclo di vita del sistema in cui deve essere gestito, al soggetto responsabile e agli strumenti necessari per documentarne l'attuazione.

La progettazione ha riguardato un'organizzazione caratterizzata da una particolare articolazione degli scenari di utilizzo dell'intelligenza artificiale. A seconda del singolo caso, l'azienda può infatti sviluppare internamente un sistema, acquistarlo da un fornitore, integrarlo in proprie soluzioni, utilizzarlo nei processi aziendali oppure commercializzarlo verso terzi. Ne deriva la possibilità di assumere ruoli regolatori differenti e di essere soggetta, per sistemi diversi, a livelli di obbligo non omogenei. Il modello non poteva quindi essere costruito intorno a un unico scenario tipo ma doveva essere in grado di instradare ciascun sistema verso il percorso coerente con la relativa combinazione di rischio e ruolo.

Il capitolo descrive la progettazione di tale architettura. Vengono prima illustrati i criteri utilizzati per tradurre obblighi e requisiti normativi in elementi operativi; successivamente sono approfonditi il censimento e l'identificazione dei sistemi, la classificazione del rischio e del ruolo, la definizione del ciclo di vita dei sistemi e il modello organizzativo di governance. Una parte specifica è dedicata all'estensione del modello alle società estere del gruppo, per le quali il problema non consiste nella creazione di un ciclo di vita alternativo ma nell'individuare modalità di coordinamento che consentano di applicare il modello comune anche in contesti caratterizzati da strutture organizzative e disponibilità di competenze differenti. La configurazione organizzativa di tale coordinamento costituisce un elemento ancora in fase di affinamento nell'ambito del progetto.

Le attività illustrate non devono essere interpretate come fasi di progetto svolte secondo una sequenza temporale rigida. Nel corso del lavoro, censimento, classificazione, ciclo di vita, governance e definizione degli strumenti si sono evoluti in modo parzialmente parallelo. Le decisioni assunte su una componente hanno spesso richiesto l'aggiornamento di altre componenti, determinando un processo di progressivo affinamento. La struttura adottata nel capitolo segue pertanto una logica funzionale del modello e non la rappresentazione cronologica delle attività svolte.

Per ragioni di riservatezza, nel seguito sono utilizzate denominazioni funzionali convenzionali, definite ai soli fini espositivi, per indicare alcuni ruoli e organi del modello. Tali denominazioni non coincidono necessariamente con quelle adottate dall'organizzazione oggetto del progetto, ma ne sono mantenute inalterate le responsabilità e le logiche operative.

2.1 Dalla normativa ai requisiti operativi

La progettazione del modello ha preso avvio dalla necessità di trasformare un insieme eterogeneo di obblighi e requisiti normativi in elementi concretamente gestibili. L'AI Act stabilisce, ad esempio, obblighi relativi alla gestione del rischio, alla governance dei dati, alla documentazione tecnica, alla registrazione degli eventi, alla trasparenza, alla sorveglianza umana, all'accuratezza, alla robustezza, alla ciphersicurezza, al monitoraggio e alla gestione degli incidenti [1]. Considerati singolarmente, tali obblighi indicano che cosa debba essere assicurato. Per diventare operativi devono però essere associati a un processo, a un responsabile, a un momento del ciclo di vita del sistema e a un'evidenza verificabile.

Sul piano logico, una prima dimensione del lavoro ha riguardato la scomposizione del problema secondo alcune variabili ricorrenti. Per ciascun requisito è stato necessario individuare i sistemi ai quali fosse applicabile, il ruolo regolatorio rilevante, le funzioni aziendali competenti, il momento del ciclo di vita nel quale dovesse essere gestito e gli strumenti necessari a supportarne l'attuazione o la verifica. Questo approccio ha consentito di superare una lettura esclusivamente giuridica della normativa e di ricondurre gli obblighi a un insieme strutturato di attività aziendali.

Una seconda dimensione ha riguardato la costruzione di una logica di applicabilità. Non tutti i sistemi devono infatti seguire lo stesso livello di approfondimento e non tutti gli obblighi si applicano in modo uniforme. La classificazione del rischio e la determinazione del ruolo regolatorio sono state quindi utilizzate come variabili di instradamento del modello. Una volta identificato il sistema, la combinazione tra rischio e ruolo consente di determinare il percorso operativo applicabile e di individuare i controlli e la documentazione pertinenti. Un ruolo centrale in questa traduzione è svolto dal Trusted AI Framework (TAF), implementato operativamente attraverso uno strumento Excel e progressivamente affinato nel corso del lavoro. Al suo interno i controlli applicabili sono organizzati in modo strutturato mentre la relativa applicazione supporta la raccolta e la verifica delle evidenze necessarie. Il TAF costituisce quindi uno dei principali strumenti di raccordo tra normativa e applicazione operativa e sarà approfondito nel capitolo successivo con riferimento alla sua struttura e al suo utilizzo nelle attività di valutazione.

Sulla base dei materiali sviluppati nel progetto e dei riferimenti normativi e metodologici richiamati nel capitolo precedente, l'impostazione adottata può essere sintetizzata attraverso alcuni principi ricorrenti. Tali principi non costituiscono una classificazione formalmente prevista dalla normativa o dalla documentazione progettuale ma rappresentano una chiave di lettura elaborata nell'ambito della presente tesi per ricondurre a sintesi le logiche emerse nel modello. Il primo è la *tracciabilità*: le decisioni relative a identificazione, classificazione, approvazione

e monitoraggio devono poter essere ricostruite nel tempo. Il secondo è la *proporzionalità*: il livello di presidio deve essere proporzionato al rischio e al ruolo regolatorio assunto dall'organizzazione. Il terzo è l'*integrazione nel ciclo di vita*: gli adempimenti devono essere collocati nei punti del processo nei quali possono essere effettivamente influenzate progettazione, sviluppo, acquisizione o utilizzo del sistema. Il quarto è la *responsabilizzazione*: ogni attività deve essere associata a funzioni e ruoli riconoscibili. Il quinto è la *scalabilità*: lo stesso impianto deve poter essere applicato a unità organizzative e società del gruppo caratterizzate da livelli differenti di maturità e disponibilità di risorse.

La Tabella 2.1 sintetizza le principali dimensioni considerate nella traduzione dei requisiti normativi in elementi operativi.

Tabella 2.1: Dimensioni utilizzate nella traduzione dei requisiti normativi

Dimensione	Domanda progettuale	Output atteso
Perimetro	La soluzione rientra nella definizione di sistema di IA e deve essere governata dal modello?	Identificazione del sistema e registrazione nel perimetro di governance
Rischio	Quale livello di rischio regolatorio caratterizza lo specifico caso d'uso?	Classificazione e determinazione del livello di presidio
Ruolo	In quale posizione della catena del valore opera l'organizzazione?	Identificazione degli obblighi del fornitore, del deployer o di altro operatore
Ciclo di vita	In quale momento deve essere gestito il requisito?	Inserimento dell'attività nel processo di progettazione, sviluppo, rilascio o monitoraggio
Responsabilità	Quale funzione possiede competenze e autorità per svolgere o validare l'attività?	Assegnazione delle responsabilità, supporto, consultazione e coinvolgimento dei livelli decisionali competenti
Evidenza	Come può essere dimostrato che l'obbligo è stato considerato e gestito?	Politiche, procedure, liste di controllo, modelli documentali, registrazioni e documentazione

Questa impostazione ha portato a concepire il modello come un insieme di componenti interdipendenti. Il registro dei sistemi fornisce la base informativa; gli strumenti di identificazione e classificazione determinano lo scenario regolatorio; il ciclo di vita stabilisce quando devono essere svolte le attività; il modello organizzativo assegna responsabilità e momenti di validazione; il TAF organizza i controlli e supporta la raccolta delle evidenze necessarie a valutarne l'attuazione. La coerenza del modello dipende quindi dal collegamento tra queste componenti più che dalla completezza del singolo documento.

Un ulteriore elemento progettuale è stato il rapporto con processi e presidi già esistenti. L'introduzione dell'AI Act non implica necessariamente la creazione di strutture completamente separate da quelle utilizzate per rischio, sicurezza, privacy, sviluppo software, acquisti o Internal Audit. Al contrario, uno degli obiettivi è stato individuare i punti nei quali i nuovi requisiti potessero essere incorporati in responsabilità e processi già presenti, introducendo nuovi passaggi soltanto quando le specificità dell'IA lo rendessero necessario. Tale impostazione è coerente con la logica dei sistemi di gestione e con l'esigenza di integrare l'AI governance nella più ampia governance aziendale [12].

La traduzione dei requisiti normativi in elementi operativi non è stata infine considerata un'attività conclusa una volta per tutte. L'evoluzione del quadro normativo, l'affinamento delle interpretazioni e l'esperienza maturata nell'applicazione degli strumenti richiedono che criteri, flussi operativi e responsabilità possano essere aggiornati. Nel corso del lavoro il modello ha quindi assunto un carattere evolutivo: le regole di classificazione, i modelli documentali e i momenti di validazione possono essere progressivamente affinati senza modificare l'impianto complessivo.

2.2 Censimento e identificazione dei sistemi di IA

La costruzione di un modello di governance richiede innanzitutto la conoscenza del perimetro. Un'organizzazione non può applicare criteri di classificazione, controlli o obblighi documentali a sistemi che non è in grado di identificare in modo sistematico. Per questo motivo il censimento dei sistemi di IA rappresenta una componente strutturale del modello e non una semplice attività preliminare da eseguire una sola volta.

Nel contesto progettuale era già disponibile una prima base informativa, costruita attraverso il coinvolgimento delle unità organizzative e la raccolta dei casi d'uso. Tale base è stata assunta come punto di partenza per strutturare un processo più stabile di identificazione e aggiornamento. L'obiettivo non era soltanto disporre di un elenco di sistemi ma costruire un inventario, gestito attraverso un file Excel strutturato, capace di alimentare le decisioni successive di governance.

L'inventario non svolge quindi una funzione esclusivamente anagrafica. Nel medesimo flusso informativo vengono raccolti anche gli elementi necessari alle successive valutazioni di classificazione, tra cui il ruolo regolatorio dell'organizzazione, l'inquadramento rispetto al perimetro dell'AI Act e il livello di rischio associato al caso d'uso. Gli esiti di tali valutazioni confluiscono quindi nell'inventario e ne aggiornano progressivamente il contenuto, evitando di trattare censimento e classificazione come attività supportate da basi informative separate.

La Figura 2.1 mostra un fac-simile semplificato della struttura dell'inventario. Le informazioni sono organizzate in aree funzionali che accompagnano il sistema dall'identificazione alla classificazione, fino alla validazione e alla determinazione del rischio regolatorio. I dati riportati sono fittizi e hanno finalità esclusivamente illustrative.

AI_Systems_Inventory.xlsx							Dati fittizi
Identificazione			Classificazione		Validazione e rischio		
AREA	USE CASE	SPoC	REGULATORY ROLE	AI ACT SCOPE	AI CHECKLIST	AI REGULATORY RISK	
BU_01	System_A Assistente virtuale	Owner_01	Deployer	IN SCOPE	Validata		LIMITED RISK
BU_01	System_B Screening candidature	Owner_02	Deployer	IN SCOPE	Validata		HIGH RISK
BU_02	System_C Sintesi di testi	Owner_03	Provider	IN SCOPE	Validata		MINIMAL RISK
BU_02	System_D Automazione processi	Owner_03	N/A	OUT OF SCOPE	Validata		N/A
BU_03	System_E Raccomandazioni	Owner_04	Provider	IN SCOPE	To do		TBD
...							
COVER OVERALL DASHBOARD							

Figura 2.1: Fac-simile semplificato dell’inventario dei sistemi di IA (dati fittizi)

Il processo di identificazione è stato progettato come un flusso a più passaggi. Il punto di ingresso è costituito dall’emersione di una nuova esigenza di business o da una modifica rilevante di una soluzione già esistente. Il soggetto richiedente avvia quindi una prima valutazione volta a comprendere se la soluzione rientri nel perimetro dell’intelligenza artificiale ai sensi del Regolamento. A supporto di questa attività è stato previsto uno strumento strutturato di identificazione, composto da domande preliminari e da una sezione dedicata alle principali caratteristiche del sistema.

La logica dello strumento è stata costruita per ridurre due rischi opposti. Il primo è quello di escludere dal perimetro soluzioni che, pur non essendo percepite internamente come sistemi di IA, presentano le caratteristiche rilevanti ai sensi della normativa. Il secondo è quello di includere software nei quali non ricorrono gli elementi della definizione regolatoria. Per questo motivo la fase di identificazione considera, tra gli altri elementi, la natura automatizzata del sistema, il livello di autonomia, l’eventuale adattabilità e la capacità di dedurre dagli input ricevuti come generare output, in coerenza con la definizione di sistema di IA richiamata nel capitolo precedente [1].

Una volta confermata l’appartenenza al perimetro, il processo prosegue con la raccolta delle informazioni necessarie alla classificazione. Il modello prevede quindi che l’identificazione non si esaurisca in una risposta binaria ma produca un insieme informativo riutilizzabile nelle fasi successive. Tra le informazioni rilevanti rientrano la finalità del sistema, il contesto di utilizzo, la relazione con eventuali fornitori, l’eventuale sviluppo interno, il soggetto che ne richiede l’introduzione e gli elementi necessari a comprendere se l’organizzazione operi come fornitore o deployer.

Il censimento è stato inoltre collegato a un processo di validazione. La prima compilazione è attribuita al soggetto che conosce il caso d’uso e le caratteristiche operative del sistema. La funzione legale interviene invece per verificare la corretta

qualificazione regolatoria e curare la formalizzazione della registrazione. Questa separazione risponde a un'esigenza di qualità del dato: le informazioni di business e tecniche provengono da chi conosce il sistema mentre l'inquadramento normativo viene validato dalla funzione che presidia l'interpretazione della disciplina applicabile.

Il registro assume così una duplice funzione. Da un lato è un inventario in quanto consente di conoscere quali sistemi siano presenti nel perimetro. Dall'altro è un meccanismo di governance poiché rende visibili classificazione, responsabilità e stato del sistema lungo il ciclo di vita. In questa seconda prospettiva, il valore del registro non dipende soltanto dalla sua completezza iniziale ma soprattutto dalla capacità di mantenerlo aggiornato quando cambiano finalità, caratteristiche, fornitori, modalità di utilizzo o responsabilità interne.

L'aggiornamento del registro è stato quindi concepito come un'attività continua. L'introduzione di una modifica rilevante, un nuovo contesto di utilizzo o una variazione della finalità può richiedere una nuova valutazione del rischio e del ruolo regolatorio. Il registro deve poter riflettere tali cambiamenti e mantenere la tracciabilità delle decisioni. Questo principio è particolarmente rilevante perché, come evidenziato nel capitolo precedente, sia il rischio sia il ruolo possono cambiare nel tempo in funzione dell'evoluzione del sistema e del modo in cui esso viene utilizzato.

La dimensione di gruppo ha introdotto un'ulteriore esigenza: distinguere tra visibilità locale e visibilità centrale. Nel modello è stata considerata la possibilità di mantenere inventari locali presso le singole società, assicurando al tempo stesso l'alimentazione di un inventario globale. Tale configurazione consentirebbe di preservare la conoscenza del contesto locale e, contemporaneamente, di fornire al livello centrale una vista consolidata dei sistemi, dei relativi ruoli e del profilo di rischio. Le modalità di coordinamento tra i due livelli sono approfondite nelle sezioni dedicate alla governance di gruppo.

Il censimento e l'identificazione costituiscono quindi il primo snodo del modello operativo. Senza questa base informativa non sarebbe possibile applicare in modo coerente le regole di classificazione, attribuire le responsabilità, selezionare il percorso operativo applicabile o monitorare nel tempo il livello di conformità. Il passaggio successivo consiste pertanto nella determinazione del rischio regolatorio e del ruolo assunto dall'organizzazione.

2.3 Classificazione del rischio e determinazione del ruolo regolatorio

Le informazioni raccolte nell'inventario costituiscono la base per la determinazione del rischio e del ruolo regolatorio. La classificazione non viene quindi gestita come uno strumento informativo separato, ma come una fase del processo di valutazione i cui esiti vengono registrati e mantenuti all'interno dell'inventario.

Una volta identificato il sistema, il modello richiede di determinare due elementi distinti ma strettamente collegati: il livello di rischio regolatorio e il ruolo assunto dall'organizzazione. La combinazione di tali variabili costituisce la principale

logica di instradamento del processo perché consente di associare al singolo caso d'uso il percorso operativo, i controlli e la documentazione applicabili.

La classificazione del rischio è stata strutturata a partire dal quadro basato sul rischio dell'AI Act e dalla relativa traduzione operativa adottata nel progetto. Il processo prevede una prima valutazione effettuata dal soggetto richiedente, eventualmente con il supporto delle funzioni tecniche coinvolte, seguita da una validazione della funzione legale. La scelta di articolare la classificazione in due momenti risponde all'esigenza di combinare conoscenza del caso d'uso e competenza normativa: il soggetto richiedente conosce finalità, funzionamento e contesto del sistema mentre la funzione legale verifica la coerenza della qualificazione rispetto ai criteri regolatori.

La prima verifica riguarda l'eventuale presenza di pratiche vietate. Qualora il caso d'uso rientri in una delle fattispecie dell'articolo 5, il modello non prevede un percorso di adeguamento volto a rendere il sistema conforme ma l'interruzione o la revisione dello scenario. Per i sistemi non vietati, l'analisi prosegue con la verifica delle condizioni previste per i sistemi ad alto rischio dall'articolo 6 e dagli allegati I e III, tenendo conto della finalità e del contesto di utilizzo. I sistemi che non ricadono nel perimetro dell'alto rischio vengono quindi valutati rispetto agli eventuali obblighi di trasparenza e, in assenza di ulteriori requisiti specifici, ricondotti a un percorso semplificato [1].

La seconda dimensione è il ruolo regolatorio. Anche in questo caso il modello non associa il ruolo all'organizzazione in modo statico ma al singolo sistema e allo specifico scenario. Lo sviluppo interno e la successiva immissione sul mercato o messa in servizio sotto il proprio nome o marchio possono determinare l'assunzione del ruolo di fornitore. L'utilizzo professionale di una soluzione acquistata da terzi determina invece, in linea generale, il ruolo di deployer. Devono inoltre essere considerate le situazioni nelle quali modifiche sostanziali, variazioni della finalità o modalità di commercializzazione possono determinare un cambio di ruolo ai sensi dell'articolo 25 [1].

Nel modello, rischio e ruolo sono stati combinati in una matrice di scenari regolatori utilizzata come riferimento operativo per la costruzione dei diversi percorsi. Coerentemente con i casi d'uso emersi nel perimetro progettuale, la matrice è stata sviluppata con riferimento ai ruoli di fornitore e deployer, poiché alla data di redazione non sono emersi casi riconducibili agli ulteriori ruoli previsti dal Regolamento.

La matrice distingue cinque scenari principali: sistemi ad alto rischio con ruolo di fornitore, sistemi ad alto rischio con ruolo di deployer, sistemi a rischio limitato con ruolo di fornitore, sistemi a rischio limitato con ruolo di deployer e sistemi a rischio minimo. Tali etichette sono utilizzate nel modello a fini operativi e non devono essere intese come categorie giuridiche omogenee formalmente definite dal Regolamento. Il caso delle pratiche vietate è trattato a monte perché non genera un percorso di sviluppo o utilizzo ordinario.

La Tabella 2.2 sintetizza i principali scenari regolatori utilizzati nel modello e la relativa impostazione del percorso operativo.

Tabella 2.2: Scenari regolatori utilizzati nel modello operativo

N.	Rischio	Ruolo	Impostazione del percorso
1	Alto rischio	Fornitore	Percorso completo con requisiti di sviluppo, documentazione, conformità, rilascio e monitoraggio
2	Alto rischio	Deployer	Percorso centrato su valutazione del fornitore, uso conforme, FRIA ove applicabile, sorveglianza umana, monitoraggio e gestione degli incidenti
3	Rischio limitato	Fornitore	Percorso proporzionato agli obblighi di documentazione e trasparenza applicabili
4	Rischio limitato	Deployer	Percorso semplificato basato su verifica della documentazione, trasparenza e corretto utilizzo
5	Rischio minimo	–	Presidio semplificato definito nel modello, con registrazione e gestione coerenti con le regole interne applicabili

La matrice consente di ricondurre a una struttura operativa un insieme di obblighi che il Regolamento distribuisce tra disposizioni differenti e attribuisce a soggetti diversi. Una volta determinati il livello di rischio e il ruolo regolatorio, il sistema può essere associato al percorso applicabile e alle relative attività di conformità. In questo modo, la complessità normativa viene tradotta in un insieme limitato di scenari utilizzabili come riferimento dalle funzioni aziendali.

Particolare attenzione è stata dedicata alla distinzione tra fornitore e deployer per i sistemi ad alto rischio. Nel primo caso il modello deve presidiare la conformità del sistema in quanto tale, includendo aspetti quali documentazione tecnica, governance dei dati, registrazione degli eventi, robustezza, gestione del rischio, valutazione di conformità, dichiarazione UE di conformità e monitoraggio successivo all'immissione sul mercato. Nel secondo caso, invece, l'organizzazione è soggetta agli obblighi previsti per il deployer e deve assicurare che l'utilizzo avvenga nel rispetto delle istruzioni e delle condizioni applicabili, predisponendo adeguate misure di sorveglianza umana e monitorando il funzionamento del sistema nel proprio contesto operativo. Nel modello progettuale, tali obblighi si traducono inoltre nella verifica della documentazione ricevuta dal fornitore e, quando applicabile, nello svolgimento della FRIA. Restano ferme le situazioni nelle quali, ricorrendo le condizioni previste dall'articolo 25, l'organizzazione può assumere a sua volta il ruolo di fornitore [1].

Anche gli scenari a rischio limitato sono stati differenziati per evitare un approccio eccessivamente oneroso. Coerentemente con la chiave di lettura pro-

posta nel presente lavoro, il livello di presidio è stato interpretato in termini di proporzionalità rispetto agli obblighi applicabili e alla criticità dello scenario. I casi caratterizzati principalmente da obblighi di trasparenza sono stati quindi ricondotti a un percorso meno articolato rispetto a quello previsto per i sistemi ad alto rischio, fermo restando il controllo della finalità, della documentazione e delle condizioni di utilizzo. Le modalità di validazione e di eventuale coinvolgimento dei livelli decisionali competenti per tali scenari sono state oggetto di progressivo affinamento nel corso del lavoro.

La classificazione non è stata concepita come una decisione immutabile. Una variazione della finalità, una modifica sostanziale, l'introduzione di nuove funzionalità o il trasferimento del sistema a un differente contesto possono alterare il rischio o il ruolo. Il modello prevede pertanto che cambiamenti significativi attivino una nuova valutazione e, se necessario, il passaggio a un percorso operativo diverso. Questa logica rende classificazione e ciclo di vita strettamente interdipendenti.

Il risultato della fase di classificazione non è quindi soltanto un'etichetta regolatoria. Esso determina il percorso organizzativo del sistema, le funzioni da coinvolgere, il livello di approvazione richiesto e la documentazione da predisporre. Per rendere questa logica utilizzabile nel tempo è stato necessario collocare tali attività all'interno di un ciclo di vita comune e riconoscibile, oggetto della sezione successiva.

2.4 L'AI Lifecycle: fasi, attività e responsabilità

Nel progetto, con *AI Lifecycle* si indica la rappresentazione strutturata del ciclo di vita di un sistema di IA, dalla nascita dell'esigenza fino alle attività successive al rilascio o all'avvio dell'utilizzo. Tale rappresentazione è stata formalizzata in un documento Word che organizza, per ciascuna fase, le attività da svolgere, le funzioni coinvolte, le responsabilità, gli eventuali momenti di validazione e la documentazione da produrre o aggiornare. L'*AI Lifecycle* non costituisce quindi una semplice successione temporale di fasi ma lo schema operativo attraverso cui viene strutturata la gestione del sistema lungo il suo ciclo di vita.

Questa impostazione consente di trasformare la classificazione regolatoria in un percorso concretamente applicabile. Una volta determinati il rischio e il ruolo dell'organizzazione, il sistema viene infatti associato al relativo workflow e le attività di conformità vengono collocate nel punto del ciclo di vita in cui devono essere effettivamente eseguite. L'*AI Lifecycle* costituisce quindi il raccordo tra classificazione, attività operative, responsabilità organizzative e strumenti documentali del modello.

A livello di sintesi, il ciclo di vita è stato articolato in tre macrofasi: *Design*, *Development* e *Post Production*. Tale articolazione rappresenta una struttura comune di riferimento, mentre il contenuto delle singole fasi varia in funzione della combinazione tra rischio e ruolo regolatorio. In questo senso, non esiste un unico percorso identico per tutti i sistemi ma più workflow costruiti all'interno della medesima logica di *AI Lifecycle*.

La fase di *Design* rappresenta il punto di ingresso nel ciclo di vita ed è comune ai diversi scenari. In questa fase emerge l'esigenza di business, viene verificata

l'appartenenza della soluzione al perimetro dell'IA, sono determinati il rischio e il ruolo regolatorio e viene avviata la registrazione del sistema nell'inventario. A tali attività si affianca l'individuazione dei requisiti applicabili e delle funzioni che dovranno contribuire alle fasi successive. La fase di Design assume quindi una funzione di instradamento: definisce il percorso che il sistema dovrà seguire e rende esplicite, fin dall'inizio, le responsabilità necessarie per governarlo.

La fase di *Development* comprende le attività necessarie a preparare il sistema al rilascio, alla messa in servizio o all'utilizzo, con contenuti che dipendono dallo scenario regolatorio. Quando l'organizzazione opera come fornitore, l'*AI Lifecycle* include attività di progettazione e sviluppo, governance dei dati, test, registrazione degli eventi, sorveglianza umana, robustezza, cibersecurity, gestione del rischio e predisposizione della documentazione richiesta per la conformità. Quando l'organizzazione opera come deployer, il percorso è invece incentrato sulla documentazione ricevuta dal fornitore, sulle condizioni di utilizzo, sulle misure organizzative e di sorveglianza e, nei casi ad alto rischio, sulle ulteriori valutazioni richieste al soggetto utilizzatore.

Le differenze tra i workflow possono essere lette, ai fini del presente lavoro, secondo la chiave della proporzionalità. I sistemi ad alto rischio seguono il percorso più articolato mentre, per i sistemi a rischio limitato, le attività sono più circoscritte e direttamente collegate agli obblighi applicabili. Nel caso dei sistemi a rischio limitato utilizzati in qualità di deployer, ad esempio, il percorso si concentra soprattutto sulla verifica della documentazione del fornitore, sugli obblighi di trasparenza e sulle condizioni necessarie all'utilizzo. Per i sistemi a rischio minimo non è invece previsto un percorso di Development strutturato analogo a quello degli altri scenari, ferma restando l'applicazione delle regole interne e dei presidi informativi previsti dal modello.

La fase di *Post Production* copre il periodo successivo al rilascio o all'avvio dell'utilizzo e completa il ciclo di vita del sistema attraverso le attività di monitoraggio e mantenimento. Per gli scenari ai quali essa si applica comprende l'aggiornamento dell'inventario, il monitoraggio delle prestazioni e degli indicatori rilevanti, la gestione degli incidenti, le eventuali azioni correttive e la rivalutazione del sistema quando intervengono cambiamenti significativi. Per i fornitori di sistemi ad alto rischio tale fase si collega direttamente al monitoraggio successivo all'immissione sul mercato previsto dall'AI Act. Per i deployer, invece, riguarda soprattutto il controllo del corretto utilizzo e la capacità di individuare anomalie o condizioni che richiedano il coinvolgimento delle funzioni e degli organi di governance competenti [1].

L'*AI Lifecycle* non deve inoltre essere interpretato come una rappresentazione statica. Una modifica della finalità, delle caratteristiche tecniche, del contesto di utilizzo o del ruolo regolatorio può richiedere di ripercorrere alcune attività già svolte, aggiornare la documentazione o attivare nuove valutazioni. Il modello assume quindi una logica ciclica: le informazioni prodotte durante sviluppo e monitoraggio possono riportare il sistema verso fasi precedenti dell'*AI Lifecycle*, mantenendo nel tempo coerenza tra rischio, ruolo, responsabilità e stato di conformità.

La Tabella 2.3 sintetizza le tre macrofasi dell'*AI Lifecycle*, i relativi obiettivi e

le principali attività associate.

Tabella 2.3: Struttura di sintesi dell'AI Lifecycle nel modello operativo

Macrofase	Obiettivo	Principali attività
Design	Identificare il sistema e determinarne il percorso applicabile	Esigenza di business, identificazione del sistema di IA, classificazione del rischio e del ruolo, registrazione nell'inventario, prima individuazione dei requisiti applicabili
Development	Predisporre il sistema e la documentazione necessari al rilascio, alla messa in servizio o all'utilizzo	Attività tecniche, organizzative e documentali differenziate in funzione di rischio e ruolo; test, misure di controllo, verifiche sul fornitore e preparazione al rilascio
Post Production	Assicurare il presidio del sistema dopo il rilascio o l'avvio dell'utilizzo	Monitoraggio, aggiornamento dell'inventario, gestione degli incidenti, azioni correttive, verifiche periodiche e rivalutazione in caso di cambiamenti

All'interno delle macrofasi sono stati previsti specifici momenti di validazione. Per gli scenari più critici e in particolare per i sistemi ad alto rischio, il passaggio verso lo sviluppo o il rilascio può richiedere il coinvolgimento degli organi di governance competenti. La definizione di tali momenti è stata progressivamente affinata nel corso del lavoro con l'obiettivo di bilanciare due esigenze: garantire un adeguato livello di controllo sui sistemi più rilevanti ed evitare un modello nel quale ogni decisione operativa debba essere sottoposta ai livelli decisionali più elevati. La logica progressivamente adottata è stata quindi quella di concentrare i momenti formali di validazione sui sistemi ad alto rischio e sui casi che, per criticità o impatto, richiedano il coinvolgimento dei livelli decisionali superiori, mantenendo invece percorsi più proporzionati per gli scenari meno complessi.

L'*AI Lifecycle* comprende inoltre attività trasversali che non possono essere ricondotte a un unico momento. La gestione delle modifiche accompagna l'intera vita del sistema poiché una variazione può incidere sulle prestazioni, sul rischio, sulla documentazione e sulla classificazione. Analogamente, la tracciabilità delle decisioni e l'aggiornamento dell'inventario devono essere garantiti in modo continuativo.

L'*AI Lifecycle* non deve essere confuso con la sequenza temporale delle attività progettuali che hanno portato alla sua definizione. Il primo rappresenta il percorso logico associato al sistema di IA mentre il secondo si è sviluppato in modo iterativo, attraverso attività parallele e successivi affinamenti. La struttura qui descritta presenta pertanto il modello risultante secondo una sequenza funzionale, senza

attribuire alle attività una linearità temporale che non ne ha caratterizzato lo svolgimento. La Figura 2.2 ne sintetizza graficamente l'articolazione complessiva.



Figura 2.2: Struttura dell'AI Lifecycle nel modello operativo

La definizione di un *AI Lifecycle* comune ha infine fornito la base per affrontare il problema organizzativo. Una volta individuate le attività da svolgere e il momento nel quale devono essere eseguite è infatti possibile attribuire responsabilità operative e di supporto, definire i ruoli di validazione e stabilire quando sia necessario coinvolgere livelli decisionali superiori. La sezione successiva descrive quindi il modello organizzativo progettato per rendere operativo l'*AI Lifecycle*.

2.5 Progettazione del modello organizzativo di AI governance

La definizione dell'*AI Lifecycle* rende visibili le attività da presidiare ma non è sufficiente a garantire che esse vengano effettivamente svolte. Per questo motivo una parte centrale del lavoro progettuale ha riguardato la costruzione del modello organizzativo di AI governance, con l'obiettivo di attribuire responsabilità chiare e di definire i meccanismi attraverso cui le diverse funzioni aziendali interagiscono lungo l'*AI Lifecycle*.

Il problema organizzativo è reso complesso dalla natura trasversale dell'IA. La stessa iniziativa può richiedere conoscenze di business, competenze tecniche, valutazioni legali, gestione del rischio, protezione dei dati, cibersicurezza e attività di controllo. Nessuna di queste funzioni, considerata isolatamente, dispone di tutte le informazioni e di tutte le competenze necessarie per governare il sistema. Il modello è stato quindi costruito evitando di concentrare la responsabilità dell'IA in una sola struttura e definendo invece un sistema di responsabilità distribuite ma coordinate.

La progettazione ha distinto tre componenti organizzative principali. La prima comprende i ruoli operativi e di delivery, ossia i soggetti che propongono, sviluppano, integrano o utilizzano i sistemi. La seconda riguarda le funzioni

di controllo e supporto, chiamate a presidiare gli aspetti normativi, di rischio, sicurezza e controllo. La terza è costituita dagli organi di governance, ai quali sono attribuite funzioni di indirizzo, coordinamento, validazione e gestione dei casi che richiedono un livello decisionale superiore. Questa articolazione consente di mantenere la responsabilità sul sistema vicina al business e alle funzioni tecniche, senza rinunciare a un presidio trasversale sui casi più rilevanti.

Il modello è stato rappresentato anche attraverso matrici RACI (*Responsible, Accountable, Consulted, Informed*), utilizzate per distinguere chi esegue una determinata attività, chi ne detiene la responsabilità ultima, quali soggetti devono essere consultati e quali devono essere informati. La RACI non costituisce tuttavia il modello in sé ma uno strumento di formalizzazione: il suo valore dipende dalla coerenza con le attività previste dall'*AI Lifecycle* e dalla possibilità di aggiornare le assegnazioni quando cambia l'organizzazione.

Nel modello, la distribuzione delle responsabilità si traduce anche nella distinzione tra un organo con funzione prevalentemente consultiva e di coordinamento, indicato nel seguito come *AI Advisory Committee*, e un organo con funzione decisionale e di indirizzo, indicato come *AI Governance Committee*.

Particolare attenzione è stata dedicata ai meccanismi di coinvolgimento dei livelli decisionali superiori. Un modello nel quale ogni sistema debba essere sottoposto sistematicamente all'organo decisionale rischierebbe di diventare lento e poco sostenibile. Al contrario, un modello completamente decentralizzato potrebbe generare interpretazioni disomogenee e ridurre la visibilità sui casi critici. La soluzione progettuale ha quindi cercato di distinguere le attività ordinarie, gestite dalle funzioni competenti con il supporto dell'*AI Advisory Committee*, dai casi nei quali la criticità o l'impatto richiedono il coinvolgimento dell'*AI Governance Committee*.

La stessa logica è stata successivamente considerata anche nell'estensione del modello alla dimensione di gruppo. In tale contesto, il problema consiste nel garantire la copertura delle attività dell'*AI Lifecycle* anche nelle società estere, caratterizzate da strutture organizzative e disponibilità di competenze differenti. Tra le soluzioni approfondite nel corso del lavoro è stata considerata una distribuzione delle responsabilità nella quale il processo rimane comune mentre l'esecuzione delle singole attività può essere affidata, in funzione delle competenze disponibili, a una funzione locale, a un referente funzionale o al livello centrale. La configurazione organizzativa complessiva e i relativi flussi di coordinamento risultano tuttavia ancora in fase di affinamento. Questi aspetti sono approfonditi nelle sottosezioni successive dedicate alla governance di gruppo e al coordinamento tra livello centrale e società estere.

2.5.1 Ruoli, responsabilità e organi di governance

Tra i ruoli operativi, il primo riferimento è l'*AI Business Owner*, ossia il soggetto che rappresenta il bisogno di business e presidia il caso d'uso dal punto di vista funzionale. A questo ruolo sono attribuiti l'identificazione del caso d'uso, la definizione della finalità, la raccolta delle informazioni necessarie alla classificazione e il coordinamento con le funzioni coinvolte. L'*AI Business Owner* costituisce

quindi il punto di contatto tra esigenza di business e processo di governance e rimane rilevante anche dopo il rilascio, in particolare per le attività di monitoraggio e per la gestione degli eventuali cambiamenti.

L'*AI Technical Team* rappresenta invece il presidio tecnico e di implementazione del sistema. Nei casi di sviluppo interno, è il team che progetta, sviluppa e programma concretamente la soluzione di IA. Negli altri scenari ne cura l'integrazione tecnica o supporta l'utilizzo della soluzione acquisita da terzi. Contribuisce inoltre alla predisposizione della documentazione tecnica. Rientrano nel suo perimetro attività quali la tracciabilità delle modifiche, la gestione dei dati, i test, la registrazione degli eventi, l'implementazione delle misure di sorveglianza umana e il supporto alle verifiche tecniche previste dall'*AI Lifecycle*. La distinzione tra *AI Business Owner* e *AI Technical Team* consente di separare la responsabilità sul bisogno e sull'utilizzo del sistema dalla responsabilità sulle attività tecniche necessarie a realizzarlo, svilupparlo o integrarlo.

La funzione legale svolge un ruolo trasversale lungo il processo. Tra le attività principali rientrano la validazione della classificazione regolatoria, il presidio del registro, la verifica documentale, il supporto agli obblighi di trasparenza e, nei casi applicabili, la gestione degli aspetti connessi alla FRIA, alla valutazione di conformità, alla registrazione nella banca dati dell'Unione e alla marcatura CE. Il ruolo della funzione legale non sostituisce tuttavia quello delle funzioni tecniche o di rischio: il modello è costruito proprio sulla separazione tra interpretazione normativa, responsabilità sul sistema e capacità di attuazione delle misure.

La funzione di Enterprise Risk Management (ERM) presidia la dimensione di rischio aziendale connessa ai sistemi di IA. A essa è attribuito il compito di definire criteri e metodologie per la valutazione dei rischi specifici, supportare la determinazione delle misure di trattamento e contribuire all'integrazione dell'IA nel più ampio sistema aziendale di gestione del rischio. La funzione di Internal Audit svolge invece verifiche periodiche e indipendenti sull'effettivo funzionamento dei processi e dei controlli.

Le funzioni tecnologiche e di sicurezza intervengono nei requisiti che richiedono competenze specialistiche. Il perimetro comprende, tra gli altri, registrazione degli eventi, test, strumenti tecnici, robustezza, cibersicurezza e monitoraggio delle misure di sicurezza. Nel modello organizzativo tali funzioni operano in coordinamento con l'ERM per garantire che le misure tecniche siano coerenti con il profilo di rischio e con le esigenze di controllo definite a livello aziendale.

A questi ruoli si affiancano i due organi di governance già richiamati, con funzioni differenziate: l'*AI Advisory Committee* e l'*AI Governance Committee*. L'*AI Advisory Committee* è stato concepito come organo consultivo e di coordinamento. La sua composizione riunisce competenze differenti, tra cui competenze legali, di rischio, di sicurezza, tecnologiche e specialistiche sull'IA. L'*AI Advisory Committee* supporta la definizione di politiche, procedure, metodologie e strumenti, coordina i temi di conformità, monitora l'evoluzione normativa e fornisce supporto agli *AI Business Owner* e alle funzioni operative nei casi che richiedono una lettura trasversale.

L'*AI Advisory Committee* svolge inoltre una funzione di filtro e preparazione dei casi da sottoporre al livello decisionale superiore. La logica progettuale è evitare

che ogni caso d'uso venga sottoposto automaticamente al livello decisionale più elevato. L'*AI Advisory Committee* mantiene visibilità sulle iniziative, individua i casi che presentano criticità o impatto significativo e prepara gli elementi necessari per la valutazione da parte dell'*AI Governance Committee*. Questa funzione è particolarmente importante in un contesto nel quale il numero dei sistemi può crescere nel tempo e che rende necessario bilanciare controllo e sostenibilità del processo.

L'*AI Governance Committee* rappresenta il livello di indirizzo e validazione. A esso sono attribuite le decisioni relative alla strategia di AI governance, all'approvazione del modello operativo, delle politiche e degli standard interni, nonché la gestione delle eccezioni e dei casi particolarmente critici o sottoposti al livello decisionale superiore. Per gli scenari più rilevanti, il Committee può intervenire in corrispondenza dei principali momenti di validazione dell'*AI Lifecycle*, ad esempio prima dell'avvio dello sviluppo o del rilascio. Il perimetro esatto di tali momenti di validazione è stato oggetto di affinamento nel corso del lavoro, con l'obiettivo di riservare l'intervento formale dell'*AI Governance Committee* ai casi nei quali sia realmente necessario un livello decisionale superiore.

Tra *AI Advisory Committee* e *AI Governance Committee* è stata inoltre prevista, nel disegno organizzativo, una funzione di raccordo, indicata nel presente lavoro come *AI Governance Coordinator*. L'individuazione della funzione aziendale chiamata a ricoprire tale ruolo risulta ancora oggetto di definizione. Il suo compito è assicurare continuità nel flusso informativo, consolidare le raccomandazioni dell'*AI Advisory Committee*, predisporre gli elementi da portare al livello decisionale superiore e riportare le decisioni alle funzioni interessate. Questa figura riduce il rischio di frammentazione tra organo consultivo e organo decisionale e rende più chiaro il percorso dei casi che richiedono il coinvolgimento del livello decisionale superiore.

La Tabella 2.4 sintetizza i principali ruoli e funzioni previsti nel modello organizzativo e le rispettive responsabilità prevalenti.

Tabella 2.4: Ruoli principali nel modello organizzativo di AI governance

Ruolo / funzione	Responsabilità prevalente nel modello
AI Business Owner	Definizione del bisogno e della finalità, presidio funzionale del caso d'uso e coordinamento delle attività
AI Technical Team	Progettazione, sviluppo o integrazione tecnica del sistema; documentazione, dati, test e registrazione degli eventi
Funzione legale	Validazione regolatoria, presidio del registro, verifica documentale, trasparenza e adempimenti legali applicabili
ERM	Definizione delle metodologie di rischio e integrazione con il sistema aziendale di gestione del rischio
Funzioni tecnologiche e di sicurezza	Presidio specialistico di tecnologia, robustezza, cibersecurity, registrazione degli eventi e misure tecniche
Internal Audit	Verifiche periodiche e indipendenti sul funzionamento della governance e dei relativi controlli
AI Advisory Committee	Coordinamento consultivo, supporto alle funzioni, definizione di metodologie e preparazione dei casi da sottoporre al livello decisionale superiore
AI Governance Committee	Indirizzo strategico, validazione del modello e decisione sui casi critici o sottoposti al livello decisionale superiore
AI Governance Coordinator	Raccordo tra i due organi di governance e gestione del flusso informativo; assegnazione organizzativa ancora in definizione

Il modello organizzativo non è stato quindi progettato come una struttura autonoma e separata dal resto dell'azienda. Esso valorizza ruoli e competenze già presenti, introducendo organi e meccanismi di coordinamento ove necessario. Questa impostazione consente di integrare l'AI governance nei processi aziendali mantenendo, al tempo stesso, un presidio trasversale sui temi che richiedono il coinvolgimento di più funzioni. La Figura 2.3 sintetizza graficamente l'articolazione dei principali ruoli e dei relativi collegamenti nel modello organizzativo. La necessità di coordinamento assume particolare rilevanza in presenza di un'articolazione organizzativa internazionale, caratterizzata da realtà locali con strutture e livelli di specializzazione non omogenei. Proprio questa eterogeneità ha reso necessario approfondire le modalità con cui il modello comune possa essere esteso e coordinato anche nelle realtà estere, tema affrontato nelle sottosezioni successive.

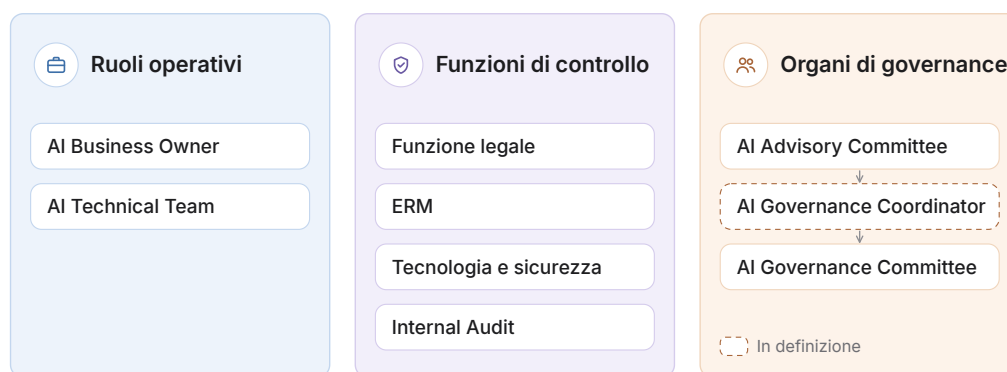


Figura 2.3: Articolazione dei ruoli nel modello organizzativo di AI governance

2.5.2 La governance a livello di gruppo

L'estensione del modello alla dimensione internazionale ha introdotto un'ulteriore esigenza progettuale. Le realtà estere ricomprese nel perimetro del gruppo presentano infatti dimensioni, strutture organizzative e livelli di specializzazione differenti. In alcuni contesti sono disponibili localmente competenze legali, di rischio, di sicurezza o tecnologiche mentre in altri il presidio di tali ambiti richiede un maggiore supporto da parte del livello centrale. Assumere una perfetta simmetria organizzativa tra tutte le realtà avrebbe quindi reso il modello difficilmente applicabile.

Nell'estensione del modello alla dimensione di gruppo, l'impostazione progettuale considerata ha mantenuto come riferimento un unico *AI Lifecycle*. I criteri di identificazione e classificazione, la determinazione del ruolo regolatorio e i percorsi operativi rimangono quindi comuni, mentre può variare il soggetto chiamato a presidiare le singole attività in funzione delle competenze effettivamente disponibili nei diversi contesti. L'obiettivo è preservare la coerenza del modello senza introdurre cicli di vita distinti per ciascuna realtà.

Questa impostazione mira a limitare due forme di frammentazione. La prima è di natura metodologica e si verificherebbe se le diverse realtà adottassero criteri autonomi di identificazione, classificazione e monitoraggio. La seconda è di natura informativa e ridurrebbe la possibilità di mantenere una visione consolidata sui sistemi di IA e sui relativi profili di rischio. Il riferimento a criteri, strumenti e flussi comuni consente invece di rendere le informazioni maggiormente confrontabili e di mantenere una base di governance coerente a livello di gruppo.

È emersa, allo stesso tempo, la necessità di distinguere tra attività che richiedono un presidio comune e attività che dipendono maggiormente dalla conoscenza del contesto locale. La definizione di principi, metodologie e strumenti condivisi così come il mantenimento di una visibilità complessiva sui sistemi più rilevanti richiede un coordinamento a livello centrale. L'identificazione del bisogno, la descrizione del caso d'uso e la raccolta delle informazioni sul contesto operativo richiedono invece il coinvolgimento diretto delle realtà interessate.

La definizione puntuale della distribuzione delle responsabilità tra livello centrale e realtà locali non risulta tuttavia ancora definitivamente formalizzata. Il lavoro progettuale si è quindi concentrato sul confronto tra configurazioni caratterizzate da differenti livelli di centralizzazione con l'obiettivo di individuare un assetto capace di bilanciare uniformità, conoscenza del contesto locale e sostenibilità operativa. Le alternative considerate sono approfondite nella sottosezione successiva.

2.5.3 Confronto qualitativo delle configurazioni organizzative

Nell'ambito della definizione della governance delle realtà estere sono state considerate configurazioni caratterizzate da differenti livelli di centralizzazione. La valutazione non ha riguardato soltanto la distribuzione formale delle responsabilità ma anche la capacità delle diverse soluzioni di funzionare in un contesto organizzativo eterogeneo. Tra i principali criteri di confronto sono stati considerati l'uniformità delle decisioni, la conoscenza del contesto locale, la disponibilità di competenze specialistiche, la rapidità del processo, la scalabilità e la capacità del livello centrale di mantenere una visibilità adeguata sui sistemi più rilevanti.

Una configurazione fortemente centralizzata presenta il vantaggio di favorire una maggiore uniformità nell'interpretazione della normativa, nella classificazione e nell'utilizzo degli strumenti comuni. La concentrazione delle attività presso le funzioni centrali può inoltre ridurre il rischio che realtà caratterizzate da differenti livelli di maturità organizzativa applichino criteri non omogenei. Tale configurazione può tuttavia generare colli di bottiglia e richiede che il livello centrale disponga di informazioni sufficienti sul processo, sul mercato e sul contesto operativo locale. In assenza di tali informazioni, la valutazione rischia di risultare formalmente coerente ma poco aderente alle caratteristiche del singolo caso d'uso.

Una configurazione decentralizzata attribuisce invece una quota maggiore di responsabilità alle realtà locali. Il principale vantaggio è la maggiore prossimità al business e la possibilità di valorizzare conoscenze e competenze presenti sul territorio. Tale impostazione può inoltre ridurre il carico operativo delle funzioni centrali. La sua sostenibilità dipende però dalla presenza, nei diversi contesti, di ruoli e competenze in grado di svolgere con sufficiente autonomia le attività previste dall'*AI Lifecycle*. In un'organizzazione eterogenea questa condizione non è necessariamente soddisfatta in modo uniforme e può determinare differenze nella qualità delle valutazioni, nella gestione della documentazione e nell'interpretazione delle responsabilità.

Tra i due estremi si colloca una configurazione ibrida, nella quale alcune attività possono rimanere presidiate a livello centrale mentre altre possono essere svolte localmente. In una configurazione di questo tipo, il livello centrale può mantenere il presidio sui principi comuni, sugli strumenti metodologici, sul coordinamento, sulla visibilità complessiva e sui principali momenti di validazione, mentre alle realtà locali può essere attribuita la responsabilità operativa sul caso d'uso e sulle attività che richiedono una conoscenza diretta del contesto. La logica non

consiste quindi nel suddividere l'*AI Lifecycle* in processi distinti ma nel distribuire l'esecuzione delle relative attività tra livello centrale e realtà locali.

La Tabella 2.5 sintetizza i principali punti di forza e le criticità delle configurazioni organizzative considerate.

Tabella 2.5: Confronto tra le configurazioni organizzative considerate per la governance di gruppo

Configurazione	Punti di forza	Principali criticità
Centralizzata	Uniformità metodologica, concentrazione delle competenze, maggiore visibilità a livello centrale	Possibili colli di bottiglia, minore conoscenza del contesto locale, elevato carico sulle funzioni centrali
Decentralizzata	Prossimità al business, maggiore rapidità a livello locale, valorizzazione delle competenze disponibili	Possibili disomogeneità, dipendenza dalla maturità organizzativa locale, minore visibilità complessiva
Ibrida	Equilibrio tra standardizzazione e conoscenza locale, coinvolgimento selettivo del livello centrale, maggiore adattabilità	Necessità di definire con chiarezza responsabilità, flussi informativi e confini tra livello centrale e realtà locali

Il confronto è stato svolto in termini qualitativi e non attraverso un sistema di scoring o una matrice di ponderazione formalizzata. Le configurazioni centralizzata, decentralizzata e ibrida sono state quindi lette rispetto ai criteri descritti, mettendone in evidenza benefici, condizioni di applicabilità e criticità. Nel contesto progettuale sono state approfondite in particolare le alternative decentralizzata e ibrida rispetto a un assetto integralmente centralizzato: la prima riconosce maggiore autonomia alle realtà locali dotate di strutture e competenze adeguate; la seconda consente di mantenere alcuni presidi a livello centrale e di modulare la distribuzione delle attività in funzione delle differenze organizzative. Tale approfondimento non costituisce una graduatoria generale tra modelli, ma un supporto alla successiva definizione dell'assetto più adatto al contesto considerato.

La valutazione ha evidenziato, in particolare, una tensione ricorrente tra conoscenza del contesto locale e disponibilità di competenze specialistiche. Alcune realtà potrebbero non disporre di risorse dedicate per presidiare localmente attività legali, di rischio o di controllo. Allo stesso tempo, le funzioni centrali potrebbero non possedere una conoscenza sufficientemente dettagliata del contesto operativo per sostituirsi integralmente ai presidi locali. Questa esigenza ha portato ad approfondire una configurazione capace di adattare l'assegnazione delle attività senza modificare i criteri, gli strumenti e l'*AI Lifecycle* comuni.

La configurazione organizzativa di riferimento non risulta ancora definitivamente formalizzata al momento della stesura della presente tesi. Il lavoro progettuale ha pertanto confrontato le diverse alternative, dedicando particolare attenzione

alla configurazione ibrida come possibile soluzione, senza però che questa possa essere considerata una scelta definitiva.

2.5.4 Il modello ibrido come configurazione in valutazione

La distinzione tra configurazioni centralizzate, decentralizzate e ibride può essere ricondotta, più in generale, al modo in cui responsabilità e diritti decisionali vengono distribuiti all'interno dell'organizzazione. La letteratura sulla data governance evidenzia come la configurazione dei meccanismi di governance debba essere adattata alle caratteristiche dell'organizzazione, alla sua struttura e ai meccanismi decisionali adottati, piuttosto che essere definita secondo un assetto universalmente applicabile [15, 16]. Questa impostazione è coerente anche con la letteratura sull'AI governance, che richiama la necessità di definire strutture, processi e responsabilità capaci di coordinare soggetti e funzioni diverse all'interno dell'organizzazione [4].

Anche la letteratura professionale più recente sull'organizzazione dell'IA rappresenta la scelta del modello di governance lungo differenti livelli di centralizzazione. PwC distingue tra approcci centralizzati, decentralizzati e una configurazione ibrida *Hub & Spoke*, nella quale un nucleo centrale concentra funzioni di controllo, indirizzo e supporto, mantenendo al tempo stesso responsabilità operative nelle unità organizzative [17]. Gartner considera analogamente la scelta tra modelli centralizzati, ibridi o federati e decentralizzati come una decisione organizzativa che richiede una chiara attribuzione dei diritti decisionali, delle responsabilità e delle deleghe [18]. Tali contributi non individuano quindi un'unica configurazione ottimale ma forniscono un riferimento utile per interpretare le diverse alternative considerate nel progetto.

In questo quadro, la logica *Hub & Spoke* rappresenta una possibile declinazione della configurazione ibrida. L'*hub* costituisce il punto di coordinamento centrale nel quale vengono concentrati principi, metodologie, strumenti comuni e specifiche responsabilità di governance; gli *spoke* operano invece in prossimità dei diversi contesti organizzativi, mantenendo la conoscenza locale e svolgendo le attività per le quali dispongono delle competenze necessarie. La caratteristica distintiva non consiste quindi nella separazione dei processi ma nella distribuzione delle responsabilità all'interno di un impianto comune.

L'approfondimento delle alternative è stato supportato anche da un benchmark preliminare sviluppato nel corso del lavoro. L'analisi ha confrontato quattro grandi organizzazioni caratterizzate dalla presenza di entità controllate al di fuori dell'Europa, utilizzando un insieme comune di macro-attività di AI governance per osservare la distribuzione delle responsabilità tra livello centrale e locale. Tra i quattro casi analizzati, tre configurazioni, relative ai settori finanziario, dei servizi e industriale, sono state ricondotte a una logica ibrida *Hub & Spoke*, mentre il caso relativo al settore farmaceutico ha mostrato una configurazione maggiormente centralizzata.

Il benchmark ha avuto una funzione esplorativa e di supporto alla progettazione: non è stato costruito come campione statistico, né viene utilizzato nella tesi per stimare la diffusione dei diversi modelli sul mercato. La numerosità limitata dei casi

e il carattere progettuale della ricognizione non consentono infatti generalizzazioni. L'evidenza viene quindi mantenuta come elemento di confronto qualitativo, da leggere insieme ai criteri organizzativi e ai riferimenti di letteratura richiamati in precedenza, e non come validazione autonoma della configurazione ibrida.

Alla luce di tali elementi, tra le alternative approfondite nel corso del lavoro particolare attenzione è stata dedicata a una configurazione ibrida assimilabile a una logica *Hub & Spoke*. Nell'ipotesi progettuale considerata, il livello centrale assumerebbe il ruolo di hub di governance, mantenendo il presidio su politiche, procedure, metodologie, modelli documentali comuni, visibilità complessiva e principali momenti di validazione. Le realtà estere conserverebbero invece la conoscenza del contesto locale e la responsabilità operativa sulle attività che richiedono prossimità al business. Il riferimento rimarrebbe un unico *AI Lifecycle*, comune a livello di gruppo, rispetto al quale varia il soggetto chiamato a presidiare le singole attività.

La configurazione ibrida rimane tuttavia una soluzione in valutazione e non un assetto organizzativo già stabilizzato. Il lavoro progettuale ne ha delineato l'architettura generale, mentre la distribuzione puntuale delle responsabilità e i relativi meccanismi di coordinamento risultano ancora oggetto di affinamento e validazione organizzativa. Tali aspetti sono approfonditi nella sottosezione successiva.

2.5.5 Coordinamento tra livello centrale e realtà estere

La configurazione ibrida delineata nella sottosezione precedente richiede meccanismi di coordinamento in grado di rendere effettiva la distribuzione delle responsabilità. Nella dimensione internazionale tale esigenza è particolarmente rilevante: il livello centrale deve poter mantenere un presidio coerente sul modello comune senza perdere la conoscenza del contesto locale, mentre le realtà estere devono poter svolgere le attività di propria competenza senza dipendere sistematicamente dal supporto centrale.

Nell'ipotesi organizzativa considerata, la figura del *Local AI Coordinator* svolgerebbe il principale ruolo di raccordo tra livello locale e centrale. Il suo compito consisterebbe nel mantenere visibilità sulle iniziative di IA della realtà di riferimento, coordinare la raccolta delle informazioni necessarie, facilitare il coinvolgimento delle funzioni locali e attivare il supporto del livello centrale quando necessario. In presenza di un nuovo caso d'uso, tale figura contribuirebbe quindi a favorire l'emersione tempestiva dell'iniziativa e ad assicurare l'avvio coerente delle attività di identificazione, classificazione e registrazione previste dall'*AI Lifecycle* comune.

Un ulteriore meccanismo di coordinamento riguarda l'assegnazione delle attività alle funzioni competenti. Nella configurazione considerata, il primo livello di presidio è rappresentato dalla funzione locale, quando presente e adeguatamente competente. In sua assenza può essere coinvolto il referente funzionale associato alla realtà interessata e, qualora anche tale presidio non risulti sufficiente, la funzione competente a livello centrale. Questa logica consente di mantenere invariati contenuto e finalità delle attività previste dall'*AI Lifecycle*, adattandone

l'esecuzione alla struttura organizzativa effettivamente disponibile nei diversi contesti.

Il coordinamento riguarda anche la gestione delle informazioni contenute negli inventari. Le informazioni raccolte a livello locale devono poter alimentare una visibilità complessiva di gruppo e le variazioni rilevanti devono essere riflesse in modo coerente nei diversi livelli informativi. Il funzionamento della configurazione richiede pertanto di definire con chiarezza le responsabilità di aggiornamento, le modalità di riconciliazione tra inventari locali e inventario globale e la gestione degli eventuali disallineamenti. Tale esigenza assume particolare rilevanza quando cambiano finalità, ruolo regolatorio, livello di rischio o stato del sistema.

Un ulteriore flusso riguarda il raccordo con gli organi centrali di governance. L'*AI Advisory Committee* deve disporre di una visibilità sufficiente sulle iniziative più rilevanti per fornire supporto, garantire coerenza metodologica e individuare i casi che richiedono un ulteriore livello di valutazione. Ciò non implica la validazione sistematica di ogni caso d'uso: negli scenari meno critici può essere mantenuta una gestione più proporzionata a livello locale mentre il coinvolgimento degli organi centrali aumenta in presenza di dubbi di classificazione, criticità rilevanti, esigenze specialistiche o casi che richiedono il coinvolgimento di livelli decisionali superiori.

La Figura 2.4 sintetizza la configurazione organizzativa considerata, evidenziando i principali meccanismi di raccordo tra livello centrale e realtà estere e la logica di assegnazione delle attività lungo l'*AI Lifecycle*.

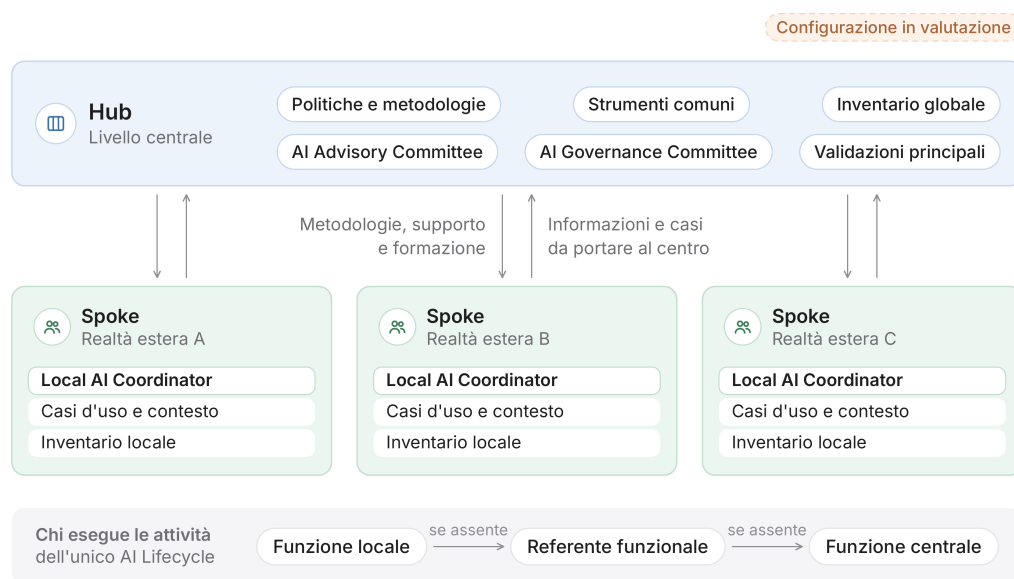


Figura 2.4: Configurazione ibrida in valutazione per il coordinamento tra livello centrale e realtà estere

Per i sistemi ad alto rischio, il coordinamento con il livello centrale assume una rilevanza maggiore pur variando in funzione del ruolo regolatorio assunto dall'organizzazione. A seconda dello scenario possono infatti rendersi necessarie attività quali *Risk Assessment*, FRIA ove applicabile, verifiche della documentazione,

valutazioni di conformità e specifici momenti di validazione lungo l'*AI Lifecycle*. Le realtà locali mantengono il presidio delle informazioni di contesto e delle attività di propria competenza mentre le funzioni e gli organi centrali contribuiscono a garantire coerenza metodologica e supporto nei passaggi maggiormente sensibili.

Il coordinamento richiede inoltre attività di formazione e diffusione delle metodologie. La disponibilità di strumenti e modelli documentali comuni non è sufficiente se i referenti locali non dispongono delle conoscenze necessarie per utilizzarli correttamente. Nell'impostazione progettuale sono quindi considerati momenti di formazione, sensibilizzazione e supporto dedicati, con particolare attenzione all'identificazione dei sistemi, alla determinazione del ruolo regolatorio, alla classificazione e ai criteri per il coinvolgimento delle funzioni centrali. Tale presidio contribuisce anche alla qualità delle informazioni raccolte nell'inventario, riducendo il rischio che errori o incompletezze iniziali si propaghino nelle fasi successive del processo.

Il coordinamento tra livello centrale e realtà estere deve infine essere considerato dinamico. L'aumento della maturità organizzativa e delle competenze disponibili a livello locale può consentire nel tempo di attribuire maggiori responsabilità alle realtà interessate; viceversa, l'emergere di casi più complessi o di nuovi requisiti può richiedere un maggiore coinvolgimento delle funzioni centrali. La distribuzione delle attività può quindi essere progressivamente adattata, mantenendo come riferimento un unico *AI Lifecycle*, criteri comuni e meccanismi di coordinamento coerenti a livello di gruppo.

2.6 Integrazione delle componenti nel modello operativo

Le componenti descritte nelle sezioni precedenti acquistano valore solo se considerate come parti di un unico sistema. Censimento, classificazione, *AI Lifecycle* e governance organizzativa non rappresentano infatti moduli indipendenti ma componenti interdipendenti che alimentano reciprocamente il processo decisionale. Il modello operativo è stato progettato proprio per rendere esplicite tali dipendenze e trasformare l'adeguamento all'AI Act in un processo continuo, tracciabile e aggiornabile nel tempo.

Il processo prende avvio dall'emersione del bisogno o dall'identificazione di un sistema già esistente. Le informazioni raccolte attraverso lo strumento di identificazione dei sistemi di IA permettono di stabilire se la soluzione rientri nel perimetro e forniscono gli elementi necessari per determinare rischio e ruolo regolatorio. La classificazione produce quindi lo scenario regolatorio, che a sua volta consente di associare il sistema al percorso previsto dall'*AI Lifecycle*. Quest'ultimo stabilisce quali attività devono essere svolte mentre il modello organizzativo identifica le funzioni responsabili, i soggetti da coinvolgere e gli eventuali momenti di validazione o di coinvolgimento dei livelli decisionali superiori.

Come illustrato nella Figura 2.5, le principali componenti del modello sono collegate secondo una sequenza logica che parte dall'identificazione del sistema e conduce, attraverso la classificazione e la determinazione dello scenario regolatorio,

alla definizione del percorso nell'*AI Lifecycle*, delle responsabilità e dei controlli applicabili, fino alle attività di monitoraggio e aggiornamento.

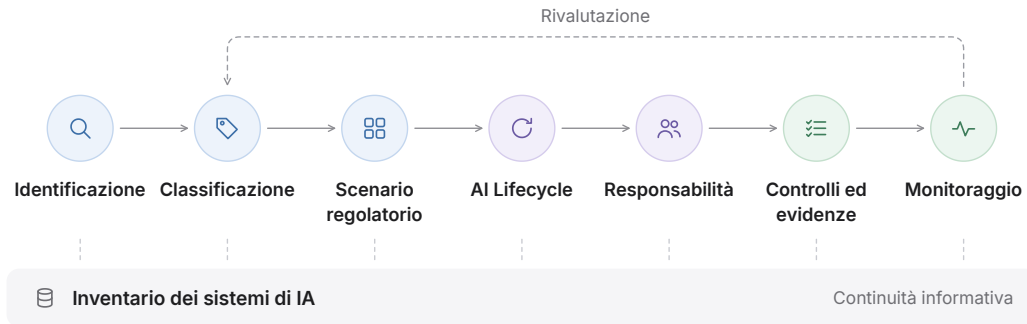


Figura 2.5: Integrazione delle principali componenti del modello operativo di AI governance

Tale sequenza non deve tuttavia essere interpretata come un processo strettamente lineare. Le informazioni prodotte nelle fasi successive possono richiedere una revisione delle decisioni assunte in precedenza. Un'attività di test può evidenziare caratteristiche non considerate inizialmente; una modifica del sistema può incidere sulla finalità o sul ruolo regolatorio; il monitoraggio può far emergere nuovi elementi di rischio che richiedono ulteriori controlli; una realtà estera può segnalare un requisito locale che rende necessario adattare alcune modalità operative. Il modello prevede quindi meccanismi di ritorno e aggiornamento che consentono di mantenere coerenti nel tempo classificazione, documentazione, controlli e responsabilità.

L'inventario costituisce il principale elemento di continuità informativa tra le diverse componenti del modello. Esso non rappresenta soltanto il punto iniziale di registrazione dei sistemi ma il riferimento nel quale devono essere riflesse le principali variazioni di stato e le informazioni rilevanti ai fini della governance. La qualità complessiva del modello dipende quindi anche dalla capacità di collegare le decisioni assunte lungo l'*AI Lifecycle* all'aggiornamento dell'inventario, evitando che modifiche, valutazioni o approvazioni rimangano confinate in documenti o scambi informativi non riconciliati con il registro.

La combinazione tra rischio e ruolo regolatorio costituisce invece la principale chiave di instradamento del modello. La stessa architettura di governance può infatti generare percorsi differenti in funzione dello scenario applicabile. Un sistema ad alto rischio per il quale l'organizzazione opera come fornitore richiede un insieme articolato di attività tecniche, documentali e di conformità. Nel caso di un sistema ad alto rischio utilizzato in qualità di deployer, il presidio è maggiormente orientato alle condizioni di utilizzo, alla documentazione ricevuta dal fornitore e alle valutazioni richieste nel contesto operativo. Gli scenari a rischio limitato seguono invece percorsi proporzionati agli obblighi applicabili mentre quelli a rischio minimo sono gestiti con un livello di formalizzazione più contenuto. La matrice rischio-ruolo consente quindi di applicare una struttura comune senza appiattire scenari caratterizzati da obblighi e responsabilità differenti.

Il modello organizzativo rende eseguibile questa logica attraverso l'attribuzione delle responsabilità. L'*AI Business Owner* presidia il bisogno e il caso d'uso mentre l'*AI Technical Team* segue le attività tecniche. La funzione legale, l'ERM, le funzioni tecnologiche e di sicurezza e le altre funzioni di controllo intervengono nei rispettivi ambiti di competenza. L'*AI Advisory Committee* e l'*AI Governance Committee* assicurano il coordinamento trasversale e, nei casi che lo richiedono, i necessari momenti di validazione e il coinvolgimento dei livelli decisionali superiori. Nella dimensione di gruppo, il *Local AI Coordinator* e la logica di copertura basata su funzione locale, referente funzionale e livello centrale consentirebbero di applicare il medesimo *AI Lifecycle* anche in contesti organizzativi caratterizzati da strutture e competenze differenti.

L'architettura descritta definisce la struttura logica e organizzativa del modello, la cui attuazione operativa è supportata da un insieme di strumenti sviluppati e progressivamente affinati nel corso del lavoro. Tra questi rientrano il TAF, le politiche e le procedure interne, le liste di controllo, i modelli documentali e gli strumenti utilizzati per l'analisi degli scostamenti, la definizione delle azioni di adeguamento e il monitoraggio della loro attuazione. Tali artefatti costituiscono il collegamento tra il disegno organizzativo e l'esecuzione delle attività, trasformando responsabilità, controlli e requisiti in evidenze concretamente verificabili.

Il capitolo successivo approfondisce pertanto l'implementazione operativa del modello e lo sviluppo degli strumenti predisposti a supporto della sua applicazione. L'attenzione si sposta sul quadro dei controlli, sulla formalizzazione attraverso politiche e procedure, sull'analisi degli scostamenti e sul progressivo avvio delle azioni di adeguamento. Sono inoltre approfondite la predisposizione della metodologia di *Risk Assessment* per i sistemi classificati ad alto rischio e, per i casi in cui risulta applicabile, la metodologia per la FRIA. Il capitolo distingue così gli strumenti già sviluppati e progressivamente affinati dalle attività di applicazione che, al momento della stesura della presente tesi, risultano ancora in corso o da completare.

CAPITOLO 3

Implementazione operativa del modello di AI governance e sviluppo degli strumenti di valutazione

Il capitolo precedente ha descritto l'architettura del modello operativo, mostrando come censimento, classificazione, *AI Lifecycle* e modello organizzativo siano stati progettati come componenti interdipendenti di un unico sistema di governance. La definizione dell'architettura costituisce tuttavia soltanto una parte del percorso di adeguamento. Per rendere il modello concretamente applicabile è stato necessario tradurre requisiti, responsabilità e momenti decisionali in regole operative, controlli, evidenze, documenti, strumenti di valutazione e azioni di adeguamento utilizzabili dalle funzioni coinvolte.

L'implementazione del modello si è articolata lungo più direttrici tra loro strettamente collegate. Una prima direttrice ha riguardato la formalizzazione dell'*AI Lifecycle*, inteso non soltanto come rappresentazione delle fasi attraversate da un sistema di IA ma anche come procedura operativa in grado di associare a ciascuno scenario attività, responsabilità, documentazione e momenti di validazione. A questa si sono affiancati il TAF, l'analisi degli scostamenti e i piani di adeguamento, attraverso i quali i requisiti applicabili vengono tradotti in controlli verificabili e, ove necessario, in azioni concrete. Per i sistemi classificati ad alto rischio sono state inoltre predisposte una metodologia di *Risk Assessment* e, nei casi pertinenti, una metodologia per la FRIA. Accanto agli strumenti direttamente associati al flusso operativo, è stata inoltre oggetto di sviluppo e aggiornamento la politica interna sull'utilizzo dell'IA, con l'obiettivo di formalizzare principi generali, regole di comportamento e responsabilità organizzative in coerenza con il modello di governance definito.

Le attività descritte non sono state svolte secondo una sequenza temporale rigida ma si sono sviluppate in modo parzialmente parallelo e iterativo. Lo sviluppo dei controlli ha richiesto di intervenire anche su procedure e modelli documentali; l'affinamento dell'*AI Lifecycle* ha portato a precisare ruoli, responsabilità e momenti di validazione; l'analisi degli scostamenti ha evidenziato la necessità di definire con maggiore precisione le evidenze attese; la predisposizione del *Risk Assessment* e della FRIA ha infine rafforzato il raccordo con l'ERM e con la funzione legale. Il capitolo presenta pertanto tali componenti secondo una sequenza logica, distinguendo gli strumenti già sviluppati e progressivamente affinati dalle attività di applicazione che, al momento della stesura della presente tesi, risultano ancora in corso o da completare.

3.1 Dall'architettura del modello alla sua implementazione operativa

Il passaggio dalla progettazione all'implementazione richiede che ciascun requisito applicabile sia ricondotto a un'attività concreta, a una funzione responsabile e a un'evidenza verificabile. Questa traduzione è stata perseguita evitando di trattare la conformità come una verifica esclusivamente documentale svolta a valle del processo. I requisiti sono stati invece integrati nei diversi momenti dell'*AI Lifecycle*, così da collegarne l'attuazione alle funzioni che dispongono delle competenze necessarie per presidiarli e verificarli. In questa logica, le diverse componenti e i principali passaggi operativi svolgono funzioni distinte ma strettamente connesse:

- il processo di identificazione delimita il perimetro dei sistemi di IA e raccoglie le informazioni necessarie alle successive valutazioni;
- la classificazione determina il livello di rischio e il ruolo regolatorio dell'organizzazione;
- l'inventario consolida e rende tracciabili le informazioni raccolte e gli esiti della classificazione;
- l'*AI Lifecycle* definisce il percorso operativo applicabile allo specifico scenario;
- il TAF individua i controlli pertinenti e le relative evidenze;
- l'analisi degli scostamenti confronta lo stato atteso con quello corrente e consente di individuare le conseguenti azioni di adeguamento.

Per i sistemi classificati ad alto rischio, questo impianto è inoltre integrato dal *Risk Assessment* e, ove applicabile, dalla FRIA, che approfondiscono rispettivamente il profilo di rischio del sistema e i potenziali impatti sui diritti fondamentali [1].

L'elemento distintivo dell'impostazione non risiede quindi nella presenza di un singolo documento o di un singolo strumento ma nella continuità tra le diverse componenti. Una revisione della classificazione può modificare il percorso previsto dall'*AI Lifecycle*; un controllo non coperto può generare uno scostamento e una conseguente azione di adeguamento; una modifica del sistema può richiedere l'aggiornamento della documentazione, del *Risk Assessment* o della FRIA. L'implementazione operativa assume pertanto la forma di un sistema di governo che deve mantenere coerenza nel tempo.

Questa logica ha influenzato anche la progettazione degli strumenti. I modelli Excel utilizzati nel progetto non sono stati concepiti come archivi isolati ma come supporti a specifici passaggi del processo: identificazione e classificazione, selezione dei controlli, valutazione dello stato di attuazione, definizione delle azioni, valutazione del rischio e monitoraggio. La standardizzazione dei campi e delle logiche di calcolo mira a ridurre la variabilità delle valutazioni senza sostituire il contributo delle funzioni competenti nell'interpretazione del caso concreto.

Il risultato è un modello nel quale la dimensione normativa viene progressivamente tradotta in attività operative. L'AI Act definisce il quadro normativo e gli obblighi applicabili; la governance assegna responsabilità e momenti decisionali; procedure e strumenti traducono tali responsabilità in attività operative; controlli ed evidenze consentono infine di verificarne l'attuazione. È su questo passaggio dalla struttura concettuale alla concreta esecuzione che si concentra il presente capitolo.

3.2 Formalizzazione dell'AI Lifecycle

3.2.1 Obiettivi e funzione della procedura

Uno dei principali strumenti formalizzati nel corso del lavoro è la procedura dedicata all'*AI Lifecycle*. Il documento è stato concepito per fornire un quadro comune e strutturato per la gestione dell'intero ciclo di vita dei sistemi di IA, dalla definizione iniziale del bisogno fino alle attività successive al rilascio. La sua funzione non è quindi soltanto rappresentare in forma sequenziale le fasi attraversate da un sistema ma rendere espliciti, per ciascuna fase, i requisiti applicabili, le responsabilità, gli strumenti da utilizzare e le evidenze da produrre.

La procedura si applica sia alle nuove iniziative sia alle modifiche significative di sistemi già esistenti. Tale scelta è rilevante perché il profilo regolatorio e di rischio di un sistema non può essere considerato immutabile. Cambiamenti nella finalità, nell'architettura, nei dati, nelle modalità di utilizzo o nella catena di fornitura possono infatti incidere sullo scenario originariamente individuato e rendere necessaria una nuova valutazione. L'*AI Lifecycle* è stato quindi impostato come un processo da riesaminare e aggiornare nel tempo, coerentemente con una logica di monitoraggio continuo.

Un ulteriore obiettivo della procedura consiste nel creare un riferimento comune per funzioni caratterizzate da competenze differenti. Unità di business, funzioni tecniche, funzione legale, ERM, funzioni di sicurezza e organi di governance intervengono in momenti diversi e con responsabilità differenti. Senza un percorso condiviso, il rischio sarebbe quello di gestire i singoli requisiti come attività indipendenti con possibili sovrapposizioni o vuoti di responsabilità. L'*AI Lifecycle* è stato quindi utilizzato come struttura di raccordo tra dimensione regolatoria, organizzativa e tecnica.

3.2.2 Fasi comuni: dal bisogno al registro e alla selezione dei controlli

La parte iniziale del percorso è comune ai diversi scenari e precede la differenziazione per rischio e ruolo regolatorio. Il primo passaggio consiste nella definizione del bisogno e della finalità del sistema. Questa fase richiede di chiarire quale problema o opportunità debba essere affrontato, quali obiettivi debbano essere raggiunti e quale valore aggiunto sia atteso dalla soluzione. La definizione della finalità assume un'importanza particolare perché costituisce il riferimento rispetto al quale

vengono successivamente valutati il perimetro regolatorio, la classificazione e gli eventuali cambiamenti del sistema.

Segue l'identificazione del sistema attraverso il processo descritto nel Capitolo 2. L'obiettivo è determinare se la soluzione rientri nella nozione di sistema di IA e raccogliere gli elementi necessari alla successiva classificazione. Quando la soluzione è considerata in perimetro, sulla base delle informazioni disponibili vengono determinati il livello di rischio e il ruolo regolatorio assunto dall'organizzazione. La combinazione tra rischio e ruolo rappresenta la principale chiave di instradamento del processo: a parità di tecnologia, i requisiti applicabili possono infatti variare in modo rilevante a seconda che l'organizzazione agisca come fornitore oppure utilizzi il sistema in qualità di deployer.

Una volta completate l'identificazione e la classificazione, le informazioni raccolte e i relativi esiti vengono consolidati nell'inventario. La funzione legale interviene nella valutazione finale della classificazione prima del consolidamento, contribuendo a mantenere una base informativa coerente per le attività successive. Per i sistemi classificati ad alto rischio è inoltre previsto il coinvolgimento degli organi di governance nei passaggi in cui sia richiesta una validazione prima di procedere alle attività successive previste dal percorso applicabile.

Dopo il consolidamento nell'inventario, il passaggio al TAF consente di tradurre lo scenario regolatorio nei requisiti e nei controlli pertinenti. Il livello di rischio e il ruolo regolatorio vengono utilizzati per filtrare i controlli applicabili. Le funzioni responsabili vengono quindi coinvolte nella valutazione dello stato corrente e nella raccolta delle evidenze. In questo senso, la fase di *Design* non termina con la classificazione del sistema ma comprende anche una prima verifica del livello di presidio rispetto ai requisiti applicabili.

3.2.3 Differenziazione dei percorsi per rischio e ruolo regolatorio

L'*AI Lifecycle* è stato costruito a partire da una matrice che combina livello di rischio e ruolo regolatorio. In coerenza con il perimetro progettuale, i percorsi formalizzati fanno riferimento ai ruoli di fornitore e deployer, gli unici effettivamente riscontrati nei casi d'uso analizzati alla data di redazione della tesi. Tale impostazione consente di mantenere una struttura comune evitando al tempo stesso di applicare un percorso indistinto a scenari caratterizzati da requisiti differenti. La combinazione tra rischio e ruolo determina infatti la profondità delle attività da svolgere, il livello di formalizzazione richiesto e le funzioni da coinvolgere lungo il percorso.

Gli elementi iniziali di identificazione, classificazione e registrazione costituiscono la base comune del processo, pur con un livello di approfondimento coerente con lo scenario considerato. Le fasi successive assumono invece contenuti differenti. Per un sistema ad alto rischio rispetto al quale l'organizzazione opera come fornitore, il percorso comprende un insieme esteso di attività tecniche, documentali e di conformità. Per un sistema ad alto rischio utilizzato in qualità di deployer, l'attenzione si sposta sulla documentazione ricevuta dal fornitore, sulle condizioni concrete di utilizzo, sulla sorveglianza umana, sulla FRIA ove applicabile, sulla

registrazione degli eventi e sul monitoraggio. Negli scenari a rischio limitato le attività sono circoscritte ai requisiti effettivamente applicabili, mentre per i sistemi a rischio minimo il percorso presenta un livello di formalizzazione più contenuto.

La differenziazione assume rilievo anche sotto il profilo organizzativo. Una medesima area di controllo può infatti richiedere modalità di presidio diverse a seconda del ruolo assunto dall'organizzazione. In uno scenario di fornitore può essere necessario produrre direttamente specifiche evidenze mentre in uno scenario di deployer il presidio può consistere nella verifica e nell'utilizzo della documentazione resa disponibile dal fornitore insieme alle informazioni relative al contesto di utilizzo. L'*AI Lifecycle* consente quindi di rendere espliciti i requisiti applicabili a ciascuno scenario e le modalità con cui devono essere presidiati.

La Tabella 3.1 sintetizza i principali percorsi previsti dall'*AI Lifecycle* in funzione della combinazione tra livello di rischio e ruolo regolatorio. Per i sistemi ricondotti al percorso a rischio minimo il modello non prevede un'ulteriore differenziazione operativa in funzione del ruolo; tale scenario è pertanto rappresentato unitariamente.

Tabella 3.1: Sintesi dei percorsi dell'*AI Lifecycle* in funzione del rischio e del ruolo regolatorio

Rischio	Ruolo	Impostazione del percorso
Alto rischio	Fornitore	Percorso esteso con requisiti tecnici, documentali e di conformità, gestione del rischio e monitoraggio successivo all'immissione sul mercato
Alto rischio	Deployer	Verifica della documentazione del fornitore, condizioni di utilizzo, sorveglianza umana, FRIA ove applicabile, registrazione degli eventi e monitoraggio
Rischio limitato	Fornitore	Percorso proporzionato ai requisiti applicabili, con particolare attenzione agli adempimenti documentali e di trasparenza pertinenti allo scenario
Rischio limitato	Deployer	Verifica delle informazioni e della documentazione rese disponibili dal fornitore e presidio dei requisiti applicabili al contesto di utilizzo
Rischio minimo	–	Percorso semplificato con mantenimento dell'identificazione e della registrazione ai fini della governance interna

Ai fini espositivi, le sottosezioni successive approfondiscono i due percorsi relativi ai sistemi ad alto rischio distinguendo lo scenario in cui l'organizzazione opera come fornitore da quello in cui agisce come deployer. I due percorsi sono inoltre rappresentati graficamente nelle figure successive. La scelta consente di rappresentare i workflow caratterizzati dal maggiore livello di articolazione in

termini di attività, responsabilità e presidi, evitando di duplicare graficamente i percorsi a rischio limitato e minimo già sintetizzati nella Tabella 3.1. Le rappresentazioni sono state rielaborate a un livello di dettaglio coerente con le esigenze di riservatezza del progetto.

3.2.4 Percorso dei sistemi ad alto rischio in qualità di fornitore

Lo scenario nel quale l'organizzazione opera come fornitore di un sistema ad alto rischio rappresenta il percorso più articolato previsto dalla procedura. Dopo la fase iniziale di *Design*, il sistema entra nelle successive attività di sviluppo e conformità che traducono gli obblighi applicabili in presidi tecnici, documentali e organizzativi. Tra le principali componenti rientrano la predisposizione della documentazione tecnica prevista dall'Allegato IV, le misure di governance dei dati, la sorveglianza umana, la registrazione degli eventi, i requisiti di accuratezza, robustezza e cibersecurity e il sistema di gestione del rischio [1].

La procedura considera inoltre le attività di test, comprese le verifiche in condizioni reali ove pertinenti, e la predisposizione delle istruzioni per l'uso e delle ulteriori informazioni richieste. Prima dell'immissione sul mercato o della messa in servizio, il percorso comprende anche gli adempimenti di conformità previsti per lo specifico sistema, tra cui la valutazione di conformità, la dichiarazione UE di conformità, la marcatura CE e la registrazione nella banca dati dell'Unione nei casi previsti dalla normativa. A tali attività si affianca la predisposizione del monitoraggio successivo all'immissione sul mercato. La procedura non tratta questi adempimenti come elementi isolati ma li colloca lungo il ciclo di vita e li collega alle funzioni chiamate a predisporre, verificare o approvare le relative evidenze.

La fase successiva all'immissione sul mercato o alla messa in servizio mantiene il sistema all'interno del perimetro di governance. L'inventario deve essere aggiornato quando necessario, il piano di monitoraggio deve essere attuato e gli incidenti o le anomalie rilevanti devono poter essere gestiti attraverso flussi definiti. Anche le verifiche periodiche e il riesame degli indicatori rientrano quindi nel percorso. Il rilascio non rappresenta la conclusione del processo ma il passaggio a una fase nella quale il comportamento del sistema deve essere osservato e riesaminato nel tempo.

La Figura 3.1 rappresenta graficamente il workflow operativo previsto per tale scenario.

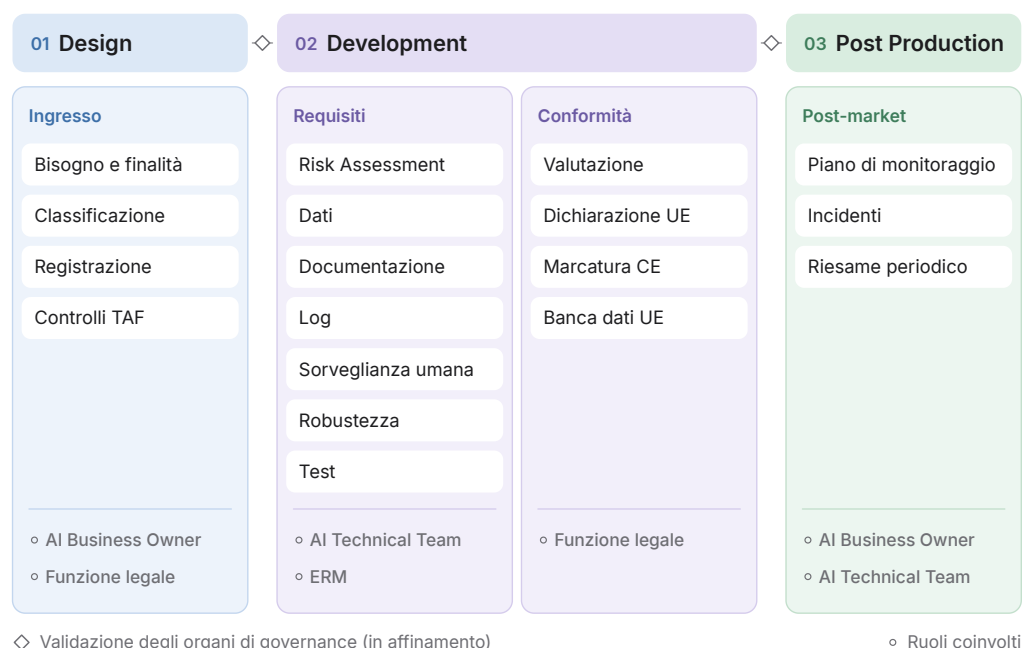


Figura 3.1: Workflow operativo per sistemi di IA ad alto rischio in qualità di fornitore

3.2.5 Percorso dei sistemi ad alto rischio utilizzati in qualità di deployer

Quando l'organizzazione utilizza un sistema acquisito da un soggetto esterno, il percorso operativo assume caratteristiche diverse rispetto allo scenario di fornitore. Il deployer non è chiamato a replicare le attività proprie del fornitore ma deve disporre delle informazioni necessarie a utilizzare il sistema nelle condizioni previste e a presidiare gli adempimenti che ricadono sul proprio ruolo. Per i sistemi ad alto rischio il percorso comprende quindi l'analisi della documentazione e delle istruzioni per l'uso ricevute dal fornitore, la definizione e l'attuazione della sorveglianza umana, il monitoraggio dell'utilizzo, la registrazione degli eventi nei casi applicabili e la gestione degli incidenti. Nei casi previsti rientrano inoltre gli obblighi di informazione dei lavoratori e le verifiche periodiche sul corretto utilizzo del sistema.

La documentazione resa disponibile dal fornitore costituisce quindi un riferimento operativo per il deployer. Essa deve consentire di comprendere la finalità prevista, le condizioni d'uso, le limitazioni, le prestazioni, i rischi residui e le misure da rispettare durante l'utilizzo. L'organizzazione deve verificare che le modalità concrete di impiego siano coerenti con tali indicazioni e che le persone incaricate della sorveglianza dispongano delle informazioni, delle competenze e dell'autorità necessarie per intervenire quando richiesto.

Per alcuni sistemi ad alto rischio il percorso include inoltre la FRIA prevista dall'articolo 27 dell'AI Act. La metodologia sviluppata per tale valutazione, descritta nelle sezioni successive, si inserisce nell'*AI Lifecycle* come attività specifica del deployer nei casi in cui ne ricorrano le condizioni di applicabilità. Non si tratta

quindi di un adempimento indistinto per tutti i sistemi ad alto rischio. Questa distinzione consente di mantenere separati gli obblighi propri del fornitore dalle valutazioni che dipendono dal concreto contesto di utilizzo.

La Figura 3.2 sintetizza il workflow operativo previsto per i sistemi ad alto rischio utilizzati in qualità di deployer.

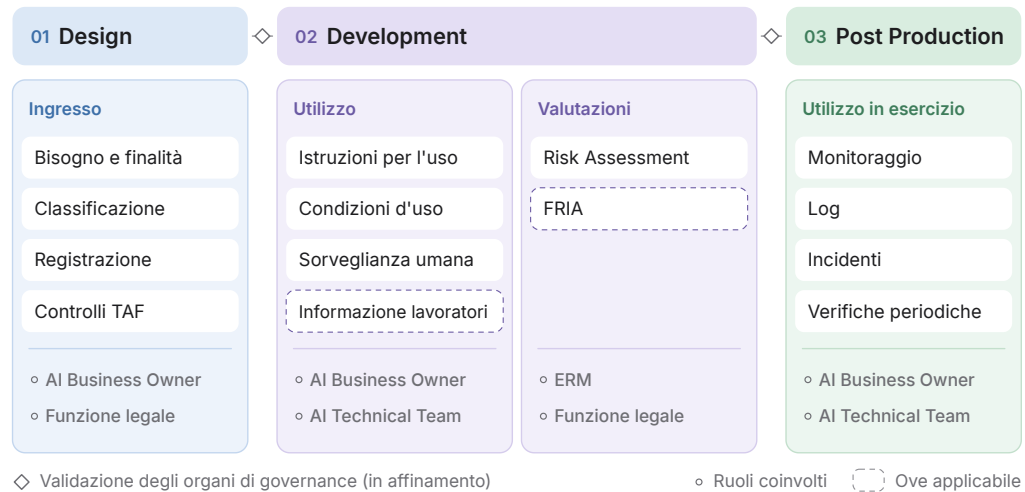


Figura 3.2: Workflow operativo per sistemi di IA ad alto rischio utilizzati in qualità di deployer

3.2.6 Attività tecniche e di monitoraggio lungo il ciclo di vita

Nel corso del lavoro, alcuni requisiti e aree di controllo sono stati tradotti in attività tecniche concretamente verificabili. La definizione ha riguardato in particolare le attività previste per i sistemi ad alto rischio sviluppati in qualità di fornitore. Tra gli esempi considerati rientrano la gestione delle modifiche, la registrazione degli eventi, la valutazione delle distorsioni (*bias*), la validazione dei dati in ingresso e la pulizia dei dati di addestramento. Questi casi mostrano come un requisito debba essere ricondotto a operazioni tecniche, responsabilità ed evidenze affinché possa essere presidiato in modo verificabile.

La gestione delle modifiche richiede, ad esempio, di mantenere traccia della motivazione del cambiamento, della sua descrizione, dei test e delle attività di validazione effettuate, delle modalità di rilascio e dell'impatto su rischio e prestazioni. Tale tracciabilità è rilevante perché una modifica apparentemente tecnica può incidere sulla finalità, sulla classificazione o sulle condizioni di conformità del sistema. La registrazione degli eventi svolge invece una funzione di ricostruzione e monitoraggio: le informazioni disponibili devono consentire di ricostruire il funzionamento del sistema, le versioni rilevanti, gli eventuali interventi umani e i comportamenti anomali.

Nel modello è stata definita anche una logica progressiva per il monitoraggio delle anomalie. Il percorso parte dalla disponibilità delle registrazioni tecniche e

può evolvere verso la definizione di schemi ricorrenti utili a individuare anomalie, il monitoraggio delle deviazioni e l'analisi delle relative segnalazioni. Una logica analoga riguarda la qualità dei dati e la valutazione delle distorsioni. Tali verifiche non si esauriscono necessariamente prima del rilascio ma possono essere ripetute durante l'utilizzo del sistema poiché cambiamenti nei dati o nella popolazione interessata possono incidere sulle prestazioni e sugli effetti prodotti.

Questi esempi evidenziano il ruolo dell'*AI Lifecycle* come struttura di raccordo tra requisiti, attività tecniche e responsabilità. La procedura non sostituisce le metodologie specialistiche utilizzate dalle funzioni competenti ma colloca le attività nel percorso applicabile, individua i soggetti da coinvolgere e rende esplicite le evidenze da produrre o mantenere nelle diverse fasi del ciclo di vita.

3.3 Sviluppo e aggiornamento dell'AI Policy e raccordo con il modello operativo

3.3.1 Finalità, perimetro e natura evolutiva

Nel corso del lavoro è stata sviluppata una politica interna dedicata all'utilizzo dei sistemi di IA, formalizzata nell'*AI Policy*. Tale documento è stato concepito come uno strumento trasversale di formalizzazione del modello di governance, complementare alle componenti operative descritte nel Capitolo 2. Nel periodo considerato nella presente tesi, il documento era già stato predisposto ed era oggetto di aggiornamento, anche per mantenerne la coerenza con l'evoluzione del quadro normativo, dell'*AI Lifecycle* e dell'assetto organizzativo definito nel progetto. Il documento svolge infatti una funzione distinta rispetto alla procedura: mentre l'*AI Lifecycle* definisce il percorso operativo applicabile ai diversi scenari, l'*AI Policy* stabilisce il quadro generale di principi, regole di comportamento, ambito di applicazione e responsabilità entro il quale tale percorso deve essere attuato.

Il documento è stato concepito come uno strumento evolutivo da aggiornare in funzione dei cambiamenti tecnologici, normativi e organizzativi. Tale caratteristica è particolarmente rilevante in un ambito nel quale le modalità di utilizzo dell'IA e il quadro regolatorio possono modificarsi rapidamente. L'*AI Policy* non assume quindi la forma di un insieme statico di divieti ma di uno strumento volto a orientare l'utilizzo della tecnologia, conciliandolo con il presidio dei rischi e con le esigenze di conformità.

Il documento è stato impostato con un perimetro di gruppo e una prospettiva globale, prevedendo tuttavia che la sua applicazione concreta tenga conto dell'impatto territoriale dei sistemi e delle normative pertinenti. La declinazione operativa nelle diverse realtà del gruppo e i relativi flussi di governance intercompany risultano ancora in progressiva definizione. Lo sviluppo e l'aggiornamento del documento si collegano pertanto anche al lavoro sulla governance internazionale descritto nel Capitolo 2.

3.3.2 Principi generali e regole di utilizzo

L'*AI Policy* traduce il concetto di utilizzo responsabile dell'IA in un insieme di principi che costituiscono il riferimento per decisioni e comportamenti lungo il ciclo di vita. Tra i principi individuati rientrano equità, trasparenza, spiegabilità, responsabilizzazione, integrità dei dati, affidabilità, sicurezza, tutela della persona e protezione dei dati. Nel modello sviluppato, tali principi trovano una successiva declinazione operativa nelle regole di utilizzo, nei controlli del TAF e nelle attività previste dall'*AI Lifecycle*.

Il principio di equità richiama la necessità di prevenire trattamenti ingiustamente discriminatori e di considerare le possibili fonti di distorsione (*bias*) derivanti dai dati, dalle scelte progettuali e dall'interazione umana. La trasparenza riguarda invece la disponibilità di informazioni adeguate ai diversi destinatari e la possibilità di mantenere tracciabilità sulle caratteristiche e sull'utilizzo del sistema. La responsabilizzazione richiede che ruoli e responsabilità siano identificabili lungo il processo e che siano previsti meccanismi di verifica e auditabilità.

A tali principi si affiancano regole di utilizzo rivolte agli utenti dei sistemi. Il documento considera, tra gli altri, i rischi connessi alla condivisione di informazioni riservate, alla protezione dei dati, alla proprietà intellettuale, all'utilizzo di piattaforme esterne e alla necessità di verificare criticamente gli output prodotti dai sistemi di IA. Quest'ultimo aspetto assume particolare rilievo per i sistemi generativi, i cui risultati possono contenere errori o informazioni non affidabili. L'utilizzo del sistema non elimina quindi la responsabilità dell'utente, che è comunque chiamato a verificare criticamente gli output e a mantenere un adeguato presidio umano sul loro utilizzo.

La Figura 3.3 sintetizza i principali principi di riferimento richiamati nell'*AI Policy*.



Figura 3.3: Principi di riferimento dell'AI Policy per un utilizzo responsabile dell'IA

3.3.3 Gestione dei nuovi casi d'uso e collegamento con l'AI Lifecycle

Lo sviluppo e il successivo aggiornamento del documento hanno rafforzato il collegamento tra regole generali e processo operativo. Quando emerge un nuovo caso d'uso, l'*AI Policy* richiede che esso venga analizzato in funzione della finalità, delle modalità di utilizzo e del contesto di riferimento. Nei casi previsti, tale analisi comporta l'attivazione della procedura formalizzata attraverso l'*AI Lifecycle*, che consente di ricondurre l'iniziativa alle attività di identificazione e classificazione, al consolidamento delle informazioni e dei relativi esiti nell'inventario e al successivo instradamento previsto dal modello di governance.

Particolare attenzione è dedicata agli utilizzi vietati e agli scenari nei quali la tecnologia può generare rischi maggiori. La classificazione del caso d'uso non dipende soltanto dalla tecnologia impiegata ma anche dalla finalità, dal contesto e dagli effetti che il sistema può produrre. Nel modello sviluppato il livello di rischio individuato attraverso tale analisi viene poi integrato con il ruolo regolatorio assunto dall'organizzazione, così da determinare il percorso applicabile all'interno dell'*AI Lifecycle*.

L'*AI Policy* disciplina inoltre l'utilizzo di sistemi e piattaforme di terzi, prevedendo specifiche regole in materia di sicurezza, riservatezza, protezione dei dati e utilizzo di strumenti autorizzati. Nei casi in cui ricorrano le condizioni previste, il ricorso a piattaforme esterne richiede quindi il coinvolgimento delle funzioni competenti e l'attivazione delle verifiche e delle procedure interne applicabili.

3.3.4 Ruoli, monitoraggio e aggiornamento

Il documento contiene anche una componente organizzativa. I ruoli descritti nel Capitolo 2 trovano nell'*AI Policy* una traduzione in compiti di indirizzo, supporto, implementazione e controllo. La funzione legale presidia gli aspetti legali e regolatori; l'ERM presidia le metodologie di rischio; le funzioni tecnologiche e di sicurezza intervengono sui controlli specialistici; le unità di business e i team tecnici forniscono e presidiano le informazioni e le attività di propria competenza relative al caso d'uso, allo sviluppo e all'utilizzo del sistema.

L'*AI Policy* è inoltre soggetta a monitoraggio e aggiornamento. Tale previsione è coerente con il carattere evolutivo dell'intero modello: l'emergere di nuovi casi d'uso, nuovi rischi o modifiche normative può richiedere di aggiornare le regole interne e, di conseguenza, procedure, controlli e modelli documentali. In questo senso, *AI Policy* e *AI Lifecycle* non costituiscono documenti paralleli ma livelli complementari dello stesso sistema: la prima definisce principi, regole generali e responsabilità mentre il secondo li traduce in attività, responsabilità operative ed evidenze lungo il ciclo di vita.

La Tabella 3.2 sintetizza il rapporto tra i due livelli, mettendone in evidenza finalità, oggetto, livello di dettaglio, meccanismi di applicazione e logiche di aggiornamento.

Tabella 3.2: Rapporto tra AI Policy e AI Lifecycle nel modello operativo

Dimensione	AI Policy	AI Lifecycle
Finalità	Definisce principi, regole di comportamento e perimetro generale	Traduce il quadro generale in un percorso operativo
Oggetto	Utilizzo responsabile dei sistemi di IA e responsabilità generali	Attività da svolgere lungo il ciclo di vita del singolo sistema
Livello di dettaglio	Generale e organizzativo	Operativo-procedurale
Meccanismo di applicazione	Regole comuni e rinvio alle procedure	Differenziazione per rischio e ruolo regolatorio
Aggiornamento	Aggiornamento in funzione dell'evoluzione normativa, tecnologica e organizzativa	Riesame e aggiornamento in funzione delle modifiche del sistema e dello scenario applicabile

3.4 Sviluppo del TAF e del sistema dei controlli

3.4.1 Finalità e architettura del framework

La formalizzazione di policy e procedure non è sufficiente, da sola, a rendere verificabile il livello di adeguamento di un singolo sistema. Per questa ragione una parte centrale del lavoro ha riguardato lo sviluppo e l'affinamento del TAF, utilizzato come strumento di raccordo tra requisiti applicabili, responsabilità operative, evidenze disponibili e azioni necessarie per colmare eventuali scostamenti.

Il framework è stato implementato operativamente attraverso un file Excel strutturato per supportare la selezione dei controlli applicabili, la raccolta delle evidenze e la valutazione del relativo stato di attuazione. Lo strumento include inoltre una macro che consente di filtrare i controlli in funzione del ruolo regolatorio e del livello di rischio selezionati, rendendo immediatamente visibile il sottoinsieme pertinente allo specifico scenario considerato.

La Figura 3.4 mostra un fac-simile semplificato dello strumento, costruito con dati fittizi, evidenziando la vista dei controlli filtrata in funzione del ruolo regolatorio e del livello di rischio.

Trusted_AI_Framework.xlsx Dati fittizi

▼ Ruolo Deployer/User Livello di rischio High-risk Systems Vista filtrata dei 54 controlli

Controllo		Valutazione		Mappatura	
CONTROL ID	CONTROL TOPIC · PILLAR	STATUS	GAP	OWNER	MAPPING
RSK_TRA.03	User Information Transparency	Globally Covered	–	Funzione legale	AI Act Art. 50 ISO 42001 A.8.2
RSK_HS.01	Human Surveillance Safety	Partially Covered	Di processo	AI Business Owner	AI Act Art. 26 ISO 42001 A.9.2
RSK_LOG.02	Logging Reliability	Not Covered	Tecnologico	AI Technical Team	AI Act Art. 26 ISO 42001 A.6.2.8
RSK_INC.02	Incident & Communication Accountability	Under Development	Documentale	Funzione legale	AI Act Art. 26 ISO 42001 A.8.4
RSK_PM.01	Post Monitoring Reliability	Partially Covered	Documentale	AI Technical Team	AI Act Art. 26 ISO 42001 A.6.2.6
...					

Index Trusted AI RCM Role and Risk Level Filter Ratio

Figura 3.4: Fac-simile semplificato dello strumento Excel del TAF (dati fittizi)

Il framework è stato costruito secondo una logica orientata al controllo. Il punto di partenza non è il documento da produrre ma il requisito da presidiare e la possibilità di dimostrarne l'effettiva attuazione. Ciascun controllo rappresenta quindi un'unità verificabile alla quale possono essere associati uno o più requisiti, una funzione responsabile, un insieme di evidenze attese e uno stato di copertura o attuazione. Questa impostazione consente di passare da una lettura prevalentemente normativa a una rappresentazione operativa e verificabile del livello di presidio.

Nella versione utilizzata nel progetto il TAF comprende 54 requisiti di controllo organizzati per aree tematiche. Tra queste rientrano governance e ciclo di vita, gestione del rischio, FRIA e conformità, qualità dei dati e tracciabilità, documentazione tecnica, trasparenza e sorveglianza umana, accuratezza, robustezza e cibersicurezza, gestione dei fornitori e delle terze parti, test, monitoraggio continuo e riesame delle prestazioni. Il framework non è stato costruito come una mera trasposizione testuale dell'AI Act ma come uno strumento capace di integrare requisiti normativi, riferimenti metodologici e presidi aziendali. In tale prospettiva sono stati considerati anche riferimenti già richiamati nel Capitolo 1, tra cui ISO/IEC 42001 e NIST AI RMF [12, 3].

La struttura del TAF svolge inoltre una funzione di standardizzazione. In un contesto nel quale sistemi differenti possono essere sviluppati, acquistati o utilizzati da unità organizzative diverse, la presenza di un riferimento comune consente di ridurre la variabilità delle valutazioni. Il framework fornisce infatti una base condivisa per discutere il livello di presidio, raccogliere le evidenze e documentare le eventuali carenze, mantenendo al tempo stesso la possibilità di selezionare soltanto i controlli pertinenti allo specifico scenario in funzione del livello di rischio e del ruolo regolatorio assunto dall'organizzazione.

3.4.2 Applicabilità dei controlli in funzione di rischio e ruolo

La logica di applicabilità costituisce uno degli elementi più rilevanti del TAF. Il framework non richiede infatti che tutti i controlli siano applicati indistintamente a ogni sistema. Il livello di rischio e il ruolo regolatorio individuati nella fase di classificazione vengono utilizzati come criteri di selezione dei requisiti pertinenti. In questo modo, la classificazione non rimane un risultato descrittivo ma produce un effetto diretto sulla profondità e sulla natura delle attività da svolgere.

Per un sistema ad alto rischio in qualità di fornitore, l'insieme dei controlli applicabili è più ampio e comprende requisiti tecnici, documentali, organizzativi e di conformità. Per un sistema ad alto rischio utilizzato come deployer l'attenzione si concentra invece sui controlli relativi alle condizioni di utilizzo, alla documentazione ricevuta, alla sorveglianza umana, al monitoraggio e alle valutazioni che ricadono sul soggetto utilizzatore. Negli scenari a rischio limitato vengono selezionati i requisiti pertinenti, mentre per i sistemi a rischio minimo il percorso mantiene le attività di identificazione e registrazione previste ai fini della governance interna, con un livello di formalizzazione più contenuto.

Tale meccanismo consente di evitare due criticità contrapposte. La prima consiste nell'applicare indiscriminatamente il massimo livello di controllo a ogni iniziativa, rendendo il processo poco sostenibile. La seconda consiste nel sottovalutare requisiti rilevanti perché non tradotti in attività specifiche. La logica rischio-ruolo permette quindi di mantenere una struttura comune senza appiattire scenari regolatori sostanzialmente differenti.

La Tabella 3.3 sintetizza le principali aree presidiate dal TAF, raggruppate per affinità, e la relativa finalità operativa.

Tabella 3.3: Principali dimensioni presidiate dal TAF

Area	Finalità operativa
Governance e ciclo di vita	Collegare requisiti, responsabilità e momenti decisionali lungo l' <i>AI Lifecycle</i>
Gestione del rischio e conformità	Collegare valutazioni, misure di trattamento, FRIA e ulteriori adempimenti applicabili
Dati e tracciabilità	Presidiare qualità, provenienza, utilizzo dei dati, registrazione degli eventi e ricostruibilità delle attività
Documentazione e trasparenza	Assicurare disponibilità e coerenza delle informazioni richieste ai diversi destinatari
Sorveglianza umana	Rendere esplicite modalità, responsabilità e condizioni dell'intervento umano
Accuratezza, robustezza e cibersicurezza	Verificare prestazioni, resilienza e misure tecniche contro errori, anomalie e attacchi
Terze parti e catena di fornitura	Gestire dipendenze, responsabilità, informazioni e verifiche relative a fornitori e componenti esterni
Test e monitoraggio	Supportare validazione, riesame delle prestazioni e aggiornamento dei presidi nel tempo

3.4.3 Dal requisito al controllo verificabile

La costruzione dei controlli ha richiesto di tradurre requisiti di carattere generale in controlli e verifiche concretamente eseguibili. Per ciascun requisito sono stati quindi definiti almeno quattro elementi:

- il comportamento o presidio atteso;
- la funzione competente a presidiare il requisito;
- l'evidenza utile a dimostrarne l'attuazione;
- il tipo di scostamento da registrare in caso di copertura insufficiente.

Questa logica è particolarmente evidente nei requisiti tecnici. Ad esempio, il tema della registrazione degli eventi non può essere considerato coperto soltanto dichiarando che il sistema produce registrazioni tecniche. Occorre comprendere quali informazioni vengano registrate, per quanto tempo siano disponibili, se consentano di ricostruire l'utilizzo del sistema e gli eventuali interventi umani e se esistano meccanismi per individuare comportamenti anomali. È stata quindi definita una logica progressiva che distingue la presenza delle registrazioni tecniche, la definizione di schemi ricorrenti utili a riconoscere anomalie, il monitoraggio delle deviazioni e l'analisi delle relative segnalazioni.

Un ragionamento analogo è stato applicato ai requisiti di accuratezza, robustezza e cibersicurezza. Il controllo deve poter essere ricondotto ad attività quali

validazione dei dati in ingresso, pulizia dei dati di addestramento, verifica di valori anomali o dati manipolati, test delle prestazioni, valutazione delle distorsioni (*bias*) e misure contro attacchi o alterazioni del modello. Nel corso dei workshop progettuali sono stati considerati, tra gli altri, rischi associati a *data poisoning*, *model poisoning*, *adversarial examples* e *model evasion*. Come supporto all'interpretazione di tali rischi e dei possibili presidi sono stati utilizzati riferimenti tecnici quali l'Open Worldwide Application Security Project (OWASP) Machine Learning Security Top Ten [19], la tassonomia NIST sull'*Adversarial Machine Learning* [20], il rapporto European Union Agency for Cybersecurity (ENISA) sulla sicurezza degli algoritmi di machine learning [21] e MITRE ATLAS (*Adversarial Threat Landscape for AI Systems*) [22].

Il valore di questi esempi non risiede nell'introdurre un catalogo completo di misure tecniche nella governance ma nel mostrare il principio seguito per la costruzione del framework: un requisito è realmente governabile quando può essere tradotto in un'attività osservabile e in un'evidenza verificabile.

3.4.4 Valutazione dello stato di attuazione

Una volta individuati i controlli applicabili, il TAF viene utilizzato come base per l'autovalutazione e per il confronto con le funzioni competenti. Per ciascun controllo viene descritta la situazione corrente e vengono raccolte le evidenze disponibili. Il livello di copertura viene quindi ricondotto a quattro stati previsti dal framework: *Globally Covered*, *Partially Covered*, *Under Development* e *Not Covered*. L'applicabilità del controllo viene invece determinata a monte in funzione del livello di rischio e del ruolo regolatorio associati allo specifico scenario.

Lo stato assegnato rappresenta il livello di copertura del controllo risultante dalla valutazione svolta. Tale valutazione deve essere supportata dalle evidenze disponibili e dal confronto con le funzioni competenti. Un controllo classificato come *Globally Covered* deve poter essere ricondotto a un presidio esistente e a evidenze coerenti; lo stato *Partially Covered* indica invece una copertura solo parziale del requisito. *Under Development* segnala che le attività necessarie sono state avviate ma non ancora completate mentre *Not Covered* identifica l'assenza di un presidio sufficiente rispetto al requisito considerato.

Le evidenze possono assumere forme diverse in funzione della natura del controllo. Possono essere utilizzate politiche, procedure, specifiche tecniche, configurazioni, registrazioni, risultati di test, documentazione di progetto, verbali di approvazione o ulteriori elementi utili a dimostrare l'attuazione del presidio. La raccolta richiede pertanto il contributo delle funzioni competenti e può coinvolgere più soggetti in relazione alla natura del controllo e delle evidenze richieste.

3.4.5 Affinamento del framework attraverso l'applicazione

Il TAF non è stato trattato come uno strumento statico. Le prime applicazioni del framework e il confronto con le funzioni coinvolte hanno consentito di individuare esigenze di affinamento relative alla chiarezza dei controlli, alle evidenze attese e all'attribuzione delle responsabilità. In termini operativi, gli affinamenti hanno

riguardato tre tipologie ricorrenti: rendere meno ambigua la formulazione di alcuni controlli, precisare quali evidenze fossero idonee a dimostrarne l'attuazione e chiarire quale funzione dovesse fornire o validare le informazioni necessarie. Tali elementi sono riportati a livello aggregato per preservare la riservatezza dei casi esaminati. L'applicazione ha quindi alimentato un processo iterativo di affinamento del framework.

Questo processo assume particolare rilievo perché controlli formulati in modo troppo generico possono produrre valutazioni non omogenee. Se due unità organizzative interpretano in modo diverso lo stesso requisito, gli esiti dell'autovalutazione diventano meno confrontabili. La standardizzazione del linguaggio, delle evidenze e dei criteri di valutazione favorisce quindi l'estensione del framework a un numero crescente di sistemi e realtà organizzative, mantenendo maggiore coerenza tra le valutazioni.

3.5 Formalizzazione documentale degli adempimenti

3.5.1 La documentazione come componente del controllo

Nel modello sviluppato la documentazione non viene considerata come un adempimento separato dall'operatività ma come una componente necessaria alla tracciabilità e alla verificabilità dei processi. Un requisito può infatti essere tecnicamente attuato ma non risultare dimostrabile se non esistono evidenze sufficienti a ricostruire chi ha svolto l'attività, secondo quali criteri e con quale esito.

Per questa ragione, accanto a policy, procedure e TAF, sono stati previsti la predisposizione e l'affinamento di modelli documentali specifici. Essi hanno la funzione di standardizzare le informazioni da raccogliere, ridurre la dipendenza da interpretazioni individuali e facilitare le verifiche successive. L'utilizzo di modelli comuni permette inoltre di collegare in modo più diretto il requisito regolatorio alla relativa evidenza.

Ai fini espositivi, le sottosezioni successive approfondiscono la formalizzazione documentale con riferimento ai sistemi ad alto rischio, distinguendo tra lo scenario in cui l'organizzazione opera come fornitore e quello in cui agisce come deployer. La scelta riflette il maggiore livello di articolazione degli adempimenti documentali previsti in tali scenari mentre per gli altri livelli di rischio il presidio documentale è ricondotto ai requisiti effettivamente applicabili.

3.5.2 Documentazione dei sistemi ad alto rischio in qualità di fornitore

Per i sistemi ad alto rischio rispetto ai quali l'organizzazione opera come fornitore, il percorso documentale è particolarmente articolato. Tra i principali documenti considerati rientrano la documentazione tecnica prevista dall'Allegato IV, le istruzioni per l'uso, il piano di monitoraggio successivo all'immissione sul mercato e la dichiarazione UE di conformità. A questi si affiancano le evidenze necessarie

a dimostrare l'attuazione dei requisiti relativi, tra gli altri, alla governance dei dati, alla sorveglianza umana, alla registrazione degli eventi, all'accuratezza, alla robustezza e alla cibersecurity. La valutazione di conformità costituisce invece il processo all'interno del quale tale documentazione e le relative evidenze concorrono a dimostrare il rispetto dei requisiti applicabili [1].

La documentazione tecnica fornisce una rappresentazione strutturata e tracciabile del sistema. Deve consentire di comprenderne finalità, architettura, dati, logiche di sviluppo e validazione, prestazioni, limitazioni, misure di controllo e gestione del rischio. Il relativo modello è stato impostato in modo da rendere più chiaro il contributo richiesto alle diverse funzioni, evitando che la predisposizione del documento ricada interamente su un unico soggetto.

Un'attenzione specifica è stata dedicata alla distinzione tra documentazione tecnica, istruzioni per l'uso e ulteriori informazioni di trasparenza. La documentazione tecnica supporta la dimostrazione della conformità e descrive in modo strutturato il sistema. Le istruzioni per l'uso forniscono al deployer le informazioni necessarie per utilizzarlo nelle condizioni previste. Infine, le ulteriori informazioni di trasparenza devono essere predisposte nei casi in cui siano richieste dallo specifico scenario normativo. Mantenere chiara tale distinzione riduce il rischio di produrre documenti ridondanti o incompleti.

3.5.3 Documentazione dei sistemi ad alto rischio utilizzati in qualità di deployer

Negli scenari in cui l'organizzazione utilizza un sistema ad alto rischio in qualità di deployer, l'obiettivo non è replicare la documentazione predisposta dal fornitore ma assicurare che le informazioni ricevute siano sufficienti a governare correttamente l'utilizzo del sistema nel contesto specifico.

Il presidio documentale riguarda quindi la disponibilità e l'analisi delle istruzioni per l'uso e della documentazione fornita dal fornitore, le condizioni concrete di utilizzo, le modalità di sorveglianza umana, le registrazioni generate dal sistema nella misura in cui siano sotto il controllo del deployer nonché la documentazione relativa al monitoraggio e alla gestione degli incidenti. Nei casi previsti rientrano inoltre la FRIA e gli eventuali obblighi di informazione che ricadono sul soggetto utilizzatore.

Questa impostazione evidenzia come la catena documentale sia strettamente collegata alla distribuzione dei ruoli. Il fornitore mette a disposizione la documentazione e le istruzioni previste per l'utilizzo del sistema mentre il deployer utilizza tali informazioni per configurare il proprio presidio e lo integra, quando necessario, con quelle relative allo specifico contesto di utilizzo. La qualità della governance dipende quindi anche dalla continuità informativa tra i soggetti della catena di fornitura.

3.6 Analisi degli scostamenti e avvio delle azioni di adeguamento

3.6.1 Dall'autovalutazione all'individuazione degli scostamenti

L'analisi degli scostamenti utilizza gli stessi controlli già ricompresi nel TAF e selezionati in funzione del livello di rischio e del ruolo regolatorio. Per ciascun controllo applicabile lo stato di copertura attribuito nel framework viene confrontato con le evidenze disponibili per verificare se il presidio risulti pienamente attuato o presenti ancora elementi di carenza.

Operativamente vengono coinvolte le funzioni indicate come responsabili o contributrici e viene descritta la situazione corrente. L'attenzione è rivolta sia al presidio adottato sia alla capacità di dimostrarne l'attuazione: una prassi non formalizzata può infatti non essere sufficiente a dimostrare la piena copertura di un controllo quando il requisito richiede tracciabilità, documentazione o stabilità nel tempo.

Il confronto tra stato di copertura ed evidenze consente quindi di individuare gli eventuali scostamenti rispetto al livello atteso. Tali scostamenti costituiscono l'input per le successive attività di qualificazione e per la definizione delle relative azioni di adeguamento.

3.6.2 Qualificazione dello scostamento

Quando un controllo non risulta pienamente coperto, lo scostamento viene qualificato in funzione della sua natura. Tale passaggio è necessario perché criticità apparentemente simili possono richiedere interventi differenti. La classificazione utilizzata distingue, in particolare, scostamenti di natura documentale, tecnologica e di processo.

Uno scostamento documentale riguarda la mancanza, l'incompletezza o il mancato aggiornamento di un'evidenza formalizzata. Uno scostamento tecnologico riguarda invece l'assenza o l'inadeguatezza di una misura tecnica, come meccanismi di registrazione, test, controlli sui dati in ingresso o misure di sicurezza. Uno scostamento di processo riguarda infine la mancanza di un'attività, di un momento di approvazione o validazione, di un meccanismo di coordinamento o di una chiara attribuzione di responsabilità.

La distinzione consente di indirizzare l'intervento verso la funzione competente e di distinguere azioni di formalizzazione da modifiche che incidono direttamente sul sistema o sul processo organizzativo.

Tabella 3.4: Tipologie di scostamento considerate nell'analisi

Tipologia	Caratteristica	Esempi di intervento
Documentale	Evidenza assente, incompleta o non formalizzata	Procedura, modello documentale, aggiornamento della documentazione tecnica
Tecnologico	Misura tecnica assente o insufficiente	Registrazione degli eventi, test, configurazioni di sicurezza, controlli sui dati o sul modello
Di processo	Attività o responsabilità non definite in modo adeguato	Nuovo passaggio operativo, momento di approvazione o validazione, coordinamento tra funzioni

3.6.3 Definizione delle azioni di adeguamento

Una volta qualificato lo scostamento, viene definita la relativa azione di adeguamento specificando la funzione responsabile, gli eventuali soggetti contributori, la tempistica attesa e, ove possibile, l'evidenza che dovrà dimostrarne l'avvenuta attuazione. In questo modo il piano di adeguamento costituisce la prosecuzione operativa della valutazione svolta nel TAF.

La definizione dell'azione richiede di evitare formulazioni troppo generiche. Indicazioni come «adeguare la documentazione» o «migliorare il controllo» non sono sufficienti se non chiariscono quale risultato debba essere prodotto e chi debba esserne responsabile. È stata quindi ricercata una formulazione che rendesse le azioni verificabili alla chiusura.

Un'azione documentale può consistere nella predisposizione di una nuova procedura o nell'integrazione di un modello già esistente. Un'azione tecnologica può richiedere lo sviluppo di funzionalità di registrazione degli eventi, nuovi test, controlli sui dati o misure di sicurezza. Un'azione di processo può invece introdurre un nuovo momento di verifica, una responsabilità formale o un meccanismo di coordinamento. In alcuni casi la chiusura di uno scostamento richiede una combinazione di più interventi poiché una misura tecnica può dover essere accompagnata da una procedura e da responsabilità definite.

3.6.4 Primo ciclo di applicazione e stato di avanzamento

Nel corso del lavoro è stato avviato un primo ciclo di attività su alcuni sistemi e unità organizzative in perimetro con particolare attenzione agli scenari maggiormente rilevanti. Le sessioni hanno consentito di raccogliere informazioni sullo stato dei controlli, individuare gli scostamenti e avviare la definizione delle corrispondenti azioni di adeguamento.

Alla data di stesura della presente tesi, il processo non può tuttavia essere considerato concluso. Una parte degli approfondimenti deve proseguire e alcune azioni risultano ancora da formalizzare, completare o verificare. Il framework, la logica di analisi degli scostamenti e la struttura del piano sono stati predisposti

mentre il ciclo di adeguamento deve continuare fino alla chiusura e alla verifica delle misure previste.

3.6.5 Monitoraggio delle azioni nel tempo

Per supportare il monitoraggio delle azioni definite a partire dal TAF è stato previsto un file Excel dedicato, complementare al framework e finalizzato a seguirne l'avanzamento nel tempo. La necessità di uno strumento separato deriva dall'aumento del numero di azioni, sistemi coinvolti, responsabili e scadenze che rende utile disporre di una vista consolidata delle attività aperte.

Nel file Excel, per ciascuna azione vengono mantenute informazioni quali sistema di riferimento, controllo associato, descrizione dello scostamento, intervento previsto, responsabile, tempistiche e grado di avanzamento. Quest'ultimo può essere espresso anche in termini percentuali e rappresenta lo stato di avanzamento dell'azione, non una nuova valutazione del livello di copertura del controllo.

La Figura 3.5 mostra un fac-simile semplificato del file Excel utilizzato per il monitoraggio dei piani di adeguamento, costruito con dati fittizi. Nella parte inferiore è inoltre richiamato il passaggio dalla conclusione operativa dell'azione alla verifica dell'evidenza e al successivo aggiornamento del TAF.

Remediation_Plan_Monitoring.xlsx Dati fittizi

AREA: BU_01 AI System: System_A
Business line: BL_01 Regulatory Risk Level: High-Risk

1. AI Use Cases Scenario Update +

2. Gap Progress Status

ID TAF	CONTROL GAP	RESPONSE PLAN	OWNER	% PROGRESS	DUE DATE
RSK_LOG.02	Log incompleti Tecnologico	Estensione dei log	AI Technical Team	50%	30/11/2026
RSK_INC.02	Procedura assente Documentale	Procedura incidenti	Funzione legale	25%	15/12/2026
RSK_HS.01	Ruoli non definiti Di processo	Assegnazione ruoli	AI Business Owner	100%	31/10/2026
RSK_PM.01	Piano incompleto Documentale	Piano di monitoraggio	AI Technical Team	0%	TBD

...

3. AI Committee Issue Status +

Cover: System_A System_B System_C

Azione al 100% → Verifica dell'evidenza → Aggiornamento del TAF

Figura 3.5: Fac-simile semplificato del file Excel per il monitoraggio dei piani di adeguamento e flusso di verifica delle azioni (dati fittizi)

Il completamento dell'azione non determina automaticamente la chiusura dello scostamento. Una volta implementato l'intervento e resa disponibile l'evidenza

prevista, il controllo deve essere nuovamente verificato e il relativo stato nel TAF aggiornato ove ne ricorrano le condizioni. In questo modo il monitoraggio delle azioni rimane collegato alla valutazione dei controlli e consente di mantenere coerenza tra i due strumenti.

Questa esigenza di consolidamento costituisce il punto di collegamento con il Capitolo 4. La soluzione sperimentale in Power BI nasce infatti dalla necessità di trasformare i dati contenuti nei piani di adeguamento in una vista sintetica e navigabile, utile a supportare monitoraggio, reporting e prioritizzazione delle azioni.

3.7 Predisposizione del Risk Assessment per i sistemi di IA ad alto rischio

3.7.1 Finalità, perimetro e collegamento con il sistema di gestione del rischio

Per i sistemi classificati ad alto rischio la sola verifica del livello di attuazione dei controlli non è sufficiente a rappresentare il profilo di rischio del sistema. È stata quindi predisposta una metodologia dedicata di *Risk Assessment* finalizzata a identificare e valutare i rischi noti e ragionevolmente prevedibili che possono interessare salute, sicurezza, diritti fondamentali e capacità dell'organizzazione di utilizzare il sistema in modo conforme, sicuro e affidabile.

La metodologia è stata sviluppata integrando il quadro regolatorio definito dall'AI Act con riferimenti metodologici e di gestione del rischio. L'articolo 9 disciplina il sistema di gestione del rischio richiesto ai fornitori dei sistemi di IA ad alto rischio e costituisce quindi un riferimento normativo diretto per gli scenari nei quali l'organizzazione assume tale ruolo [1]. Negli scenari in cui l'organizzazione opera come deployer, invece, il *Risk Assessment* descritto in questa sezione rappresenta uno strumento interno di governo del rischio, raccordato con le responsabilità del deployer, e non deve essere interpretato come trasposizione di un obbligo dell'articolo 9 a esso direttamente applicabile. ISO/IEC 42001 e ISO/IEC 23894 forniscono ulteriori riferimenti utili alla strutturazione del processo e dei relativi presidi [12, 13]. La metodologia è stata formalizzata in un documento Word che ne struttura finalità, perimetro, logica di valutazione, ruoli e criteri applicativi e costituisce il riferimento metodologico per il relativo strumento Excel.

Il perimetro della metodologia comprende i sistemi classificati ad alto rischio, con contenuti e controlli differenziati in funzione del ruolo regolatorio assunto dall'organizzazione. L'obiettivo non è produrre soltanto un livello sintetico ma creare una base comune per comprendere da quali caratteristiche deriva l'esposizione, quali misure siano già presenti, quale livello di rischio permanga dopo l'applicazione dei controlli e quali azioni debbano essere eventualmente introdotte.

L'individuazione dei sistemi da sottoporre alla metodologia è collegata all'inventario dei sistemi di IA. I sistemi classificati ad alto rischio vengono individuati attraverso il processo di censimento e classificazione e costituiscono il punto di ingresso della valutazione. Il *Risk Assessment* non è quindi un processo parallelo

rispetto all'*AI Lifecycle* ma un'attività specifica del percorso previsto per i sistemi ad alto rischio.

La metodologia è stata inoltre impostata come processo da mantenere nel tempo. La valutazione è soggetta a riesame periodico e può dover essere aggiornata in seguito a cambiamenti significativi nella finalità, nei dati, nella configurazione tecnica, nei processi aziendali o nel contesto di utilizzo nonché in presenza di eventi o incidenti rilevanti. La metodologia prevede in particolare un riesame almeno annuale o più frequente quando necessario. Anche sotto questo profilo il *Risk Assessment* si inserisce nella logica iterativa del modello e non rappresenta una verifica una tantum.

Sul piano operativo, la metodologia si articola in una sequenza di passaggi tra loro collegati. La definizione dei pillar e delle minacce fornisce la base per il questionario di rischio e per una checklist complementare dedicata ai gruppi vulnerabili. Le informazioni così raccolte alimentano il calcolo del rischio intrinseco. Successivamente vengono valutate le misure compensative e il relativo livello di implementazione; l'incrocio tra rischio intrinseco e livello dei controlli consente quindi di determinare il rischio residuo. L'esito della valutazione alimenta infine le eventuali azioni di trattamento e il monitoraggio nel tempo attraverso gli indicatori previsti dalla metodologia.

La Tabella 3.5 sintetizza la sequenza logica della metodologia e il ruolo svolto da ciascun passaggio nel processo di valutazione.

Tabella 3.5: Struttura logica della metodologia di Risk Assessment

Passaggio	Finalità
Definizione dei pillar	Stabilire le dimensioni attraverso cui leggere il rischio dei sistemi di IA
Individuazione delle minacce	Collegare le dimensioni di rischio a possibili eventi o condizioni di esposizione
Questionario e checklist sui gruppi vulnerabili	Raccogliere le caratteristiche rilevanti del sistema e considerare l'eventuale presenza di categorie vulnerabili nel calcolo del rischio intrinseco
Rischio intrinseco	Valutare le caratteristiche del sistema prima dell'effetto delle misure compensative
Valutazione dei controlli	Verificare il livello di implementazione dei presidi organizzativi e specifici del sistema
Rischio residuo	Combinare esposizione intrinseca e livello di implementazione dei controlli
Trattamento	Definire eventuali azioni quando il rischio residuo supera il livello ritenuto accettabile
Monitoraggio	Riesaminare il rischio attraverso aggiornamenti della valutazione e indicatori dedicati

3.7.2 Definizione dei pillar e delle minacce

La metodologia prende avvio dalla definizione di dieci pillar utilizzati come riferimento per strutturare l'analisi. Essi comprendono equità, trasparenza, spiegabilità, responsabilizzazione, integrità dei dati, affidabilità, sicurezza (*Security*), tutela della persona (*Safety*), protezione dei dati (*Privacy*) e sostenibilità. La funzione dei pillar è ordinare rischi eterogenei all'interno di categorie comuni e impedire che la valutazione venga ridotta ai soli aspetti tecnici.

Per ciascuna dimensione vengono poi individuate minacce o condizioni che possono determinare un'esposizione. La logica non consiste nel descrivere soltanto attacchi informatici o malfunzionamenti tecnici. Una minaccia può anche derivare da responsabilità non chiare, documentazione insufficiente, assenza di trasparenza, dati non adeguati, comportamenti discriminatori, incapacità di garantire un livello sufficiente di robustezza o carenze nella sorveglianza del sistema. La relativa libreria di minacce costituisce una base di lavoro della metodologia ed è suscettibile di affinamento e validazione progressiva.

A partire dai pillar e dalla libreria delle minacce sono stati strutturati gli strumenti utilizzati per la prima fase della valutazione. Il questionario di rischio, integrato nel template Excel, raccoglie informazioni sulle caratteristiche tecnologiche, organizzative e contestuali del sistema e riconduce le risposte alle dimensioni di rischio e agli scenari di minaccia individuati. A esso si affianca una checklist dedicata ai gruppi vulnerabili, utilizzata per rilevare la presenza di categorie potenzialmente esposte a impatti più rilevanti. In questo modo la successiva determinazione del rischio intrinseco rimane collegata alle caratteristiche osservate nel sistema e alle condizioni del relativo contesto di utilizzo.

3.7.3 Questionario e valutazione del rischio intrinseco

La prima valutazione quantitativa riguarda il rischio intrinseco, ossia il livello di esposizione associato alle caratteristiche del sistema prima di considerare l'effetto delle misure compensative. Il questionario costituisce lo strumento principale di raccolta delle informazioni relative al caso d'uso, alla configurazione del sistema, ai dati, al contesto operativo e agli ulteriori elementi considerati rilevanti dalla metodologia. Le possibili risposte sono associate a livelli qualitativi e valori numerici che alimentano il calcolo automatico effettuato dal template Excel.

La distinzione tra rischio intrinseco e rischio residuo è metodologicamente importante. Se la valutazione considerasse direttamente i controlli implementati, un sistema caratterizzato da un'elevata esposizione originaria potrebbe apparire poco critico soltanto perché dotato di misure compensative. Separare i due momenti consente invece di mantenere visibile la natura del rischio iniziale e, successivamente, di valutare in quale misura i controlli siano effettivamente in grado di ridurlo.

Al risultato del questionario si affianca la checklist sui gruppi vulnerabili. Quando vengono individuate categorie vulnerabili interessate dal sistema, il template applica un fattore correttivo al punteggio di rischio intrinseco, incrementandolo progressivamente in funzione delle categorie rilevate. Il punteggio complessivo viene quindi ricondotto a una classe di rischio secondo le soglie definite nella

metodologia. L'automazione del calcolo aumenta coerenza e ripetibilità ma non elimina la necessità del giudizio professionale: la qualità del risultato dipende dalla corretta comprensione del sistema, dalla completezza delle informazioni raccolte e dalla motivazione delle risposte fornite.

3.7.4 Valutazione delle misure compensative

Dopo aver determinato il rischio intrinseco, la metodologia considera le misure compensative già presenti. Nel modello progettuale queste misure sono ricondotte a due categorie complementari: controlli organizzativi e controlli specifici del sistema di IA. La distinzione consente di valutare sia il contesto di governance nel quale il sistema è inserito sia le misure tecniche e operative implementate sul singolo sistema.

La definizione dei controlli è stata inoltre raccordata agli obiettivi della ISO/IEC 42001. La metodologia include una mappatura tra i controlli organizzativi e di sistema utilizzati nel *Risk Assessment* e gli obiettivi previsti dall'Allegato A dello standard [12], così da integrare nella valutazione presidi relativi, tra gli altri, a governance, ruoli e responsabilità, gestione dei dati, sorveglianza, robustezza e miglioramento continuo. Il riferimento allo standard non sostituisce il quadro regolatorio dell'AI Act ma contribuisce a tradurlo in un insieme strutturato di controlli valutabili.

I controlli organizzativi comprendono, ad esempio, politiche, procedure, ruoli, responsabilità, meccanismi di validazione e ulteriori presidi che operano a livello trasversale. Essi non sono necessariamente legati a un singolo sistema e costituiscono l'ambiente di governance entro cui i diversi casi d'uso vengono gestiti. I controlli specifici del sistema riguardano invece misure tecniche e operative direttamente associate al caso oggetto di valutazione.

Per ciascun controllo applicabile viene valutato il livello di implementazione. La metodologia distingue tra *Implemented*, *Partially Implemented*, *Not Implemented* e *Not Applicable*. Ai primi tre stati sono associati valori numerici utilizzati nelle elaborazioni: 1 per un controllo pienamente implementato, 0 per un controllo non implementato e valori intermedi pari a 0,25, 0,50 o 0,75 nei casi di implementazione parziale. I controlli non applicabili vengono invece esclusi dalla valutazione.

La verifica del livello di implementazione deve essere svolta con il contributo delle funzioni competenti e può essere supportata da incontri dedicati, riscontri documentali e verifiche sulle evidenze. Possono quindi essere utilizzate politiche, configurazioni, documentazione tecnica, esiti di verifiche, risultati di audit o ulteriori evidenze utili a dimostrare la presenza e l'effettivo funzionamento del presidio.

Il risultato di questa fase viene sintetizzato in un livello di esposizione derivante dal grado di implementazione dei controlli. Tale valore è distinto dal rischio intrinseco e costituisce la componente utilizzata per rappresentare l'effetto dell'ambiente di controllo nella successiva determinazione del rischio residuo.

3.7.5 Determinazione del rischio residuo

Il rischio residuo viene determinato combinando il livello di rischio intrinseco con il livello derivante dalla valutazione dei controlli. La metodologia utilizza una matrice che incrocia i due risultati e restituisce un livello complessivo di rischio. La logica sottostante è intuitiva: a parità di rischio intrinseco, un sistema con controlli maggiormente implementati produce un rischio residuo inferiore rispetto a un sistema nel quale i presidi siano mancanti o insufficienti.

La Figura 3.6 rappresenta in forma semplificata la matrice utilizzata per determinare il rischio residuo, evidenziando l'incrocio tra il livello di rischio intrinseco e il livello derivante dall'implementazione dei controlli.

		Livello derivante dall'implementazione dei controlli				
Celle: rischio residuo		Molto basso	Basso	Medio	Alto	Molto alto
Rischio intrinseco	Molto alto	Basso	Medio	Alto	Alto	Molto alto
	Alto	Basso	Medio	Medio	Alto	Alto
	Medio	Basso	Basso	Medio	Medio	Medio
	Basso	Molto basso	Basso	Basso	Basso	Basso
	Molto basso	Molto basso	Molto basso	Molto basso	Molto basso	Molto basso
		Controlli più implementati ← → Controlli meno implementati				

Figura 3.6: Matrice per la determinazione del rischio residuo nella metodologia di Risk Assessment

L'utilizzo di una matrice consente di mantenere separati i due momenti della valutazione e, al tempo stesso, di produrre un risultato sintetico utilizzabile per le successive decisioni. Tale risultato non deve però essere letto come un numero autosufficiente. Il valore acquista significato soltanto se interpretato insieme alle dimensioni di rischio, alle evidenze raccolte e agli eventuali punti di debolezza identificati durante la valutazione.

La Tabella 3.6 distingue inoltre i principali livelli di origine delle scelte metodologiche. La distinzione è rilevante perché né l'AI Act né gli standard richiamati prescrivono, ad esempio, la specifica scala numerica adottata nel template o la matrice utilizzata per combinare i risultati: tali elementi costituiscono scelte progettuali e devono essere valutati come tali.

Tabella 3.6: Tracciabilità delle principali scelte della metodologia di Risk Assessment

Elemento	Origine principale	Natura della scelta
Perimetro e differenziazione per ruolo	AI Act e processo interno di classificazione	Inquadramento regolatorio tradotto nel percorso operativo del progetto
Pillar e libreria delle minacce	Riferimenti normativi e di risk management, integrati nel progetto	Tassonomia progettuale utilizzata per organizzare rischi eterogenei
Questionario e checklist sui gruppi vulnerabili	Metodologia di progetto	Strumenti operativi per rendere ripetibile la raccolta delle informazioni e introdurre nel calcolo un fattore correttivo legato alle categorie vulnerabili interessate
Controlli organizzativi e di sistema	ISO/IEC 42001 e framework progettuale	Selezione e mappatura dei presidi rilevanti rispetto al caso valutato
Scala di implementazione e valori intermedi	Metodologia di progetto	Regola quantitativa interna; non prescritta dall'AI Act o dagli standard richiamati
Matrice di rischio residuo e indicatori di rischio	Impostazione ERM del progetto	Meccanismo di sintesi e monitoraggio da consolidare attraverso le successive applicazioni sistema-specifiche

3.7.6 Trattamento del rischio e monitoraggio

Quando il rischio residuo supera i livelli di tolleranza definiti dall'organizzazione la metodologia prevede la definizione di un piano di trattamento. Le principali opzioni considerate sono la riduzione del rischio attraverso ulteriori misure, il trasferimento, l'evitamento o, nei casi motivati, l'accettazione. La scelta deve essere valutata tenendo conto del beneficio atteso, dello sforzo di implementazione e dei vincoli legali e regolatori applicabili.

Per le azioni di trattamento devono essere individuati un responsabile e una tempistica. Tale previsione crea un collegamento diretto con la logica dei piani di adeguamento descritta in precedenza: anche il risultato del *Risk Assessment* può generare azioni che devono essere monitorate fino alla loro chiusura.

La metodologia include inoltre un insieme di *Key Risk Indicators* (KRI) utilizzati come segnali di allerta per il monitoraggio nel tempo. Gli indicatori considerano dimensioni organizzative e operative e sono associati a metriche, frequenze di rilevazione e soglie di riferimento. Il confronto periodico con tali soglie consente di individuare situazioni che richiedono approfondimenti o azioni correttive.

L'introduzione dei KRI amplia la prospettiva del *Risk Assessment*: la valutazione del singolo sistema viene affiancata da indicatori capaci di rappresentare

l'esposizione complessiva dell'organizzazione. In questo modo il monitoraggio non si limita alla verifica puntuale del caso d'uso ma può supportare anche una lettura del portafoglio di sistemi ad alto rischio.

3.7.7 Ruoli, strumento operativo e stato di avanzamento

L'ERM assume un ruolo centrale nella metodologia: definisce e mantiene l'impianto di valutazione, conduce il *Risk Assessment* e coinvolge le funzioni necessarie in relazione alle caratteristiche del sistema e ai presidi da verificare. L'*AI Business Owner* e l'*AI Technical Team* contribuiscono fornendo informazioni sul caso d'uso, sulla configurazione tecnica, sui dati e sui controlli adottati, mentre le funzioni tecnologiche e di sicurezza supportano la valutazione delle misure specialistiche.

La funzione legale non partecipa direttamente all'esecuzione del *Risk Assessment*, che rimane di competenza dell'ERM. Gli esiti della valutazione possono tuttavia essere condivisi con la funzione legale qualora emergano profili che richiedano ulteriori approfondimenti di natura legale o regolatoria, inclusi quelli relativi ai diritti fondamentali.

La metodologia è accompagnata da uno strumento Excel progettato per guidare la raccolta delle informazioni e automatizzare parte delle elaborazioni. Una sezione preliminare consente di verificare il ruolo regolatorio e di filtrare i controlli pertinenti; seguono il questionario di rischio e la checklist sui gruppi vulnerabili, il calcolo del rischio intrinseco, la valutazione distinta dei controlli organizzativi e dei controlli specifici del sistema e la determinazione del rischio residuo. Una vista di sintesi riporta i principali esiti della valutazione. L'automazione consente di applicare in modo uniforme le regole di calcolo previste dalla metodologia e facilita la tracciabilità delle valutazioni senza sostituire la motivazione delle risposte né il confronto con le funzioni coinvolte.

La Figura 3.7 mostra un fac-simile semplificato dello strumento Excel, costruito con dati fittizi, che sintetizza il collegamento tra questionario, rischio intrinseco, valutazione dei controlli e determinazione del rischio residuo.

The screenshot displays the 'AI_Risk_Assessment_Template.xlsm' application. At the top, it shows 'Dati fittizi' (Fictitious Data) and configuration options: 'AI System' (System_A), 'Ruolo regolatorio' (Regulatory Role) set to 'Deployer', 'Classificazione' (Classification) set to 'High-Risk', and a 'Filtro dei controlli pertinenti' (Filter relevant controls) option.

The interface is divided into two main sections:

- Questionario e rischio intrinseco** (Questionnaire and inherent risk):

Q2	Hosting del modello	Medium
Q3	Persone impattate	High
Q12	Livello di automazione	Low
...		

Gruppi vulnerabili: 1 categoria · ×1,10

Rischio intrinseco (punteggio 142) **High**
- Valutazione dei controlli** (Controls evaluation):

Organizzativi		
ORG_01	Implemented	1
ORG_02	Partially Implemented	0,50
Specifici del sistema		
SYS_01	Partially Implemented	0,75
SYS_02	Not Implemented	0
SYS_03	Not Applicable	-

Livello da controlli **Medium**

At the bottom, a summary calculation is shown: **Rischio intrinseco** (High) × **Livello da controlli** (Medium) → **Rischio residuo** (Medium).

The bottom navigation bar includes: Pre Assessment, Questionnaire, Inherent Risk, Controls, and **Risk Evaluation**.

Figura 3.7: Fac-simile semplificato dello strumento Excel per il Risk Assessment (dati fittizi)

Alla data di stesura della presente tesi risultano completati la predisposizione della metodologia e lo sviluppo del relativo strumento Excel. Le sessioni sistema-specifiche di *Risk Assessment* non risultano invece ancora avviate. Non vengono pertanto presentati risultati riferiti ai singoli sistemi in perimetro.

3.8 Predisposizione della metodologia per la FRIA

3.8.1 Finalità e perimetro di applicazione

Accanto al *Risk Assessment* è stata sviluppata la metodologia per la valutazione degli impatti sui diritti fondamentali prevista dall'articolo 27 dell'AI Act. La Fundamental Rights Impact Assessment (FRIA) risponde a una finalità distinta rispetto alla più ampia valutazione del rischio del sistema: il suo oggetto è il potenziale impatto che l'utilizzo concreto di un sistema di IA può produrre sui diritti delle persone e dei gruppi interessati, tenendo conto dello specifico contesto nel quale il sistema viene impiegato [1].

La metodologia è stata formalizzata in un documento in formato Word che ne struttura finalità, perimetro di applicazione, ruoli, responsabilità, sequenza operativa, criteri di valutazione e modalità di aggiornamento. Il documento costituisce il riferimento metodologico per il relativo template Excel e per le istruzioni operative di compilazione, mantenendo distinto il livello metodologico dallo strumento utilizzato per eseguire e documentare la valutazione.

Nel perimetro progettuale la metodologia è stata sviluppata con particolare riferimento ai sistemi ad alto rischio utilizzati dall'organizzazione in qualità di deployer, in particolare quando il sistema è acquisito da un fornitore esterno. La valutazione non si applica tuttavia indistintamente a tutti i sistemi ad alto rischio: prima di avviarla deve essere verificato che il caso d'uso rientri effettivamente nel perimetro previsto dall'articolo 27. Quando l'organizzazione opera esclusivamente come fornitore, la valutazione relativa allo specifico utilizzo ricade sul soggetto che impiega il sistema come deployer, ove richiesta. Se invece l'organizzazione assume entrambi i ruoli, la FRIA riguarda il proprio utilizzo del sistema [1].

La valutazione deve essere completata prima del primo utilizzo nel contesto operativo rilevante. In casi analoghi il deployer può fare affidamento su FRIA svolte in precedenza o su valutazioni d'impatto esistenti effettuate dal fornitore. Qualora durante l'utilizzo cambino gli elementi sui quali la valutazione si fonda, le relative informazioni devono essere aggiornate [1]. La FRIA non è quindi un documento statico ma una valutazione contestuale legata a finalità, modalità di utilizzo, persone e gruppi interessati, durata e frequenza dell'impiego, misure di sorveglianza umana e possibili rischi di danno.

3.8.2 Governance della valutazione

La metodologia attribuisce alla funzione legale il coordinamento della FRIA. La funzione verifica l'applicabilità dell'articolo 27, presidia l'identificazione dei diritti potenzialmente interessati, documenta il razionale della valutazione e valuta i fattori relativi all'impatto. Tale ruolo è coerente con la natura della FRIA: l'individuazione del diritto potenzialmente inciso e la motivazione dell'impatto richiedono una valutazione giuridica e contestuale che non può essere sostituita da un calcolo automatico o da una sola analisi tecnica.

L'*AI Business Owner* e l'*AI Technical Team* contribuiscono alla contestualizzazione del sistema e alla raccolta delle informazioni sul caso d'uso, sulla finalità, sui processi interessati e sulle caratteristiche tecniche del sistema. A seguito dell'identificazione, da parte della funzione legale, dei diritti potenzialmente interessati, le medesime funzioni individuano e descrivono le misure rilevanti sulla base della documentazione del fornitore e contribuiscono alla valutazione della configurazione e della maturità dei relativi controlli. La funzione legale mantiene invece la responsabilità dell'identificazione dei diritti e della valutazione della gravità e della possibilità di rimedio dei potenziali impatti.

L'ERM interviene fornendo il livello derivante dalla valutazione dell'implementazione dei controlli applicabili al deployer, indicato nello strumento come *Risk level based on Control implementation* e risultante dal *Risk Assessment*. Tale informazione costituisce un input specifico della FRIA e viene utilizzata nella determinazione del rischio residuo. L'ERM non identifica i diritti fondamentali interessati e non sviluppa la relativa valutazione giuridica, mantenendo così distinta la valutazione dei controlli dalla valutazione degli impatti sui diritti fondamentali.

Quando il sistema tratta dati personali o può incidere in modo rilevante sui diritti alla vita privata e alla protezione dei dati, il Data Protection Officer può essere coinvolto a supporto della valutazione e del raccordo con l'eventuale valu-

tazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment*, DPIA). Qualora alcuni degli obblighi della FRIA risultino già soddisfatti attraverso la DPIA, la FRIA può richiamarne le sezioni pertinenti o incorporarne le parti rilevanti, evitando duplicazioni documentali [1, 9].

La FRIA viene quindi sottoposta all'*AI Advisory Committee* per il riesame degli esiti della valutazione e per eventuali ulteriori considerazioni. Nei casi che richiedano un livello decisionale ulteriore, il Committee può procedere all'escalation verso l'*AI Governance Committee* secondo i meccanismi definiti nel modello.

3.8.3 Definizione dell'insieme dei diritti fondamentali

Una fase preliminare della metodologia riguarda la definizione e l'aggiornamento dell'insieme dei diritti fondamentali da considerare. Il riferimento principale è la Carta dei diritti fondamentali dell'Unione europea e le relative spiegazioni [23, 24]. L'obiettivo è mantenere una base di valutazione completa e coerente, utilizzabile in modo sistematico nei diversi casi e aggiornata quando necessario.

Questa attività preliminare è distinta dalla successiva identificazione dei diritti effettivamente interessati dal singolo caso d'uso. La prima definisce infatti il catalogo di riferimento utilizzabile nelle valutazioni, mentre la seconda determina quali elementi di tale catalogo siano concretamente rilevanti rispetto al sistema e al relativo contesto di utilizzo.

3.8.4 Contestualizzazione del sistema

Il primo passaggio operativo riferito al singolo sistema consiste nella raccolta delle informazioni necessarie a comprenderne lo specifico contesto di utilizzo. Vengono descritti il sistema, la sua finalità, il processo nel quale viene inserito, le funzionalità principali e il modo in cui gli output vengono utilizzati. A questi elementi si aggiungono durata e frequenza dell'impiego, che consentono di distinguere, ad esempio, un utilizzo continuativo da un utilizzo periodico, occasionale o limitato a uno specifico progetto.

Particolare attenzione è dedicata alle persone e ai gruppi che possono essere interessati direttamente o indirettamente dal sistema. La metodologia richiede di considerare anche la presenza di persone o gruppi vulnerabili poiché il medesimo output può produrre effetti differenti in funzione delle caratteristiche dei destinatari. La contestualizzazione comprende inoltre la documentazione disponibile, incluse le istruzioni per l'uso, la documentazione di trasparenza e le ulteriori informazioni messe a disposizione dal fornitore.

Questa fase è metodologicamente rilevante perché evita che la FRIA venga ridotta a una lista astratta di diritti. Lo stesso sistema può infatti produrre impatti differenti se utilizzato in contesti, processi o popolazioni diverse. La valutazione deve quindi partire dall'uso concreto e non dalla sola classificazione tecnica del sistema.

3.8.5 Identificazione dei diritti potenzialmente interessati

Sulla base delle informazioni raccolte nella fase di contestualizzazione, la funzione legale esamina i diritti presenti nel catalogo di riferimento e valuta se l'utilizzo del sistema possa determinarne un impatto diretto o indiretto.

Qualora venga individuato un potenziale impatto, la valutazione deve essere accompagnata da una motivazione che descriva come esso possa concretamente manifestarsi nel contesto considerato. Il razionale così formulato documenta il collegamento tra caratteristiche del sistema, modalità di utilizzo, persone o gruppi interessati e diritto potenzialmente inciso e costituisce la base per le successive fasi della FRIA.

L'identificazione dei diritti interessati delimita quindi il perimetro della valutazione successiva. I fattori di rischio non vengono analizzati indistintamente per l'intero catalogo ma con riferimento ai diritti per i quali sia stato individuato un potenziale impatto. In questo modo l'approfondimento rimane collegato agli aspetti effettivamente rilevanti per lo specifico caso d'uso.

3.8.6 Valutazione delle misure e dei fattori di rischio

Per i diritti considerati potenzialmente interessati, la metodologia prevede la descrizione delle misure disponibili e la valutazione di quattro fattori ricondotti alle dimensioni di probabilità e impatto. La probabilità viene rappresentata attraverso la configurazione dei controlli e la maturità degli stessi. L'impatto viene invece valutato considerando la gravità del potenziale danno e la possibilità di porvi rimedio.

La configurazione dei controlli considera l'esistenza e la struttura delle misure descritte nella documentazione disponibile, distinguendo situazioni in cui i presidi siano assenti, isolati, parzialmente coordinati, sistematici o ridondanti. La maturità considera invece il livello di implementazione, documentazione, monitoraggio e verifica delle misure. L'*AI Business Owner*, con il supporto dell'*AI Technical Team*, individua e descrive le misure rilevanti sulla base della documentazione del fornitore e valuta queste due componenti della probabilità.

Sul versante dell'impatto, la funzione legale valuta la gravità del possibile pregiudizio e la possibilità di rimedio. La prima misura l'intensità del danno potenziale mentre la seconda considera quanto sia realisticamente possibile correggere, compensare o invertire il danno una volta verificatosi. La scomposizione dei fattori rende più trasparente la motivazione del risultato e consente di mantenere distinta la valutazione delle misure dalla valutazione giuridica dell'impatto sui diritti fondamentali.

La Tabella 3.7 sintetizza i quattro fattori utilizzati nella valutazione e il significato attribuito a ciascuno di essi.

Tabella 3.7: Fattori utilizzati nella valutazione FRIA

Dimensione	Fattore	Significato
Probabilità	Configurazione dei controlli	Struttura delle misure disponibili rispetto al potenziale impatto
Probabilità	Maturità dei controlli	Livello di implementazione, documentazione, monitoraggio e verifica delle misure
Impatto	Gravità del danno	Intensità del possibile pregiudizio per persone o gruppi interessati
Impatto	Possibilità di rimedio	Possibilità di correggere, compensare o invertire il danno

Per ciascun fattore il template utilizza una scala qualitativa ordinata alla quale sono associati valori numerici. Valori più elevati corrispondono a una maggiore esposizione: nel caso della configurazione e della maturità dei controlli ciò avviene quando le misure risultano meno strutturate o meno mature, mentre per i fattori di impatto valori maggiori corrispondono a danni più gravi o più difficilmente rimediabili. Le selezioni devono essere supportate dalle informazioni disponibili e motivate con riferimento allo specifico contesto di utilizzo.

3.8.7 Determinazione del livello di rischio FRIA e integrazione con il Risk Assessment

Lo strumento Excel associa valori numerici ai livelli qualitativi selezionati per i quattro fattori considerati. Per ciascun diritto interessato, il valore di conversione deriva dalla combinazione di configurazione dei controlli, maturità dei controlli, gravità del potenziale danno e possibilità di rimedio. Nel template progettuale il risultato così ottenuto è denominato *rischio intrinseco* associato al singolo diritto.

Tale denominazione richiede tuttavia una precisazione metodologica. In senso strettamente riconducibile alla gestione del rischio, un rischio intrinseco rappresenta l'esposizione prima dell'effetto dei controlli; nella FRIA progettata, invece, configurazione e maturità dei controlli concorrono già alla componente di probabilità. Il primo risultato non coincide quindi con un rischio pre-controllo puro. Nel presente elaborato viene mantenuta l'etichetta utilizzata nello strumento per coerenza con l'artefatto progettuale ma il valore viene interpretato come un livello di rischio FRIA già contestualizzato rispetto alle misure considerate. Questa distinzione evita di attribuire alla terminologia del template un significato metodologico più ampio di quello effettivamente supportato dalla formula adottata.

Il livello complessivo viene determinato sulla base dei valori relativi ai diritti effettivamente sottoposti a valutazione. In particolare, lo strumento calcola la media aritmetica dei relativi valori di conversione e la arrotonda all'intero più vicino secondo la logica definita nella metodologia. La media fornisce un indicatore sintetico ma può attenuare la visibilità di un impatto particolarmente elevato

riferito a un singolo diritto. Per questo motivo il valore aggregato non dovrebbe sostituire la lettura dei risultati a livello di singolo diritto.

Ai fini dell'interpretazione critica proposta dalla tesi, un valore elevato su uno specifico diritto deve pertanto rimanere oggetto di valutazione e, se necessario, di escalation anche quando la media complessiva risulta più contenuta. Tale presidio interpretativo rappresenta una cautela metodologica e non una modifica automatica della formula implementata nel template.

Il livello complessivo non viene utilizzato isolatamente. La funzione legale acquisisce dall'ERM il *Risk level based on Control implementation*, ovvero il risultato derivante dalla valutazione dell'implementazione dei controlli applicabili all'organizzazione in qualità di deployer effettuata nell'ambito del *Risk Assessment*. Tale valore riguarda il sistema nel suo complesso e non viene ricalcolato separatamente per ciascun diritto fondamentale.

Il raccordo richiede attenzione perché entrambi gli strumenti considerano, con finalità differenti, la presenza e l'implementazione di misure di controllo. Nella FRIA configurazione e maturità sono valutate rispetto al possibile impatto sul singolo diritto; il *Risk Assessment* restituisce invece un risultato riferito all'implementazione dei controlli del deployer sul sistema nel suo complesso.

La distinzione di finalità riduce la sovrapposizione concettuale ma, poiché le applicazioni sistema-specifiche non risultano ancora avviate, la tesi non assume come già dimostrata l'assenza di duplicazioni. Nella fase di applicazione sarà quindi necessario mantenere la tracciabilità tra misure FRIA e controlli del *Risk Assessment*, verificando che il medesimo effetto mitigante non venga conteggiato due volte.

La metodologia progettuale combina infine il livello complessivo FRIA con il *Risk level based on Control implementation* comunicato dall'ERM per determinare il rischio residuo. Tale regola costituisce una scelta metodologica interna e non una formula prescritta dall'AI Act. Il risultato va pertanto interpretato insieme alle valutazioni sui singoli diritti, alle misure considerate e alle motivazioni documentate e non come indicatore autosufficiente.

3.8.8 Azioni, valutazione finale e aggiornamento

Una volta determinato il rischio residuo, la funzione legale valuta le informazioni emerse e individua eventuali azioni necessarie a prevenire, mitigare o rimediare gli impatti. Le azioni vengono formalizzate in un piano nel quale sono definite almeno la relativa finalità, le attività previste, le responsabilità e le tempistiche di attuazione. Quando richiedono interventi tecnici, documentali o di processo, tali attività possono essere collegate ai più ampi piani di adeguamento previsti dal modello.

Gli esiti della valutazione vengono sottoposti all'*AI Advisory Committee* che può formulare ulteriori considerazioni e individuare i casi da escalare all'*AI Governance Committee*. La funzione legale tiene conto delle valutazioni emerse e formalizza quindi l'esito finale della FRIA sulla base delle informazioni raccolte, dei livelli di rischio determinati e delle eventuali azioni individuate.

La FRIA deve inoltre essere aggiornata quando cambiano gli elementi sui quali l'analisi si basa, ad esempio in caso di modifica del sistema, della finalità o delle modalità di utilizzo, delle categorie di persone interessate, della documentazione del fornitore o delle misure considerate. L'aggiornamento non riguarda quindi soltanto il risultato finale, ma richiede il riesame delle fasi interessate dalla modifica.

Una volta completata la valutazione, il deployer notifica i risultati all'autorità di vigilanza del mercato mediante il modello previsto dall'articolo 27, salvo i casi di esenzione previsti dall'articolo 46, paragrafo 1 [1].

Nel complesso, il flusso metodologico può essere sintetizzato nei seguenti passaggi:

1. verifica dell'applicabilità dell'articolo 27 e del ruolo di deployer;
2. definizione e aggiornamento dell'insieme dei diritti fondamentali da considerare;
3. contestualizzazione del sistema e raccolta delle informazioni sul caso d'uso;
4. identificazione motivata dei diritti potenzialmente interessati;
5. descrizione delle misure e valutazione dei fattori relativi a probabilità e impatto;
6. determinazione del livello di rischio FRIA per i diritti interessati e del relativo valore complessivo;
7. integrazione del *Risk level based on Control implementation* fornito dall'ERM attraverso il *Risk Assessment*;
8. determinazione del rischio residuo;
9. definizione delle eventuali azioni, riesame da parte degli organi di governance e formalizzazione della valutazione finale.

3.8.9 Strumento operativo e stato di avanzamento

La metodologia è accompagnata da un template Excel che guida la compilazione e automatizza le principali elaborazioni. Lo strumento comprende una sezione di contestualizzazione del sistema, un foglio dedicato alla valutazione dei diritti fondamentali e dei relativi fattori di rischio e una sezione *Decision* nella quale confluiscono il livello di rischio FRIA (indicato nel template come rischio intrinseco), il *Risk level based on Control implementation*, il rischio residuo, l'eventuale piano di azione e le valutazioni finali. Completano lo strumento le sezioni di supporto contenenti le scale di valutazione, i criteri di conversione, la matrice di rischio e il catalogo dei diritti fondamentali.

La Figura 3.8 mostra un fac-simile semplificato del template Excel sviluppato a supporto della FRIA, costruito con dati fittizi. La vista rappresenta in forma sintetica la valutazione dei diritti fondamentali e il successivo raccordo tra il livello complessivo risultante dalla FRIA e il *Risk level based on Control implementation*

fornito dall'ERM attraverso il *Risk Assessment*, dalla cui combinazione deriva il rischio residuo.

The screenshot shows the 'FRIA_Template.xlsx' interface with a 'Dati fittizi' (Fictitious Data) button in the top right. The main settings at the top are: AI System: System_B, Ruolo: Deployer, Utilizzo: Continuativo, and Gruppi vulnerabili: Sì.

The section 'Valutazione dei diritti fondamentali' (Fundamental Rights Assessment) contains a table with the following data:

Diritto (Carta UE)	Interessato	Config.	Probabilità		Impatto		Σ	Rischio
			Maturità	Danno	Rimedio			
Non discriminazione	Sì	3	3	4	2	12	Medium	
Protezione dei dati personali	Sì	2	3	3	3	11	Medium	
Tutela dei consumatori	Sì	3	2	3	2	10	Medium low	
Libertà di espressione	No	-	-	-	-	-	-	

Below the table, a summary calculation is shown: Rischio intrinseco (Medium) × Livello da controlli (Low) → Rischio residuo (Low). The 'Medium' is labeled 'Media dei diritti' and the 'Low' is labeled 'Dal Risk Assessment'.

At the bottom, there are navigation buttons: Contextualization, Fund. Rights (highlighted), Decision, Risk matrix, and FR Catalogue.

Figura 3.8: Fac-simile semplificato dello strumento Excel per la FRIA (dati fittizi)

La struttura dello strumento consente quindi di mantenere nello stesso artefatto la descrizione del contesto di utilizzo, la valutazione dei singoli diritti, le motivazioni associate alle scelte effettuate e gli esiti complessivi della FRIA. Le elaborazioni automatiche riguardano in particolare l'associazione dei valori numerici alle scale qualitative, il calcolo dei valori di conversione, la determinazione dei livelli di rischio e il raccordo tra il risultato complessivo della FRIA e l'input proveniente dal *Risk Assessment*.

La progettazione dello strumento ha richiesto la definizione delle scale, delle formule di conversione e dei campi da compilare. La struttura è stata progressivamente affinata per rendere più chiaro il confine tra informazioni richieste alle funzioni tecniche e di business, valutazioni di competenza della funzione legale e input provenienti dall'ERM. Questo aspetto è rilevante perché la qualità della FRIA dipende non soltanto dalle elaborazioni previste ma anche dalla chiarezza con cui vengono distribuite le responsabilità di compilazione e valutazione.

Alla data di stesura della presente tesi risultano predisposti la metodologia, le istruzioni operative e il relativo strumento Excel. Le valutazioni sistema-specifiche non risultano invece ancora avviate e non vengono pertanto presentati risultati riferiti a specifici sistemi in perimetro.

3.9 Integrazione degli strumenti e stato di avanzamento del modello

Le attività descritte nel presente capitolo mostrano come l'implementazione dell'AI governance non coincida con la produzione di un singolo framework o di un singolo documento. Il modello acquisisce operatività attraverso il collegamento tra strumenti che svolgono funzioni differenti. L'*AI Lifecycle* definisce il percorso operativo, la policy stabilisce principi e regole generali, il TAF traduce i requisiti in controlli verificabili, i modelli documentali supportano la raccolta e la tracciabilità delle evidenze, l'analisi degli scostamenti individua le differenze tra il livello di presidio atteso e quello rilevato, i piani di adeguamento trasformano gli scostamenti in azioni, il *Risk Assessment* approfondisce l'esposizione dei sistemi ad alto rischio e infine la FRIA integra, ove applicabile, la prospettiva dei diritti fondamentali.

La continuità tra tali strumenti costituisce un elemento essenziale del modello. Un aggiornamento del TAF può richiedere di riesaminare evidenze o modelli documentali; il completamento di un'azione di adeguamento deve essere seguito dalla verifica del controllo interessato e dall'eventuale aggiornamento del relativo stato di copertura; una modifica significativa del sistema può richiedere il riesame della classificazione, del *Risk Assessment* o della FRIA. Il modello assume quindi la forma di un ciclo di governo nel quale valutazione, attuazione, verifica e monitoraggio si alimentano reciprocamente.

Lo stato del progetto riflette questa natura progressiva. Le principali componenti del modello di governance (l'*AI Lifecycle*, la policy, il TAF e diversi modelli documentali) sono state sviluppate e progressivamente affinate. Le attività di analisi degli scostamenti e di adeguamento sono state avviate su alcuni sistemi e unità organizzative e devono proseguire fino alla chiusura e alla verifica delle azioni previste. Per il *Risk Assessment* sono stati predisposti la metodologia e il relativo strumento operativo mentre le sessioni sistema-specifiche non risultano ancora avviate. Analogamente, per la FRIA risultano predisposti la metodologia, le istruzioni operative e lo strumento di supporto senza che nella presente tesi vengano presentati risultati riferiti a specifici sistemi. Alcuni elementi del modello, tra cui la declinazione della governance nelle diverse realtà del gruppo, rimangono inoltre in progressiva definizione. Nel complesso il modello non viene quindi presentato come un assetto concluso ma come un sistema operativo in progressiva implementazione e affinamento.

Questa condizione rende particolarmente rilevante il tema del monitoraggio. Con l'aumento del numero di sistemi, controlli e azioni aperte, la capacità di mantenere una visione consolidata dello stato di avanzamento diventa un requisito importante per la sostenibilità del modello. Il capitolo successivo sviluppa tale esigenza attraverso la progettazione e la sperimentazione di una soluzione dedicata al monitoraggio dei piani di adeguamento.

CAPITOLO 4

Sviluppo di una soluzione sperimentale per il monitoraggio dei piani di adeguamento

4.1 Obiettivi e impostazione della sperimentazione

Il capitolo precedente ha mostrato come l'analisi degli scostamenti rispetto ai controlli del TAF possa portare alla definizione di azioni di adeguamento da attuare e monitorare nel tempo. Per ciascuna azione è necessario mantenere almeno il collegamento con il controllo da cui deriva, il sistema o perimetro interessato, il responsabile, la percentuale di avanzamento e la scadenza. Con l'aumento del numero di sistemi e unità organizzative coinvolti, la consultazione separata dei singoli file Excel rende però meno immediata la ricostruzione di una vista complessiva delle attività aperte, delle scadenze e delle situazioni che richiedono attenzione.

La sperimentazione sviluppata nel presente capitolo nasce da questa esigenza. L'obiettivo è verificare se i file Excel utilizzati per il monitoraggio dei piani di adeguamento possano continuare a essere impiegati come strumenti operativi e, nello stesso tempo, alimentare una vista trasversale capace di riunire le informazioni provenienti da più sistemi e unità organizzative. La scelta progettuale non consiste quindi nel sostituire Excel con un nuovo applicativo ma nell'aggiungere un livello dedicato alla raccolta, alla preparazione e alla visualizzazione dei dati.

A tale scopo è stato realizzato un prototipo in Power BI inteso come prova di fattibilità e non come soluzione già destinata alla messa in esercizio. La sperimentazione è stata impostata per verificare quattro aspetti principali:

- l'acquisizione uniforme di più file Excel caratterizzati da una struttura ricorrente;
- la riunione delle informazioni provenienti da fogli relativi a sistemi o perimetri differenti in un'unica tabella di monitoraggio;
- il calcolo di indicatori che si aggiornano in funzione dei filtri applicati al report;
- la costruzione di una vista di sintesi che consenta di passare dagli indicatori complessivi al dettaglio della singola azione.

La soluzione si colloca a valle degli strumenti descritti nel Capitolo 3. Il TAF continua a costituire il riferimento per la valutazione dei controlli mentre i file

Excel di monitoraggio mantengono la funzione di registrare e seguire nel tempo le azioni di adeguamento. Power BI interviene soltanto dopo questa fase: acquisisce le informazioni dai file, le organizza in modo uniforme e le rappresenta in una vista unica senza modificare la logica con cui vengono individuati gli scostamenti o definite le relative azioni.

È inoltre necessario mantenere distinta la percentuale di avanzamento di un'azione dallo stato di copertura del controllo TAF cui essa è collegata. Il raggiungimento del 100% indica che l'azione prevista è stata completata ma non comporta automaticamente la classificazione del controllo come *Globally Covered*. Come descritto nel Capitolo 3, l'aggiornamento dello stato del controllo richiede la verifica delle evidenze prodotte e una nuova valutazione. La dashboard monitora quindi l'esecuzione delle azioni di adeguamento e non la conformità dei controlli TAF.

I principali requisiti individuati per la sperimentazione sono sintetizzati nella Tabella 4.1.

Tabella 4.1: Requisiti della soluzione sperimentale di monitoraggio

Requisito	Impostazione adottata
Continuità con gli strumenti esistenti	Mantenimento dei file Excel come fonte operativa del monitoraggio
Riunione delle fonti	Lettura congiunta di più file e fogli in un'unica tabella di monitoraggio
Estendibilità	Possibilità di includere ulteriori file conformi alla stessa struttura senza ridefinire la logica generale di acquisizione
Tracciabilità	Collegamento tra azione, controllo TAF, unità organizzativa, perimetro, responsabile e scadenza
Monitoraggio	Distinzione tra stato di avanzamento dell'azione e stato rispetto alla scadenza
Analisi interattiva	Possibilità di filtrare le informazioni per unità organizzativa, perimetro, responsabile e livello di rischio regolatorio
Sintesi	Rappresentazione dei principali indicatori in un'unica pagina mantenendo la possibilità di risalire alle singole azioni

4.2 Costruzione della base informativa sperimentale

Ai fini della sperimentazione sono stati predisposti tre file Excel rappresentativi di differenti unità organizzative e dei relativi piani di adeguamento. Ciascun file contiene un foglio **Version** dedicato alle informazioni descrittive sul file e uno o più fogli di monitoraggio. Le configurazioni sono state differenziate in modo da rappresentare sia il caso in cui ciascun sistema disponga di un proprio foglio

sia quello in cui più sistemi vengano monitorati congiuntamente all'interno dello stesso perimetro.

La struttura dei fogli di monitoraggio riprende quella dello strumento descritto nel Capitolo 3. Nella parte iniziale sono riportate alcune informazioni generali tra cui unità organizzativa, ambito organizzativo, sistema o insieme di sistemi e livello di rischio regolatorio. Seguono tre sezioni: un aggiornamento relativo ai casi d'uso, la sezione **Gap Progress Status** e, ove valorizzata, una sezione dedicata ai temi da sottoporre agli organi di governance.

La sezione **Gap Progress Status** riporta i 54 controlli del TAF, ciascuno con il relativo identificativo. I campi **Control GAP** e **Response Plan** vengono valorizzati soltanto per i controlli per i quali emerge uno scostamento che richiede un intervento. Nel seguito del capitolo il **Response Plan** viene indicato come *azione di adeguamento*. L'insieme delle azioni costituisce invece il piano di adeguamento.

Ne consegue che alcune righe della sezione riportano soltanto l'identificativo del controllo mentre altre contengono anche uno scostamento, un piano di risposta, un responsabile, una percentuale di avanzamento e una scadenza. Le righe prive sia di **Control GAP** sia di **Response Plan** non rappresentano elementi da monitorare nella dashboard. La loro assenza dalla base Power BI non viene però interpretata come indicazione della non applicabilità o dello stato di copertura del controllo: tali aspetti rimangono determinati a monte attraverso il TAF.

La soluzione Power BI utilizza quindi soltanto una parte del contenuto dei fogli. Vengono acquisite le informazioni generali necessarie a identificare il perimetro e, all'interno di **Gap Progress Status**, i campi relativi a identificativo del controllo TAF, scostamento, piano di risposta, responsabile, percentuale di avanzamento e scadenza. Restano invece esclusi il foglio **Version**, la sezione di aggiornamento dei casi d'uso e quella relativa agli eventuali temi da sottoporre agli organi di governance, in quanto destinate a finalità diverse dal monitoraggio delle azioni.

Per evitare l'impiego di informazioni riconducibili a sistemi, unità organizzative o soggetti reali, i tre file sono stati popolati esclusivamente con dati sintetici. Per dati sintetici si intendono informazioni create appositamente per la sperimentazione, non riferite a casi reali ma costruite in modo da riprodurre situazioni plausibili e coerenti con la struttura del processo di monitoraggio. Le denominazioni, i responsabili, le percentuali di avanzamento e le date non rappresentano pertanto lo stato effettivo del progetto.

Nella denominazione dei file, l'espressione *Business Unit* (BU) identifica l'unità organizzativa rappresentata. La Tabella 4.2 sintetizza i tre file predisposti, i relativi fogli di monitoraggio e la configurazione rappresentata in ciascun caso.

Tabella 4.2: Configurazione dei file Excel utilizzati nella sperimentazione

File	Fogli di monitoraggio	Configurazione rappresentata
Experimental_Monitoring_BU_01.xlsx	System_A, System_B, System_C	Tre sistemi distinti, ciascuno monitorato in un foglio dedicato
Experimental_Monitoring_BU_02.xlsx	System_D, System_E	Due sistemi distinti, ciascuno monitorato in un foglio dedicato
Experimental_Monitoring_BU_03.xlsx	Un unico foglio di monitoraggio congiunto	Nove sistemi distinti (System_F1–System_F9) rappresentati attraverso un unico insieme di azioni di adeguamento

I primi due file adottano quindi la stessa logica: ciascun sistema è associato a un foglio di monitoraggio dedicato. Il terzo file rappresenta invece una configurazione differente, nella quale nove sistemi distinti sono ricondotti a un unico perimetro di monitoraggio. In questo caso l'elenco dei controlli TAF e le eventuali azioni di adeguamento sono riportati una sola volta per il perimetro complessivo, anziché essere replicati per ciascun sistema, mentre l'insieme dei sistemi interessati rimane indicato nel campo **AI System**.

La Figura 4.1 mostra, a titolo esemplificativo, un fac-simile di uno dei fogli di monitoraggio contenuti nel file **Experimental_Monitoring_BU_01.xlsx**, riferito a un singolo sistema di IA. Il file relativo a BU_02 presenta la medesima struttura generale, con fogli distinti per i sistemi monitorati. Anche il file relativo a BU_03 mantiene la stessa struttura di base del foglio, pur utilizzandola per il diverso perimetro multi-sistema appena descritto.

Experimental_Monitoring_BU_01.xlsx
Dati sintetici

AREA
BU_01
→ BU

BUSINESS LINE/SERVICE/PRODUCT/PRACTICE
BL_01
→ Business_Line

AI System
System_A
→ AI_Systems

AI System Regulatory Risk Level
High-Risk
→ Risk_Level

Casi d'uso
Esclusa

Gap Progress Status

ID TAF → TAF_ID	Control GAP → Gap	Response Plan → Azione	Owner → Owner	% progress → Progress	Due date → Due_Date_Raw
RSK_03					
RSK_04	Log incompleti	Estensione log	Owner_01	50%	30/11/2026
RSK_05					
RSK_06	Procedura assente	Nuova procedura	Owner_02	0%	TBD
...					

3. AI Committee Issue Status
Esclusa

Version
System_A
System_B
System_C

☒ Acquisito
☐ Non acquisito
→ nome
Campo Power Query

Figura 4.1: Fac-simile di un foglio di monitoraggio del file `Experimental_Monitoring_BU_01.xlsx` (dati sintetici)

Per verificare il comportamento della dashboard i file sono stati costruiti in modo da includere situazioni differenti. Alcune azioni risultano non avviate, altre in corso e altre completate, mentre le scadenze possono essere future, prossime, già superate oppure non ancora definite. Sono stati variati anche i responsabili e il numero di azioni presenti nei diversi perimetri. Questa varietà permette di controllare che classificazioni, conteggi, filtri e visualizzazioni reagiscano correttamente ai diversi casi.

Il livello di rischio regolatorio è stato mantenuto tra le informazioni disponibili e tra i filtri del report ma nei tre file sperimentali tutti i perimetri sono classificati come *High-Risk*. La prova consente quindi di verificare il collegamento tecnico del campo al modello e alla dashboard ma non una reale segmentazione tra livelli di rischio differenti.

4.3 Architettura della soluzione e trasformazione dei dati

4.3.1 Architettura e acquisizione delle fonti

La soluzione sperimentale è stata costruita secondo un'architettura semplice, coerente con l'obiettivo della prova di fattibilità. I file Excel costituiscono le fonti informative e vengono raccolti in SharePoint, piattaforma Microsoft utilizzata nel prototipo come punto centralizzato di archiviazione. Power Query, componente di Power BI dedicato all'acquisizione e alla preparazione dei dati, legge i file e applica le trasformazioni necessarie. Il risultato viene quindi caricato nel modello semantico di Power BI, ossia nella struttura dati utilizzata dal report per calcolare indicatori e alimentare le visualizzazioni.

I tre file sperimentali sono stati collocati nella cartella `Monitoring_Source` di un sito SharePoint utilizzato appositamente per la prova. In questo contesto SharePoint svolge una funzione esclusivamente tecnica: raccoglie i file in un unico punto dal quale Power BI può acquisirli. Il suo utilizzo non rappresenta una componente già definita nel progetto descritto nei capitoli precedenti ma una scelta adottata per la realizzazione del prototipo.

L'acquisizione e la trasformazione sono state realizzate in Power Query. Per alcuni passaggi è stato utilizzato l'Editor avanzato, che consente di intervenire direttamente sul codice M, il linguaggio con cui Power Query descrive le operazioni di trasformazione. La query ricerca nella cartella i file con estensione `.xlsx`, esclude gli eventuali file temporanei e ne apre il contenuto mediante la funzione `Excel.Workbook`. Un estratto della logica utilizzata è riportato di seguito:

```
Source = SharePoint.Files(
    "https://<tenant>.sharepoint.com/sites/<site>",
    [ApiVersion = 15]
),

FilteredFiles = Table.SelectRows(
    Source,
    each [Extension] = ".xlsx"
        and Text.Contains([Folder Path], "/Monitoring_Source/")
        and not Text.StartsWith([Name], "~$")
),

WithWorkbook = Table.AddColumn(
    FilteredFiles,
    "Workbook",
    each Excel.Workbook([Content], false, true)
)
```

Il collegamento alla cartella, anziché ai singoli file, permette alla query di leggere automaticamente tutte le fonti che rispettano la struttura prevista. L'aggiunta

di un ulteriore file conforme non richiede quindi una nuova connessione dedicata: il file può essere inserito nella cartella e acquisito al successivo aggiornamento. Questa caratteristica rende il prototipo estendibile rispetto al numero di fonti purché la struttura dei fogli e le etichette usate dalla query rimangano coerenti con quelle previste. Non costituisce invece una prova di scalabilità prestazionale su grandi volumi, aspetto discusso nella Sezione 4.7.

La Figura 4.2 sintetizza l'architettura logica adottata nel prototipo, evidenziando il flusso che collega i file Excel archiviati in SharePoint, le trasformazioni eseguite in Power Query e il modello semantico utilizzato da Power BI per alimentare il report.

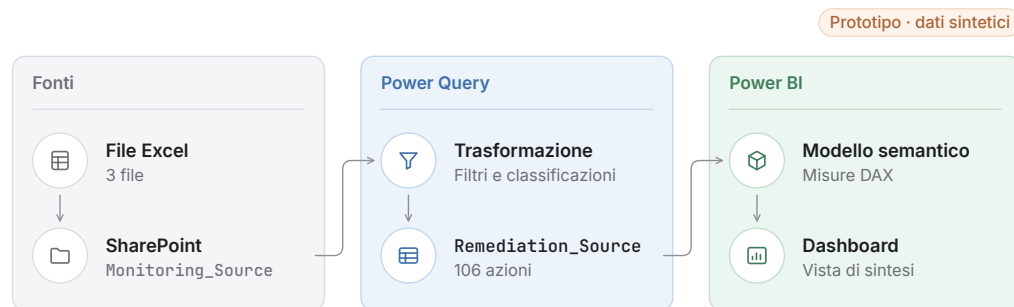


Figura 4.2: Architettura logica della soluzione sperimentale di monitoraggio

4.3.2 Trasformazione e organizzazione dei dati in Power Query

Una volta acquisiti i file dalla cartella SharePoint, Power Query ne legge il contenuto e considera i fogli contenenti i dati di monitoraggio. Il foglio **Version** viene escluso perché contiene soltanto informazioni descrittive sul file. Per ciascun foglio di monitoraggio viene invece conservato anche il nome, utilizzato nel modello per identificare il sistema o il perimetro di riferimento.

I fogli non sono organizzati come un'unica tabella continua. Nella parte iniziale sono presenti le informazioni generali sul perimetro, mentre più in basso la sezione **Gap Progress Status** contiene l'elenco dei controlli TAF e, quando presenti, le informazioni relative agli scostamenti e alle azioni di adeguamento. La query deve quindi leggere separatamente queste due parti e riunirne le informazioni sulle sole righe che rappresentano un'azione di adeguamento da monitorare.

Per recuperare le informazioni iniziali, Power Query cerca nel foglio quattro etichette: **AREA**, **BUSINESS LINE/SERVICE/PRODUCT/PRACTICE**, **AI System** e **AI System Regulatory Risk Level**. Per ciascuna etichetta viene letto il valore presente nella cella immediatamente successiva. Le informazioni ottenute vengono memorizzate nella tabella Power Query utilizzando i seguenti nomi di colonna:

AREA	-> BU
BUSINESS LINE/SERVICE/PRODUCT/PRACTICE	-> Business_Line
AI System	-> AI_Systems

AI System Regulatory Risk Level

-> Risk_Level

La ricerca avviene quindi sulla base del testo dell'etichetta e non di una coordinata fissa del foglio. Se, ad esempio, il campo **AI System** viene spostato di una riga ma mantiene la stessa etichetta e il valore rimane nella cella immediatamente a destra, la query continua a individuarlo. Rimane comunque necessario che le etichette utilizzate come riferimento e la struttura generale del foglio non vengano modificate.

La sezione **Gap Progress Status** viene letta separatamente. Power Query individua la prima riga che contiene ID TAF, la utilizza come intestazione della tabella e considera le righe successive fino alla sezione 3. **AI Committee Issue Status**. All'interno di questo intervallo vengono mantenuti soltanto i campi necessari al monitoraggio: ID TAF, Control GAP, Response Plan, Owner, % progress e Due date.

Le colonne vengono quindi rinominate in TAF_ID, Gap, Azione, Owner, Progress e Due_Date_Raw. In particolare, il campo **Response Plan** viene rinominato **Azione**: con questo termine il modello Power BI rappresenta l'azione di adeguamento prevista in risposta allo scostamento riportato nel campo **Control GAP**.

A questo punto la query elimina le righe che riportano un identificativo TAF ma non contengono né uno scostamento né un piano di risposta. Come chiarito in precedenza, la sezione contiene infatti l'intero insieme di controlli utilizzato come struttura di riferimento mentre alla dashboard interessano soltanto le righe per cui esiste un elemento da monitorare. La logica applicata può essere riassunta nel modo seguente:

```
TAF_ID inizia con "RSK_"  
and (Gap non vuoto or Azione non vuota)
```

L'esclusione delle altre righe ha una finalità esclusivamente operativa e non viene utilizzata per dedurre l'applicabilità o lo stato di copertura del controllo TAF.

Dopo aver selezionato le righe da monitorare, Power Query affianca a ciascuna di esse le informazioni già recuperate nella parte iniziale dello stesso foglio: unità organizzativa, ambito organizzativo, sistema o sistemi interessati e livello di rischio. A queste vengono aggiunti anche il nome del foglio e quello del file di origine. In questo modo, quando le righe provenienti dai diversi fogli vengono riunite in un'unica tabella, ogni azione mantiene le informazioni necessarie a identificarne il contesto di provenienza.

Il funzionamento può essere chiarito con un esempio. Se il foglio relativo a **System_A** riporta nella parte iniziale BU_01, **System_A** e il livello *High-Risk*, questi valori vengono aggiunti a tutte le azioni presenti nella sezione **Gap Progress Status** di quel foglio. Quando le azioni di **System_A** vengono poi unite a quelle degli altri sistemi, tali informazioni permettono di distinguerne immediatamente la provenienza.

La stessa logica viene applicata al terzo file sperimentale. In questo caso le azioni di adeguamento definite per il perimetro che comprende i nove sistemi

System_F1–System_F9 sono registrate una sola volta nel foglio di monitoraggio congiunto. Power Query mantiene quindi una sola riga per ciascuna azione effettivamente valorizzata nella fonte senza replicarla per ognuno dei sistemi mentre l'elenco dei nove sistemi viene conservato nel campo **AI_Systems**.

Prima del caricamento nel modello, Power Query prepara alcune informazioni necessarie alla dashboard. Il valore contenuto nel campo **Due_Date_Raw** viene innanzitutto convertito, quando possibile, in una data e memorizzato nel campo **Due_Date**. Se il valore non è convertibile, ad esempio perché contiene l'indicazione TBD, **Due_Date** viene impostato a null.

La percentuale di avanzamento viene poi utilizzata per costruire il campo **Progress_Status**. Un valore pari a 0 corrisponde a **Not started**, un valore compreso tra 0 e 1 a **In progress**, mentre il raggiungimento di 1, corrispondente al 100% di avanzamento, determina lo stato **Completed**.

Infine, Power Query costruisce il campo **Deadline_Status**. Se l'azione è completata, viene classificata come **Completed** indipendentemente dalla scadenza. Per le azioni ancora aperte, l'assenza di una data determina lo stato **To be defined**. Negli altri casi la data di scadenza viene confrontata con quella dell'aggiornamento della query. Una data già superata determina lo stato **Overdue**, una scadenza entro i successivi trenta giorni lo stato **Due soon** mentre le restanti azioni vengono classificate come **On track**.

Un estratto della logica utilizzata è il seguente:

```
Today = Date.From(DateTime.LocalNow()),

WithDeadlineStatus = Table.AddColumn(
    PreviousStep,
    "Deadline_Status",
    each
        if [Progress] <> null and [Progress] >= 1 then "Completed"
        else if [Due_Date] = null then "To be defined"
        else if [Due_Date] < Today then "Overdue"
        else if [Due_Date] <= Date.AddDays(Today, 30) then "Due soon"
        else "On track",
    type text
)
```

La soglia di trenta giorni utilizzata per la categoria **Due soon** è una scelta progettuale adottata nella sperimentazione e non deriva da un requisito dell'AI Act o del TAF. Serve esclusivamente a distinguere le azioni prossime alla scadenza da quelle con una data più lontana. Poiché il confronto viene effettuato a ogni aggiornamento della query, la classificazione temporale può variare con il trascorrere del tempo.

Al termine della trasformazione le righe provenienti da tutti i fogli vengono riunite nella tabella **Remediation_Source**. Nella configurazione sperimentale essa contiene 106 azioni: 17 per **System_A**, 16 per **System_B**, 16 per **System_C**, 17 per **System_D**, 16 per **System_E** e 24 per il perimetro di monitoraggio congiunto del terzo file.

I principali campi della tabella sono riportati nella Tabella 4.3.

Tabella 4.3: Campi principali della tabella **Remediation_Source**

Campo	Contenuto
TAF_ID	Identificativo del controllo TAF associato all'azione
Gap	Descrizione dello scostamento rilevato
Azione	Contenuto del campo Response Plan , rinominato nel modello per rappresentare l'azione di adeguamento prevista
Owner	Responsabile associato all'azione
Progress	Percentuale di avanzamento dell'azione
Due_Date	Data di scadenza utilizzata per la classificazione temporale
BU	Unità organizzativa a cui si riferisce l'azione
Business_Line	Ambito organizzativo riportato nel foglio
Perimetro	Nome del foglio utilizzato per identificare il sistema o il perimetro di monitoraggio
AI_Systems	Sistema o insieme di sistemi indicati nel foglio
Risk_Level	Livello di rischio regolatorio associato al perimetro
Source_File	File Excel dal quale proviene l'azione
Progress_Status	Stato dell'azione derivato dalla percentuale di avanzamento
Deadline_Status	Stato dell'azione derivato dalla scadenza

La tabella **Remediation_Source** costituisce quindi il risultato finale della preparazione svolta in Power Query. Ogni riga corrisponde a un'azione di adeguamento effettivamente valorizzata nella fonte e contiene sia le informazioni operative dell'azione sia quelle necessarie a identificarne il contesto di riferimento. Questa tabella viene utilizzata come base per il modello semantico e per le successive elaborazioni in Power BI.

4.4 Modello semantico e logiche di calcolo

Nel contesto di Power BI, il *modello semantico* è la struttura che rende i dati preparati in Power Query utilizzabili dal report. In pratica definisce quali tabelle e quali campi sono disponibili e quali calcoli possono essere eseguiti su di essi. Nel prototipo sviluppato il modello è volutamente semplice. La tabella principale è **Remediation_Source**, che contiene una riga per ciascuna azione di adeguamento e tutti i campi necessari per filtrare e rappresentare le informazioni nella dashboard. È presente inoltre una seconda tabella tecnica, denominata **_Misure**, che non contiene dati provenienti dai file Excel ma viene utilizzata soltanto per raccogliere e organizzare i calcoli del report.

Per realizzare questi calcoli è stato utilizzato il linguaggio *Data Analysis Expressions* (DAX), impiegato in Power BI per creare colonne calcolate e misure. Le colonne calcolate producono un nuovo valore per ciascuna riga della tabella. Le misure, invece, restituiscono un risultato aggregato che viene ricalcolato in funzione dei filtri applicati dall'utente. Ad esempio, il numero di azioni scadute non viene memorizzato come valore fisso ma viene calcolato ogni volta sul sottoinsieme di dati selezionato nella dashboard.

È inoltre necessario distinguere queste elaborazioni da quelle già svolte in Power Query. I campi **Progress_Status** e **Deadline_Status**, ad esempio, vengono creati durante la fase di trasformazione dei dati e contengono già la classificazione di ciascuna azione. DAX non ripete quindi tale classificazione ma utilizza i valori già prodotti da Power Query per costruire etichette più leggibili e indicatori da mostrare nel report.

Le colonne **Stato_Avanzamento** e **Stato_Scadenza**, ad esempio, traducono in italiano le categorie generate in Power Query. La prima viene definita come segue:

```
Stato_Avanzamento =  
SWITCH(  
    'Remediation_Source'[Progress_Status],  
    "Not started", "Non avviate",  
    "In progress", "In corso",  
    "Completed", "Completate",  
    BLANK()  
)
```

Per lo stato della scadenza viene applicata una logica analoga:

```
Stato_Scadenza =  
SWITCH(  
    'Remediation_Source'[Deadline_Status],  
    "On track", "Nei tempi",  
    "Due soon", "In scadenza",  
    "Overdue", "Scadute",  
    "To be defined", "Da definire",  
    "Completed", "Completate",  
    BLANK()  
)
```

Le due dimensioni vengono mantenute separate perché descrivono aspetti diversi. Una stessa azione può, ad esempio, essere ancora *in corso* dal punto di vista dell'avanzamento e risultare contemporaneamente *scaduta* rispetto alla data prevista. Mantenere le due informazioni distinte evita di confondere il livello di esecuzione dell'intervento con la sua situazione temporale.

È stata inoltre costruita la colonna **Stato_Sintetico**, utilizzata per fornire una lettura immediata nel dettaglio delle azioni. La logica assegna precedenza alle azioni completate e, per quelle ancora aperte, evidenzia prima le situazioni temporali che richiedono maggiore attenzione:

```

Stato_Sintetico =
SWITCH(
    TRUE(),
    'Remediation_Source'[Progress_Status] = "Completed", "Completata",
    'Remediation_Source'[Deadline_Status] = "Overdue", "Scaduta",
    'Remediation_Source'[Deadline_Status] = "Due soon", "In scadenza",
    'Remediation_Source'[Deadline_Status] = "To be defined", "Da definire",
    'Remediation_Source'[Progress_Status] = "Not started", "Non avviata",
    'Remediation_Source'[Progress_Status] = "In progress", "In corso",
    "Nei tempi"
)

```

Le misure DAX calcolano invece valori che cambiano in funzione dei filtri applicati al report. La misura di base è il numero complessivo di azioni nel contesto corrente:

```
Azioni Totali = COUNTROWS('Remediation_Source')
```

Da essa derivano, mediante CALCULATE, i conteggi relativi alle azioni non avviate, in corso, completate, nei tempi, in scadenza, scadute e con scadenza da definire. Ad esempio:

```

Azioni Scadute =
CALCULATE(
    [Azioni Totali],
    'Remediation_Source'[Deadline_Status] = "Overdue"
)

```

Alle misure di conteggio sono associate le corrispondenti percentuali. La quota di azioni scadute, ad esempio, viene calcolata come:

```

% Scadute =
DIVIDE(
    [Azioni Scadute],
    [Azioni Totali],
    0
)

```

L'utilizzo di misure è importante perché il risultato viene ricalcolato ogni volta che cambia il contesto del report. Se l'utente seleziona una determinata BU, un perimetro o un responsabile, sia il numeratore sia il denominatore si aggiornano sul sottoinsieme selezionato. Le percentuali mostrate nella dashboard non sono quindi valori fissi memorizzati nei file Excel ma risultati dell'analisi corrente.

Tra le altre misure sono stati inclusi l'avanzamento medio, il numero di controlli TAF distinti interessati dalle azioni e il numero di perimetri monitorati:

```
Avanzamento Medio =  
AVERAGE('Remediation_Source' [Progress])
```

```
Controlli TAF Interessati =  
DISTINCTCOUNT('Remediation_Source' [TAF_ID])
```

```
Perimetri Monitorati =  
DISTINCTCOUNT('Remediation_Source' [Perimetro])
```

L'avanzamento medio deve essere interpretato come indicatore dello stato di esecuzione delle azioni selezionate e non come misura della copertura dei controlli TAF. Analogamente, il numero di controlli interessati rappresenta quanti identificativi TAF compaiono tra le azioni selezionate e non quanti controlli risultano complessivamente applicabili o conformi.

Non è stato utilizzato un semplice conteggio distinto di **AI_Systems** per ricavare il numero effettivo di sistemi. Nel terzo file, infatti, il campo contiene in un'unica cella l'elenco di nove sistemi. Un **DISTINCTCOUNT** tratterebbe quell'intera stringa come un solo valore. Per questo motivo il prototipo mantiene separato il concetto di perimetro di monitoraggio dal numero di sistemi sottostanti.

Sono state inoltre predisposte due misure tecniche, **Check Avanzamento** e **Check Scadenze**, per verificare che tutte le righe ricadano in una delle categorie previste. La seconda, ad esempio, confronta il totale con la somma delle categorie temporali:

```
Check Scadenze =  
[Azioni Totali]  
- [Azioni Nei Tempi]  
- [Azioni In Scadenza]  
- [Azioni Scadute]  
- [Azioni Scadenza Da Definire]  
- [Azioni Completate Deadline]
```

Il valore atteso è zero. Un risultato diverso segnalerebbe che almeno una riga non è stata ricondotta correttamente alle categorie previste. Queste misure verificano quindi la coerenza interna del modello e non la correttezza sostanziale delle informazioni inserite nei file di origine.

La Tabella 4.4 sintetizza i principali indicatori implementati nel modello semantico e il significato attribuito a ciascuno di essi nel contesto della dashboard.

Tabella 4.4: Principali indicatori implementati nel modello semantico

Indicatore	Significato
Azioni totali	Numero complessivo di azioni nel contesto di filtro corrente
Azioni non avviate, in corso e completate	Distribuzione delle azioni rispetto allo stato di avanzamento
Azioni nei tempi, in scadenza, scadute e da definire	Distribuzione delle azioni rispetto alla scadenza
Avanzamento medio	Media delle percentuali di avanzamento delle azioni selezionate
Controlli TAF interessati	Numero di identificativi TAF distinti associati alle azioni selezionate
Perimetri monitorati	Numero di fogli o perimetri di monitoraggio distinti presenti nella selezione

4.5 Progettazione della vista di sintesi

4.5.1 Impostazione generale e filtri

La dashboard è stata progettata come una pagina unica e implementata nel prototipo Power BI con i filtri, gli indicatori, le visualizzazioni aggregate e la tabella di dettaglio descritti nelle sezioni successive. L'obiettivo è fornire una vista sintetica ma interrogabile dello stato dei piani di adeguamento. La struttura segue una lettura dall'alto verso il basso: filtri e indicatori principali nella parte superiore, distribuzioni aggregate nella fascia centrale e dettaglio delle azioni nella parte inferiore.

I filtri principali riguardano **BU**, **Perimetro**, **Owner** e **Risk_Level**. La loro combinazione modifica il contesto del report e provoca il ricalcolo delle misure DAX. La stessa pagina può quindi essere utilizzata sia come vista complessiva sia per analizzare un sottoinsieme specifico senza costruire report separati per le diverse unità organizzative o per i singoli perimetri.

I filtri **BU** e **Perimetro** sono tra loro collegati. La selezione di una determinata unità organizzativa restringe i valori disponibili nel filtro **Perimetro** ai soli sistemi o perimetri di monitoraggio associati a quella BU. Il filtro **Perimetro** rimane comunque utilizzabile anche in assenza di una precedente selezione della BU. Nelle prime due unità organizzative i valori disponibili corrispondono ai singoli sistemi monitorati mentre nel terzo scenario è disponibile un unico perimetro di monitoraggio congiunto riferito ai nove sistemi rappresentati nello stesso foglio. Il filtro per **Owner** consente invece di isolare le attività assegnate a uno specifico responsabile. Il filtro **Risk_Level** è stato incluso per mantenere il modello predisposto anche per eventuali fonti future con livelli di rischio differenti. Nella base sperimentale corrente, tuttavia, tutti i perimetri sono *High-Risk*.

4.5.2 Indicatori e visualizzazioni aggregate

La parte superiore della pagina comprende sei indicatori: azioni totali, non avviate, in corso, completate, scadute e con scadenza da definire. I primi quattro descrivono lo stato generale di avanzamento mentre gli ultimi due mettono in evidenza condizioni che richiedono un'attenzione specifica. Poiché si tratta di misure, tutti gli indicatori vengono ricalcolati automaticamente quando l'utente modifica i filtri.

Due grafici ad anello rappresentano rispettivamente la distribuzione per stato di avanzamento e quella rispetto alle scadenze. Il primo utilizza le categorie *Non avviate*, *In corso* e *Completate* mentre il secondo distingue *Nei tempi*, *In scadenza*, *Scadute*, *Da definire* e *Completate*. Le azioni concluse vengono mantenute come categoria autonoma anche nella distribuzione temporale così da non continuare a classificarle sulla sola base della scadenza originaria.

La dashboard comprende inoltre un grafico a barre per unità organizzativa, che mostra come le azioni si distribuiscono tra le diverse BU. La maggiore numerosità non viene interpretata automaticamente come indice di maggiore criticità poiché il numero di azioni può dipendere anche dal numero di sistemi analizzati e dagli scostamenti effettivamente rilevati.

4.5.3 Dettaglio delle azioni

La parte inferiore della dashboard è dedicata al dettaglio delle azioni: la tabella ne occupa l'intera larghezza, così da lasciare maggiore spazio alla consultazione delle singole azioni e delle relative informazioni operative. Per ciascuna azione sono riportati l'identificativo del controllo associato (**TAF_ID**), il perimetro di monitoraggio (**Perimetro**), l'unità organizzativa (**BU**), il sistema o insieme di sistemi interessati (**AI_Systems**), la descrizione dell'azione (**Azione**), il responsabile (**Owner**), il livello di rischio regolatorio (**Risk_Level**), la percentuale di avanzamento (**Progress**), la scadenza (**Due_Date**) e lo stato sintetico (**Stato_Sintetico**). La tabella svolge una funzione diversa rispetto ai grafici: permette di ricondurre gli indicatori aggregati alle singole azioni che li generano.

Se, ad esempio, un filtro evidenzia un numero elevato di azioni scadute, la stessa pagina consente di individuare quali azioni determinano il risultato, quale controllo TAF è associato a ciascuna azione, chi ne è responsabile, quale percentuale di avanzamento è stata registrata e quale scadenza era prevista. La dashboard mantiene così un collegamento diretto tra la vista di sintesi e il dettaglio operativo.

La Figura 4.3 rappresenta in forma grafica la dashboard implementata nel prototipo Power BI. La figura ne riproduce l'impostazione effettiva, includendo la struttura della pagina, i filtri, gli indicatori, le visualizzazioni aggregate e il dettaglio delle azioni descritti nelle sezioni precedenti. La rappresentazione è stata ricostruita appositamente ai fini della tesi, utilizzando dati ed etichette esemplificativi, per rendere più leggibili la struttura e le principali funzionalità della soluzione rispetto a una semplice schermata operativa del report. Eventuali differenze rispetto alla versione implementata riguardano pertanto aspetti di affinamento grafico e non la logica funzionale della soluzione. Alcune etichette mostrate nella figura, incluso il livello di rischio, hanno esclusivamente funzione

illustrativa: la verifica funzionale descritta nella sezione successiva utilizza la base sperimentale definita nel presente capitolo, nella quale tutti i perimetri considerati sono classificati come *High-Risk*. Nessun valore rappresenta lo stato effettivo del progetto.



Figura 4.3: Rappresentazione grafica della dashboard implementata per il monitoraggio dei piani di adeguamento

4.6 Verifica funzionale della soluzione sperimentale

La verifica della soluzione sperimentale è stata condotta con finalità esclusivamente funzionali. Poiché la base informativa utilizzata è composta da dati sintetici, i valori prodotti dalla dashboard non vengono interpretati come risultati empirici né come evidenze rappresentative del progetto reale. L'obiettivo è controllare che le trasformazioni, le classificazioni, le misure e le interazioni implementate restituiscano il comportamento atteso rispetto alle regole definite nel modello.

La verifica è stata strutturata attraverso casi di prova riconducibili ai principali requisiti della soluzione. Per ciascun caso sono stati confrontati l'input o l'azione eseguita, il comportamento atteso e il risultato osservato. La Tabella 4.5 sintetizza le verifiche principali.

Tabella 4.5: Casi principali di verifica funzionale del prototipo

Caso di prova	Input o azione	Risultato atteso	Esito osservato
Filtri gerarchici	Selezione di una BU	Indicatori e dettaglio limitati alla BU; filtro Perimetro ristretto ai valori associati	Coerente con il comportamento atteso
Filtro per responsabile	Selezione di un Owner	Ricalcolo di indicatori, grafici e tabella sulle sole azioni attribuite al responsabile	Coerente con il comportamento atteso
Avanzamento completato	Azione con avanzamento pari al 100%	Classificazione dell'azione come completata nelle logiche di avanzamento	Coerente con la regola implementata
Scadenza superata	Azione non completata con data precedente alla data di riferimento	Classificazione nella condizione di ritardo prevista dal modello	Coerente con la regola implementata
Scadenza non valorizzata	Azione senza data di scadenza	Riclassificazione nella categoria prevista per le scadenze da definire	Coerente con la regola implementata
Perimetro multi-sistema	Più sistemi associati allo stesso perimetro di monitoraggio	Una sola occorrenza dell'azione, mantenendo nel campo AI_Systems i sistemi sottostanti	Nessuna duplicazione osservata

Le selezioni per BU, Perimetro e Owner sono state verificate modificando progressivamente il contesto del report e controllando che indicatori, grafici e tabella di dettaglio reagissero in modo coerente. In particolare, la selezione di una BU restringe i valori disponibili nel filtro Perimetro ai soli elementi associati all'unità organizzativa selezionata.

La verifica ha riguardato anche le classificazioni costruite in Power Query. Le azioni predisposte nei file sperimentali coprono i diversi stati di avanzamento e le differenti condizioni temporali previste dal modello. Le misure tecniche **Check Avanzamento** e **Check Scadenze** sono state utilizzate per controllare che non rimanessero righe escluse dalle categorie definite. Tale verifica riguarda la coerenza logica del modello rispetto ai dati disponibili e non la correttezza sostanziale delle informazioni inserite nei file.

Il campo **Risk_Level** è stato verificato dal punto di vista del collegamento con il report. Poiché nella base sperimentale utilizzata per i test tutti i perimetri sono classificati come *High-Risk*, la prova consente di verificarne il funzionamento tecnico come attributo e filtro, ma non costituisce un test della segmentazione tra livelli di rischio differenti.

Una verifica specifica ha riguardato il perimetro di monitoraggio congiunto del terzo file. Il controllo ha confermato che le azioni definite a livello del perimetro vengono mantenute una sola volta nella base consolidata mentre nel campo **AI_Systems** resta disponibile l'informazione relativa ai sistemi sottostanti. Il modello conserva quindi la struttura con cui le azioni sono registrate nella fonte senza introdurre duplicazioni dovute alla presenza di più sistemi nello stesso perimetro.

Nel complesso, i casi di prova hanno fornito evidenza della coerenza funzionale del flusso rispetto ai requisiti definiti: Power Query acquisisce e uniforma le informazioni provenienti dai file Excel, il modello semantico ricalcola gli indicatori in funzione del contesto selezionato e la dashboard consente di passare dalla vista

complessiva al dettaglio della singola azione. La verifica non dimostra l'efficacia organizzativa della soluzione né un miglioramento di performance ma documenta che la soluzione sperimentale reagisce correttamente alle principali condizioni previste dal modello.

4.7 Limiti e possibili sviluppi

4.7.1 Limiti della sperimentazione

Il primo limite riguarda la natura della base informativa. La prova è stata realizzata su tre file costruiti appositamente e popolati con dati sintetici. La struttura riproduce la logica dello strumento di monitoraggio ma non consente di osservare tutte le criticità che potrebbero emergere nell'utilizzo continuativo di fonti operative reali, come errori di compilazione, etichette modificate, differenze locali nella struttura dei fogli, celle valorizzate in modo non coerente o informazioni duplicate. L'impiego di dati sintetici è stato tuttavia necessario per sperimentare la soluzione senza utilizzare informazioni riservate del progetto.

La query dipende inoltre da alcune convenzioni presenti nei file: le etichette delle informazioni iniziali, l'intestazione ID TAF, i nomi delle colonne della sezione **Gap Progress Status** e l'indicazione della sezione successiva. Una modifica sostanziale di questi elementi richiederebbe un adeguamento della trasformazione. Tale dipendenza è accettabile nella prova di fattibilità ma rappresenterebbe un punto da gestire in modo più robusto in una soluzione destinata all'uso continuativo.

Un ulteriore limite è l'assenza di una serie storica. Il prototipo rappresenta lo stato corrente delle azioni: quando una percentuale di avanzamento viene aggiornata nel file Excel, il nuovo valore sostituisce quello precedente. Non è quindi possibile ricostruire automaticamente l'evoluzione di una stessa azione nel tempo né calcolare indicatori quali velocità di avanzamento o tempi medi di chiusura.

La prova è stata inoltre eseguita su un numero limitato di fonti e su 106 azioni. Questo volume è sufficiente per verificare il funzionamento delle trasformazioni, delle misure e delle principali interazioni della dashboard ma non permette di valutare in modo significativo prestazioni e tempi di aggiornamento in presenza di centinaia di file o di un numero molto maggiore di righe. L'estendibilità della logica di acquisizione non deve quindi essere confusa con una verifica della scalabilità prestazionale.

4.7.2 Evoluzioni architetturali e del modello dati

Una possibile evoluzione consisterebbe nel separare maggiormente la funzione di compilazione dalla funzione di archiviazione. I file Excel potrebbero rimanere l'interfaccia operativa utilizzata dalle funzioni coinvolte mentre una procedura di caricamento trasferirebbe le informazioni in una fonte dati centralizzata e strutturata. Power BI potrebbe quindi leggere direttamente record organizzati

secondo uno schema condiviso, riducendo la dipendenza dalla disposizione delle celle e dalla struttura dei singoli fogli.

In un'eventuale messa in esercizio dovrebbero inoltre essere definite la frequenza di aggiornamento, le modalità di gestione degli errori e le responsabilità per la verifica del corretto caricamento. Sarebbe necessario considerare anche i profili di accesso poiché informazioni relative a sistemi, scostamenti, responsabili e scadenze potrebbero richiedere livelli di visibilità differenziati in funzione del ruolo dell'utente.

Con l'aumento del numero di sistemi e fonti anche il modello semantico potrebbe essere evoluto verso una struttura dimensionale. La tabella delle azioni potrebbe essere collegata a tabelle dedicate a sistemi, unità organizzative, controlli, responsabili, livelli di rischio e calendario. Una tabella ponte tra perimetri e sistemi permetterebbe, ad esempio, di rappresentare correttamente il caso in cui più sistemi condividono lo stesso insieme di azioni di adeguamento, mantenendo separati il conteggio delle azioni e quello dei sistemi sottostanti. Una dimensione dedicata ai controlli potrebbe inoltre consentire, in un'evoluzione futura, di integrare nel modello ulteriori informazioni descrittive provenienti dal TAF senza appesantire la tabella delle azioni.

L'introduzione di acquisizioni periodiche o di una struttura transazionale permetterebbe infine di conservare la storia delle modifiche. In questo modo la dashboard potrebbe affiancare alla fotografia dello stato corrente indicatori sull'evoluzione dei piani, sui tempi di chiusura e sulla variazione dell'avanzamento nel tempo.

4.7.3 Sviluppi della reportistica e considerazioni conclusive

La scelta di una pagina unica è coerente con l'obiettivo della sperimentazione ma non esclude ulteriori sviluppi. Una seconda pagina potrebbe essere dedicata al dettaglio operativo delle azioni mentre una vista specifica per sistema potrebbe ricostruire controlli, scostamenti e interventi riferiti a un singolo perimetro. Ulteriori estensioni potrebbero riguardare una vista storica dell'avanzamento, analisi aggiuntive sui controlli TAF qualora tali informazioni venissero integrate nel modello e indicatori relativi ai tempi di chiusura.

Nel complesso, il prototipo mostra come strumenti operativi già esistenti possano essere collegati a un livello di monitoraggio trasversale senza alterare la logica con cui vengono definite le azioni di adeguamento. I file Excel mantengono la funzione di raccolta e aggiornamento. In seguito, Power Query seleziona e organizza le informazioni necessarie, il modello semantico costruisce gli indicatori e la dashboard li rende interrogabili attraverso filtri e visualizzazioni.

La sperimentazione completa quindi il percorso sviluppato nei capitoli precedenti. Se il modello di AI governance traduce i requisiti in ruoli, procedure, controlli e azioni, il monitoraggio fornisce un supporto alla loro attuazione nel tempo. La soluzione Power BI rappresenta un esempio di come le informazioni generate dal percorso di adeguamento possano essere trasformate in una vista trasversale e interrogabile mantenendo il collegamento con gli strumenti operativi da cui hanno origine.

Conclusioni

Il lavoro ha affrontato il passaggio dai requisiti del Regolamento (UE) 2024/1689 sull'intelligenza artificiale alla costruzione e progressiva implementazione di un modello operativo di AI governance applicabile a un'organizzazione complessa. I requisiti normativi sono stati tradotti in processi, ruoli, controlli, evidenze, strumenti decisionali e meccanismi di monitoraggio, con l'obiettivo di renderli concretamente gestibili lungo il ciclo di vita dei sistemi di IA.

Il primo risultato riguarda la costruzione di una logica di instradamento dei sistemi basata sulla combinazione tra classificazione del rischio e ruolo regolatorio. Tale combinazione consente di collegare il censimento al percorso operativo applicabile e di evitare che sistemi con caratteristiche o ruoli differenti vengano gestiti attraverso un unico flusso indistinto. Il secondo risultato consiste nell'integrazione tra AI Lifecycle, modello organizzativo e TAF: le responsabilità vengono associate a momenti specifici del ciclo di vita e i requisiti sono tradotti in controlli ed evidenze verificabili, creando un collegamento tra decisione, attuazione e tracciabilità.

Il terzo risultato riguarda il passaggio dall'autovalutazione alla gestione degli scostamenti. Il TAF costituisce la base per individuare i controlli non pienamente coperti mentre i piani di adeguamento trasformano tali scostamenti in azioni con responsabilità, tempistiche e stato di avanzamento. Le prime applicazioni hanno inoltre mostrato la necessità di affinare progressivamente formulazione dei controlli, evidenze attese e attribuzione delle responsabilità, confermando la natura iterativa del modello. Per i sistemi ad alto rischio, la predisposizione del Risk Assessment e della FRIA amplia l'impianto metodologico, pur senza fornire ancora risultati sistema-specifici alla data di redazione.

Il quarto risultato riguarda la dimensione organizzativa e informativa. Sul piano della governance di gruppo, il confronto tra configurazioni centralizzate, decentralizzate e ibride ha reso espliciti i principali trade-off tra uniformità, competenze specialistiche e conoscenza del contesto locale; la configurazione ibrida rimane tuttavia una soluzione in valutazione e non un assetto già formalizzato. Sul piano del monitoraggio, il prototipo Power BI mostra la fattibilità di consolidare informazioni distribuite su più file operativi e di renderle interrogabili attraverso una vista trasversale, mantenendo il collegamento con la singola azione di adeguamento.

Un ulteriore elemento di rilievo riguarda il contesto nel quale tale percorso è stato sviluppato. La costruzione del modello si è infatti svolta in una fase nella quale il quadro normativo europeo, pur definito nei suoi principi e nei principali obblighi, è ancora accompagnato da un processo di progressiva definizione degli strumenti attuativi, degli orientamenti interpretativi e degli standard tecnici di supporto [9, 11]. In questo scenario, il lavoro non si è limitato a recepire procedure già consolidate, ma ha richiesto di tradurre requisiti normativi e riferimenti metodologici in processi, responsabilità, controlli e strumenti concretamente utilizzabili dall'organizzazione.

Da questo punto di vista, il valore del modello risiede anche nella sua funzione anticipatoria: esso consente di strutturare progressivamente il percorso di adeguamento prima che l'intero ecosistema applicativo dell'AI Act possa considerarsi stabilizzato. Il progetto ha quindi contribuito a creare le condizioni operative per governare in modo più strutturato gli adempimenti emergenti, mantenendo al contempo la flessibilità necessaria per recepire successivi chiarimenti normativi, orientamenti e standard.

Questi risultati devono essere interpretati coerentemente con l'impostazione metodologica della tesi. L'elaborato non dimostra un miglioramento quantitativo delle performance dell'organizzazione e non effettua una comparazione controllata tra una situazione precedente e una successiva. Evidenzia invece, sul piano architetturale e funzionale, come componenti originariamente gestite attraverso strumenti distinti possano essere ricondotte a un impianto comune e come le informazioni generate dal percorso di adeguamento possano essere consolidate per il monitoraggio.

Permangono inoltre limiti rilevanti. Il progetto è ancora in corso e alcune componenti non possono essere considerate concluse: le attività di adeguamento devono proseguire, le metodologie di Risk Assessment e FRIA sono state predisposte ma non risultano ancora applicate sistematicamente ai singoli sistemi e la configurazione della governance per le società estere rimane in progressiva definizione. La metodologia FRIA richiederà inoltre particolare attenzione, in fase applicativa, alla distinzione tra il livello di rischio calcolato sui diritti e l'effetto dei controlli proveniente dal Risk Assessment, così da evitare sovrapposizioni nella quantificazione dell'effetto mitigante. Anche l'uso della media tra i diritti deve essere accompagnato dalla lettura dei risultati disaggregati, affinché un impatto elevato su un singolo diritto non perda visibilità nel valore complessivo.

La soluzione Power BI ha natura sperimentale: è stata verificata su tre file e 106 azioni costruiti con dati sintetici, non conserva una serie storica e non è stata sottoposta a prove di scalabilità su volumi elevati. I risultati della sperimentazione hanno quindi valore funzionale e metodologico ma non possono essere interpretati come evidenze empiriche riferite al progetto reale. Uno sviluppo successivo potrebbe prevedere fonti maggiormente strutturate, la conservazione dello storico, controlli di qualità dei dati e una validazione su un perimetro operativo più ampio.

Il contributo della tesi consiste nella progettazione e nell'operazionalizzazione dei requisiti normativi e metodologici all'interno di un modello integrato, nonché nello sviluppo e nel progressivo affinamento delle componenti operative necessarie alla sua applicazione. Rientrano in tale percorso la costruzione degli strumenti di governance e controllo, la predisposizione delle metodologie e degli strumenti di Risk Assessment e FRIA per i sistemi ad alto rischio, la definizione delle opzioni di governance per le società estere e la progettazione e sperimentazione della soluzione informativa per il monitoraggio trasversale dei piani di adeguamento. La discussione critica delle scelte adottate e dei limiti emersi completa il percorso progettuale. In questa prospettiva, il passaggio dalla conformità normativa all'AI governance coincide con la capacità di collegare la norma a un sistema organizzativo verificabile, aggiornabile e utilizzabile lungo il ciclo di vita dei sistemi di IA.

Bibliografia e sitografia

- [1] European Parliament and Council of the European Union, *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, *Official Journal of the European Union*, L 2024/1689, 12 luglio 2024, versione consolidata vigente dal 27 luglio 2026. ELI: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.
- [2] OECD, Boston Consulting Group, INSEAD, *The Adoption of Artificial Intelligence in Firms: New Evidence for Policymaking*, OECD Publishing, Paris, 2025. DOI: <https://doi.org/10.1787/f9ef33c3-en>.
- [3] E. Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, National Institute of Standards and Technology, Gaithersburg, MD, 2023. DOI: <https://doi.org/10.6028/NIST.AI.100-1>.
- [4] M. Mäntymäki, M. Minkkinen, T. Birkstedt, M. Viljanen, “Defining organizational AI governance”, *AI and Ethics*, vol. 2, pp. 603–609, 2022. DOI: <https://doi.org/10.1007/s43681-022-00143-x>.
- [5] A. Batool, D. Zowghi, M. Bano, “AI governance: a systematic literature review”, *AI and Ethics*, vol. 5, pp. 3265–3279, 2025. DOI: <https://doi.org/10.1007/s43681-024-00653-w>.
- [6] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, European Commission, 2019. DOI: <https://doi.org/10.2759/346720>.
- [7] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, COM(2020) 65 final, Brussels, 19 febbraio 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065>.
- [8] European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, COM(2021) 206 final, Brussels, 21 aprile 2021. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>.
- [9] European Parliament and Council of the European Union, *Regulation (EU) 2026/1744 of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)*, *Official Journal of the European Union*, L 2026/1744, 24 luglio 2026. ELI: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj>.

- [10] European Commission, *Guidelines on transparency obligations for providers and deployers of AI systems*, Shaping Europe’s Digital Future, 20 luglio 2026. <https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems>, consultato il 27 settembre 2026.
- [11] European Commission, *AI Act – Regulatory framework for artificial intelligence*, Shaping Europe’s Digital Future, 2026. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>, consultato il 27 settembre 2026.
- [12] ISO/IEC, *ISO/IEC 42001:2023 – Information technology – Artificial intelligence – Management system*, International Organization for Standardization, Geneva, 2023. <https://www.iso.org/standard/81230.html>.
- [13] ISO/IEC, *ISO/IEC 23894:2023 – Information technology – Artificial intelligence – Guidance on risk management*, International Organization for Standardization, Geneva, 2023. <https://www.iso.org/standard/77304.html>.
- [14] National Institute of Standards and Technology (NIST), *AI Risk Management Framework*, pagina istituzionale aggiornata nel 2026. <https://www.nist.gov/itl/ai-risk-management-framework>, consultato il 27 settembre 2026.
- [15] K. Weber, B. Otto, H. Österle, “One Size Does Not Fit All – A Contingency Approach to Data Governance”, *ACM Journal of Data and Information Quality*, vol. 1, n. 1, Article 4, pp. 4:1–4:27, 2009. DOI: <https://doi.org/10.1145/1515693.1515696>.
- [16] B. Otto, “Organizing Data Governance: Findings from the Telecommunications Industry and Consequences for Large Service Providers”, *Communications of the Association for Information Systems*, vol. 29, Article 3, pp. 45–66, 2011. DOI: <https://doi.org/10.17705/1CAIS.02903>.
- [17] PwC Germany, *Setting up an organisation for Artificial Intelligence Excellence*, Responsible AI, s.d. <https://www.pwc.de/en/risk-regulatory/responsible-ai/setting-up-an-organisation-for-artificial-intelligence-excellence.html>, consultato il 27 settembre 2026.
- [18] S. Sicular, M. Rollings, W. Andrews, *Optimize AI Governance: Choose Centralized or Hybrid Models*, Gartner, 20 febbraio 2026. <https://www.gartner.com/en/documents/7470526>, consultato il 27 settembre 2026.
- [19] OWASP Foundation, *OWASP Machine Learning Security Top Ten*, OWASP Lab Project, versione in bozza e in aggiornamento continuo. <https://owasp.org/projects/machine-learning-security-top-ten/>, consultato il 27 settembre 2026.
- [20] A. Vassilev, A. Oprea, A. Fordyce, H. Anderson, X. Davies, M. Hamin, *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations*, NIST AI 100-2e2025, National Institute of Standards and

- Technology, Gaithersburg, MD, 2025. DOI: <https://doi.org/10.6028/NIST.A.I.100-2e2025>.
- [21] European Union Agency for Cybersecurity (ENISA), *Securing Machine Learning Algorithms*, ENISA, 14 dicembre 2021. <https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms>.
 - [22] MITRE, *ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems*, knowledge base in aggiornamento continuo. <https://atlas.mitre.org/>, consultato il 27 settembre 2026.
 - [23] European Parliament, Council of the European Union, European Commission, *Charter of Fundamental Rights of the European Union, Official Journal of the European Union*, C 326, pp. 391–407, 26 ottobre 2012. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>.
 - [24] European Parliament, Council of the European Union, European Commission, *Explanations relating to the Charter of Fundamental Rights, Official Journal of the European Union*, C 303, pp. 17–35, 14 dicembre 2007. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007X1214\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007X1214(01)).