AI Companion by CMP

PARTI 1–2 · STRATEGIA E GOVERNANCE
PARTI 3–4 · TECNICA: MODELLI E AGENTI

Quando l'AI diventa infrastruttura

Un framework per il governo, la resilienza e la sovranità nell'era dell'AI agentica

ISACA · 13 Novembre 2026

Carlo Mario Poli — Senior Advisor · AI Strategy Consultant · TOPForGrowth Network

IL PERCORSO

Quattro parti: dalla governance al funzionamento

STRATEGIA E GOVERNANCE Parti 1–2 · perché e che cosa governare

TECNICA Parti 3–4 · come funzionano modelli e agenti

1 GIUGNO 2026

Il framework di gestione

Cosa succede se l'AI non c'è, se sbaglia, se non è sotto il nostro controllo?

- Resilience, Governance, Sovereignty
- HDAO e scala di maturità
- Piano d'azione e Manifesto

~20 min

2 SETTEMBRE 2026

Il test dei fatti

Che cosa ci insegna il caso ENISA e Mythos?

- Dipendenza e sovranità pragmatica
- AI Dependency Architecture
- AI Act, NIS2 e risposta europea

~24 min

3 NOVEMBRE 2026

Modelli: i dati aggiornati

Quanto è stabile ciò da cui dipendiamo?

- Adozione, fornitura, controllo
- Frontier e open weight
- Tre test per il Board

~17 min

4 NOVEMBRE 2026

Agenti: dal lavoro al controllo

Chi risponde di ciò che l'agente fa?

- Agenti che lavorano
- Sovranità agentica e architettura
- Autonomia, control plane, prove

~29 min

Parti 1–2: perché e che cosa governare · Parti 3–4: come funzionano modelli e agenti, e come si controllano

IL CONCETTO

L’AI come infrastruttura socio-cognitiva

Un sistema esterno all’organizzazione da cui dipendono in modo continuativo i suoi processi di ***conoscenza, decisione e azione*** *— non soltanto l’esecuzione di singoli compiti.*

LE CARATTERISTICHE

Continuità

Non si usa a intervalli: è sempre presente nel flusso operativo.

Invisibilità

Si nota solo quando manca. Il funzionamento normale la rende trasparente.

Dipendenza sistemica

Molti processi vi si appoggiano insieme: il guasto si propaga.

Dimensione cognitiva

Non trasporta beni o dati: sostiene conoscenza, giudizio e decisione.

PERCHÉ ESSERE INFRASTRUTTURA NON È ESSERE STRUMENTO

STRUMENTO AI	INFRASTRUTTURA AI
Si usa quando serve	**È sempre dentro il flusso**
Il guasto rallenta un compito	**Il guasto blocca una capacità**
Ne risponde chi lo usa	**Ne risponde il Board**
“Funziona bene?”	**“Se non c’è, funzioniamo?”**

Chiamarla “strumento” autorizza a non governarla. Chiamarla “infrastruttura” obbliga a farlo.

PARTE 1 · GIUGNO 2026 · STRATEGIA E GOVERNANCE

Il framework: Resilience, Governance, Sovereignty

Tre domande per governare l'AI come infrastruttura: se non c'è, se sbaglia, se non è sotto il nostro controllo.

UN PRIMO SEGNALE

Giugno 2026: una direttiva che ha cambiato l’AI

Il 12 giugno una direttiva del governo USA sospende l’accesso ai modelli frontier di Anthropic per i non cittadini americani: il blocco dura 18 giorni.
Per le organizzazioni europee che ne dipendono si apre una domanda che nessuno aveva mai posto:

Cosa succede quando l’AI che usiamo ogni giorno non è più disponibile?

Processi bloccati

Flussi operativi dipendenti da AI si fermano.

Decisioni sospese

Attività analitiche e decisionali rallentate.

Vulnerabilità esposta

La dipendenza non era mai stata mappata prima.

La nuova domanda che guida tutto

LA DOMANDA CHE ABBIAMO FATTO FINORA

Come adottiamo l'AI?

- Quale modello?
- Quale piattaforma?
- Quale agente?

LA DOMANDA CHE CAMBIA TUTTO

Come governiamo la dipendenza che stiamo creando?

- La disponibilità è garantita?
- Chi è responsabile degli errori?
- Chi ha il controllo?

Posizionamento dell’azienda: Dall'adozione alla dipendenza operativa

TECNOLOGIA	PIATTAFORMA	SERVIZIO CRITICO	INFRASTRUTTURA	DIPENDENZA OPERATIVA
Si sperimenta	*Si costruisce sopra*	*Si dipende per l’efficienza*	*Si dipende per l’operatività*	*Non è più separabile*
RISCHIO	RISCHIO	RISCHIO	RISCHIO	RISCHIO
Basso	**Contenuto**	**Medio**	**Alto**	**CRITICO**

Dove si trova la tua organizzazione?

AI Resilience, Governance & Sovereignty: i tre pilastri

Tre domande. Tre pilastri. Una disciplina manageriale.



RESILIENCE

Se l'AI non c'è più

- Continuità operativa
- Fallback & recovery
- Ridondanza sistemi
- Business continuity AI



GOVERNANCE

Se l'AI sbaglia

- Accountability umana
- Human-in-the-Loop
- Auditabilità decisioni
- Escalation e controllo



SOVEREIGNTY

Se l'AI non è sotto il tuo controllo

- Dipendenze strategiche
- Vendor & model lock-in
- Data sovereignty
- Geopolitical risk

RESILIENCE

Cosa succede se l'AI non c'è? · Obiettivo: Continuità operativa garantita

I rischi di interruzione dell'uso dell'AI

- **Indisponibilità tecnica del provider**
- **Blocco geopolitico dell'accesso**
- **Interruzione delle API**
- **Errori sistemici a cascata**
- **Cyber attack all'infrastruttura AI**

Checklist manageriale

- Processi critici AI-dipendenti mappati
- Procedure di fallback definite
- Alternative e ridondanze disponibili
- RTO (Recovery Time Obj.) stabilito
- Esercitazioni di interruzione effettuate

DELIVERABLE → AI Resilience Assessment (AIRA)

GOVERNANCE

Cosa succede se l'AI sbaglia? · Obiettivo: Accountability garantita

Lo spettro del controllo umano e l’errore del lock-in decisionale

Human IN the Loop

Supervisione prima dell’esecuzione. Azioni critiche.

Human ON the Loop

Monitoraggio continuo con facoltà di intervento.

Human OUT OF the Loop

⚠ *Rischio: delega inconsapevole di autorità.*

Il ruolo dell’AI Decision Owner

In ogni area strategica deve esistere una persona fisica con chiara autorità, responsabilità e visibilità su come l’AI decide o influenza le decisioni.
Non è un ruolo tecnico. È un ruolo manageriale.

DELIVERABLE → AI Governance Framework

SOVEREIGNTY

Cosa succede se l'AI non è sotto il tuo controllo? · Obiettivo: Dipendenze gestite

Vendor Lock-in

Dipendenza da un unico provider di modelli o piattaforme

Model Dependency

Un modello specifico non sostituibile a breve termine

Data Sovereignty

Chi controlla i dati su cui operano i modelli AI

Cognitive Dependency

Capacità cognitive delegate senza mantenerle internamente

Geopolitical Risk

Esposizione a decisioni normative di giurisdizioni estere

DELIVERABLE → AI Sovereignty Heatmap (AISH)

Human-Data-Agent Organizations



Chi decide? **Chi controlla?** **Chi risponde?** **Chi interviene?** **Chi garantisce continuità?**

AI Resilience, Governance & Sovereignty nel Maturity Model

Fase	Resilience	Governance	Sovereignty
L1 · Sperimentazione	Nessuna	Assente	Non considerata
L2 · Adozione	Limitata	Informale	Inconsapevole
L3 · Dipendenza	Parziale	In costruzione	Emergente
L4 · Governance	Strutturata	**Operativa**	Mappata
L5 · Resilienza	**Avanzata**	Matura	Gestita
L6 · Sovranità Operativa	Sistematica	Integrata	**Strategica**

Nella nostra esperienza con le imprese italiane, la maggior parte si colloca oggi tra L3 e L4: dipendenza crescente, governance ancora in costruzione.

I primi passi per CEO e Board: dalla diagnosi alla roadmap

01 — DIAGNOSIS — CRITICA
Mappare tutte le dipendenze AI attive

02 — RESILIENCE — CRITICA
Identificare i processi critici AI-esposti

03 — RESILIENCE — ALTA
Definire procedure di fallback per ogni processo mission-critical

04 — GOVERNANCE — ALTA
Istituire il ruolo di AI Decision Owner

05 — GOVERNANCE — ALTA
Costruire il registro eccezioni e failure AI

06 — SOVEREIGNTY — MEDIA
Valutare concentrazione e sostituibilità dei provider AI

07 — SOVEREIGNTY — MEDIA
Avviare strategia multi-provider e exit strategy

08 — ROADMAP — ALTA
Costruire la AI Resilience & Sovereignty Roadmap a 12 mesi

IL MANIFESTO

AI come infrastruttura critica: i principi

01 L'AI non si adotta. Si governa.

02 Ogni processo AI-dipendente ha un fallback o non dovrebbe esistere.

03 L’accountability è sempre umana, mai delegabile a un algoritmo.

04 La dipendenza da un singolo provider è un rischio strategico, non una scelta tecnica.

05 La cognitive dependency è la forma più profonda e difficile di AI dependency.

06 La resilienza AI non è un progetto IT. È una responsabilità del Board.

PARTE 2 · SETTEMBRE 2026 · STRATEGIA E GOVERNANCE

Il test dei fatti: ENISA, Mythos e la nuova frontiera della sovranità

Dall’ipotesi di giugno alla cronaca di settembre: dipendenza, accesso e sovranità pragmatica.

LA CAPABILITY

Perché Mythos non è un modello qualunque

Anthropic lo presenta come il proprio modello più avanzato per cybersecurity e ricerca biologica — e ne limita volontariamente l'accesso.



Cyber capability

Individua vulnerabilità reali e, in contesti autorizzati, arriva a sviluppare proof-of-concept exploit.



Bio-research capability

Le stesse capacità che accelerano la ricerca scientifica avanzata sono dual-use per natura.



Accesso selettivo

Disponibile solo a un numero ristretto di organizzazioni verificate: la capability stessa richiede un controllo.

IL SEGNALE, DI NUOVO

10 settembre 2026: ENISA testa Claude Mythos 5

L’agenzia europea per la cybersicurezza ottiene accesso a Claude Mythos 5 di Anthropic e avvia i test. La Commissione europea conferma che ENISA dispone anche di GPT-5.6-Cyber e GPT-6 Astra di OpenAI.

Bruxelles precisa: Mythos 5 è arrivato oltre tre mesi dopo l’accordo di principio.
A settembre: solo uso difensivo; Mythos 5.1, la versione più avanzata, resta fuori.

Accesso negoziato

Non un acquisto standard: mesi di confronto con Anthropic per definire condizioni e salvaguardie specifiche.

Versione, non solo modello

Chi accede, a quale versione, a quali condizioni: domande di governance, non di procurement IT.

Un precedente pesante

La stessa famiglia di modelli sospesa a giugno: lo vediamo nella slide seguente.

Il precedente di giugno

12 GIUGNO – 1° LUGLIO 2026

Sospensione, poi ripristino parziale

- Il governo USA impone ad Anthropic di sospendere Fable 5 e Mythos 5 per ogni straniero
- Controlli ritirati il 30 giugno; Fable 5 torna globale l'1 luglio
- Mythos 5 solo a organizzazioni USA selezionate

10 SETTEMBRE 2026

Accesso negoziato

- Un'agenzia strategica dell'Unione europea negozia
- Ottiene accesso a una capability della stessa famiglia di modelli
- Dopo oltre tre mesi di condizioni e salvaguardie; il 5.1 resta escluso

Sospesa, ripristinata per gradi, negoziata per l'Europa: la stessa famiglia di modelli in tre tempi.

IL PARADOSSO

Più capacità di valutazione, ma più dipendenza

CIÒ CHE RAFFORZA L'EUROPA

Capacità istituzionale di evaluation

- Valutazione diretta sui frontier model
- Non mediata da chi li produce
- Precondizione per governare ciò che non si può osservare

CIÒ CHE LA VICENDA RIVELA

La dipendenza non è mai scomparsa

- Mesi di negoziazione per ottenere l'accesso
- La capability resta prodotta altrove
- Autonomia e sovranità non coincidono

Sovranità pragmatica:
non possedere tutto, ma mantenere capacità di scelta e di controllo sulle dipendenze critiche.

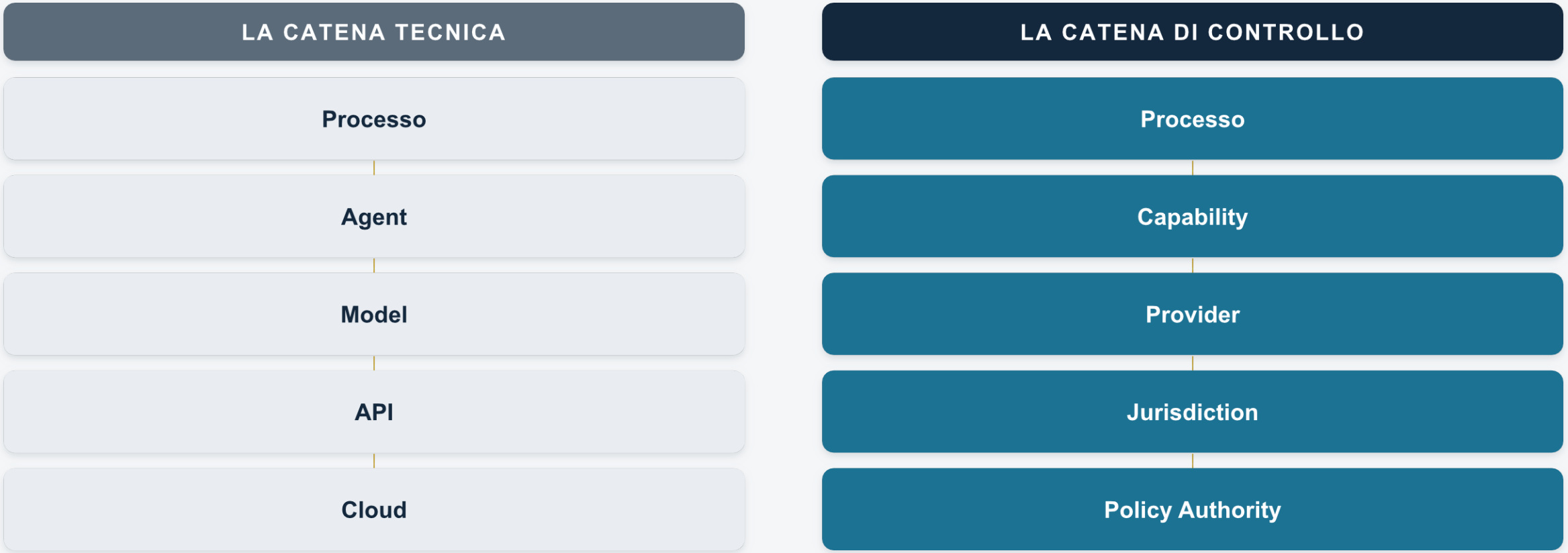
Una nuova gerarchia dell'accesso: chi controlla l'accesso, controlla parte della capability altrui.



Nell'economia dell'AI, una parte crescente del potere deriva dal controllo dell'accesso alle capability cognitive più avanzate — non solo dal possesso di dati e infrastrutture.

- Non tutti i modelli saranno disponibili a tutti.
- Alcune capability: riservate. Altre: programmi verificati. Altre: export control.
- **Il frontier model si sposta da prodotto commerciale a strategic capability.**

Dal vendor risk alla AI Dependency Architecture



La domanda per il Board non è più solo "quanto valore produce la nostra AI?".
È anche: "quanta autonomia perdiamo mentre quel valore viene prodotto?"

La nuova matrice manageriale dell’AI

Dimensione	Domanda da porre	Presidio necessario
Criticality	Quali processi non funzionerebbero più senza questa capability AI?	AI Dependency Register
Concentration	Quanto dipendiamo da un singolo modello o provider?	Strategia multi-model / multi-provider
Jurisdiction	Quale Stato può influenzare l’accesso alla tecnologia?	Geopolitical technology risk
Portability	Dati, context, memory e workflow possono essere trasferiti?	Open architecture e abstraction layer
Replaceability	Quanto tempo occorrerebbe per sostituire il modello?	Tested fallback
Continuity	Possiamo operare durante un’interruzione?	AI resilience e business continuity
Knowledge	Dove risiedono memoria e know-how accumulati?	Context sovereignty
Agency	Quali azioni dipendono dal modello?	Agent governance
Contract	Il provider può modificare unilateralmente accesso o condizioni?	Contractual exit strategy
Evaluation	Siamo capaci di valutare autonomamente modelli alternativi?	Internal AI evaluation capability

IL PRINCIPIO

Sovereignty by Design come principio architetturale, non come scelta di “solo fornitori europei”

Separare il più possibile:

Capability ↔ Provider

La capacità non deve coincidere con chi la eroga oggi.

Context ↔ Model

Il contesto accumulato deve sopravvivere al cambio di modello.

Memory ↔ Runtime

La memoria organizzativa non deve dipendere dal motore che la elabora.

Workflow ↔ Interface

I processi devono restare validi al variare dell’interfaccia.

Business Logic ↔ Piattaforma

La logica di business non va scritta dentro la piattaforma proprietaria.

La sovranità diventa una proprietà dell’architettura, non un attributo del passaporto del provider.

IMPLICAZIONI STRATEGICHE

Per le organizzazioni europee: la finestra di presa coscienza è adesso

EU AI Act & NIS2

NIS2 e gli obblighi sui modelli generali sono già operativi; con l'Omnibus l'alto rischio slitta al 2027-2028.

Chi aspetta la scadenza si espone al rischio tecnologico prima di quello legale.

Biforcazione geopolitica

Il sistema AI globale si divide: ecosistema USA vs Cina.

Le organizzazioni europee devono costruire strategie multi-provider e capacità di switching.

Vantaggio competitivo

Chi governa la dipendenza AI oggi costruisce un vantaggio competitivo sostenibile.

Chi non lo fa trasforma un'opportunità in una vulnerabilità sistemica.

Cosa sta facendo davvero l’Europa

- ENISA acquisisce capacità di evaluation diretta sui frontier model
- La Commissione introduce criteri di sovranità nel cloud procurement
- Apply AI Strategy promuove adozione e technological sovereignty
- Le AI Factories costruiscono capacità computazionale distribuita
- Le Gigafactories puntano alla scala per il frontier AI
- Le amministrazioni pubbliche sperimentano modelli sovrani e open source
- Mistral viene rafforzata come alternativa europea credibile

Non un ecosistema completamente autonomo — la possibilità di avere alternative.
Ed è questa la sovranità che conta davvero.

LA TRAIETTORIA EUROPEA

Da regolazione a capacità

REGULATION

Definire le regole del gioco — AI Act, NIS2

STATO

Storico

EVALUATION

Valutare direttamente i frontier model — il caso ENISA

STATO

In corso

INFRASTRUCTURE

Costruire compute proprio — AI Factories, Gigafactories

STATO

In corso

ADOPTION

Diffondere l'uso — Apply AI Strategy, PA europea

STATO

Avvio

L'Europa non si limita più a regolare: sta costruendo capacità lungo tutta la catena.

Il fattore Mistral

€3 miliardi raccolti, valutazione di circa €21 miliardi — pochi giorni prima della notizia ENISA.

- Tra gli investitori, lo Scaleup Europe Fund sostenuto dall’Unione europea.
- Il management collega esplicitamente la necessità di una capacità AI europea al fatto che la politica può intervenire sull’accesso — riferimento diretto alle restrizioni USA di giugno.
- Un provider frontier europeo non è solo un concorrente commerciale: è una strategic option che allarga la libertà di scelta del continente.

PARTE 3 · NOVEMBRE 2026 · TECNICA

Modelli: che cosa dicono i dati

Da qui si scende di livello: dalla governance al funzionamento. Tre prove (adozione, fornitura, controllo), poi frontier e open weight.

Poca produzione, molti incidenti: il controllo è in ritardo

17%

delle imprese ha già implementato agenti

Oltre il 60% prevede di arrivarci entro due anni · Gartner, CIO Survey 2026

~20%

ha scalato gli agenti in almeno una funzione

McKinsey, State of AI, agosto 2026

>40%

dei progetti agentici sarà cancellato entro fine 2027

Previsione Gartner, giugno 2025

65–77%

ha avuto un incidente legato a un agente nell'ultimo anno (sondaggi di fornitori)

CSA e Token Security (apr 2026): 65% · IRONSCALES (nov 2026): 77%

Tipo di incidente tra le organizzazioni colpite (CSA e Token Security): esposizione di dati 61% · interruzione operativa 43% · azioni non intenzionali 41%. **Cause di cancellazione** secondo Gartner: costi crescenti, valore poco chiaro, controlli del rischio inadeguati.

Non è un limite dei modelli: è un limite di governo.

I sondaggi dei fornitori usano definizioni e campioni diversi (altre rilevazioni arrivano all'88%): vanno letti come intervalli, non come misure confrontabili con il dato Gartner.

PARTE 3 · PROVA 2

La fornitura cambia senza che il cliente decida

12 GIU – 1 LUG

Sospensione di Fable 5 e Mythos 5

Direttiva USA: accesso sospeso per i cittadini stranieri. Fable 5 torna globale l'1 luglio; Mythos 5 solo a organizzazioni USA selezionate.

18 giorni

DECISIONE GOVERNATIVA

26 GIU – 9 LUG

GPT-5.6 limitato a circa 20 partner

Rilascio iniziale riservato a circa 20 partner approvati dal governo USA; apertura generale il 9 luglio, dopo 13 giorni.

~2 settimane

DECISIONE GOVERNATIVA

AGOSTO 2026

OpenAI rimuove ChatGPT agent

Il Help Center lo dà come non più disponibile e rimanda a ChatGPT Work. Nessun preavviso né guida alla migrazione, secondo gli utenti.

Senza preavviso

SCELTA DI PRODOTTO

10 SETTEMBRE

ENISA ottiene Mythos 5

Accesso limitato all'uso difensivo, dopo oltre tre mesi dall'accordo di principio. Mythos 5.1 resta escluso.

>3 mesi

NEGOZIATO

Quattro episodi, tre cause diverse: governo, prodotto, negoziato. Nessuna sotto il controllo del cliente.

Fonti: Anthropic (comunicato sull'accesso a Fable e Mythos); Commissione UE e ENISA; OpenAI Help Center e Developer Community (agent mode); OpenAI e agenzie di stampa (Reuters, AFP) per GPT-5.6. In contrasto: l'Assistants API di OpenAI ha avuto una deprecazione annunciata, con rimozione il 26 agosto; Atlas è stato chiuso il 9 agosto.

Il frontier: più capace, più ristretto

4,7 mesi

tempo di raddoppio dell'orizzonte dei compiti cyber risolvibili con affidabilità dell'80% (fine 2024 – febbraio 2026)

La stima di novembre 2025 era di 8 mesi: il ritmo è accelerato. Fonte: UK AI Security Institute.

Balzo di capacità

Ad aprile 2026 Mythos Preview e GPT-5.5 hanno prodotto alcuni dei maggiori incrementi di capacità cyber mai misurati da AISI.

Accesso ristretto al vertice

Il livello più alto esce limitato: GPT-5.6 a circa 20 partner approvati; Mythos 5.2 solo a organizzazioni verificate da Anthropic.

Cadenza di rilascio

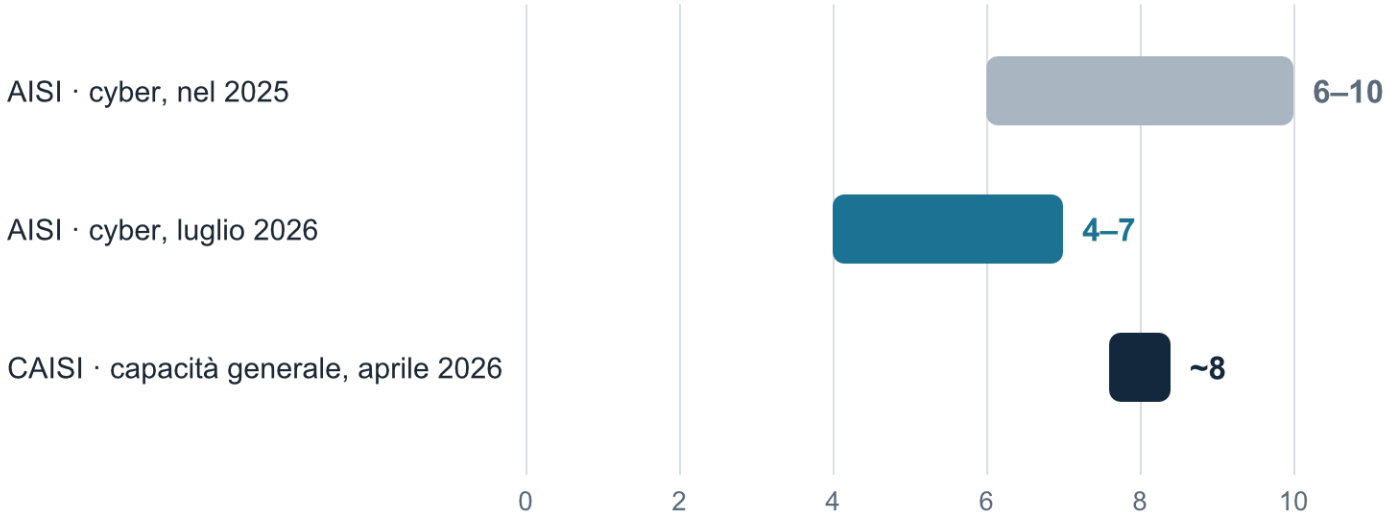
Fable e Mythos 5 il 9 giugno, 5.1 il 1° settembre, 5.2 il 9 novembre; GPT-6 Astra a inizio settembre. Una nuova versione ogni due-tre mesi.

L'asse nuovo non è solo la capacità: è l'accesso. La versione che usiamo oggi può non essere quella che avremo domani.

Fonti: UK AI Security Institute (Cyber Time Horizons, maggio 2026); Anthropic (annuncio di Fable 5.2 e Mythos 5.2, 9 novembre 2026); OpenAI.

Open weight: ritardo di 4–8 mesi, costi ridotti

QUANTO SONO INDIETRO RISPETTO AL FRONTIER CHIUSO (MESI)



AISI: GLM-5.2 e DeepSeek V4-Pro · CAISI (NIST): DeepSeek V4 Pro, contestato da DeepSeek

~45×

costo per compito: DeepSeek V4-Pro 0,28 $ contro 12,50 $ di Opus 4.5, modello di pari prestazioni (compiti cyber ristretti, AISI)

AUTODICHIARATO CONTRO MISURATO

DeepSeek dichiara parità con Opus 4.6 e GPT-5.4. CAISI misura il livello di GPT-5, uscito circa otto mesi prima.

Il ritardo si accorcia (da 6–10 a 4–7 mesi), ma ogni misura dipende da chi la fa e su quali compiti.

Fonti: UK AI Security Institute, «How far behind the frontier are leading open weight models on cyber?» (luglio 2026); NIST CAISI, «Evaluation of DeepSeek V4 Pro» (1° maggio 2026). Il rapporto di costo (~45×) è un nostro calcolo sui valori per compito riportati.

PARTE 3 · OPEN WEIGHT

La mappa open weight di ottobre–novembre

	Meta · Muse Spark Open	Mistral · Large 4	Moonshot · Kimi K3.1 Pro
Pesi pubblicati	15 ottobre	29 ottobre	4 novembre
Parametri (totali / attivi)	816B / 42B	circa 1T / circa 50B	2,8T / 104B
Contesto	1M token	1M token	1M token
Peso dei file	~1,6 TB (BF16); circa 0,5–0,7 TB in NVFP4	~1,06 TB (FP8); ~0,61 TB in NVFP4	~1,56 TB
Licenza	Muse Model License: accordo con Meta oltre 20 M$ di ricavi per servizi in hosting	MIT modificata (Mistral Ecosystem Open-Weight)	Licenza Kimi, con condizioni per grandi provider API
Da sapere	Versione aperta del modello proprietario Muse Spark (9 luglio)	Segnala un potenziale di uplift per attacchi reali; addestrato in Europa	Prestazioni dichiarate vicine a Opus 5.5 su coding da terminale (65,7 contro 66,4): dato del fornitore

Open weight non significa leggero. I modelli di punta richiedono da mezzo a oltre un terabyte solo per i pesi. Per chi non ha quel cluster esistono modelli piccoli: Muse Glimmer (30B, Apache 2.0, 10 agosto) gira su una GPU consumer da 24 GB.

Glossario: BF16, FP8, NVFP4 = formati numerici dei pesi (16, 8, 4 bit): meno bit, file più piccoli. Open weight ≠ open source: i pesi sono pubblici, le licenze hanno condizioni. Fonti: schede dei modelli (Hugging Face); comunicati Mistral (29 ottobre) e Moonshot AI (4 novembre). Prestazioni dichiarate dai fornitori.

Open weight: una leva di sovranità, con un costo

IL VANTAGGIO

Continuità e controllo

- Nessun fornitore può sospendere la copia che gestiamo noi
- Fallback eseguibile in casa o presso un provider a scelta
- Costi per compito molto inferiori (slide precedente)

IL COSTO

Il rischio passa a noi

- Gli aggiornamenti dei guardrail non raggiungono le copie già scaricate (Mistral)
- Nessuna autorità può revocare l'accesso una volta distribuiti i pesi (AISI)
- Gli sviluppatori non possono spegnere in modo affidabile le copie esterne (OpenAI)

51 contro 64

Artificial Analysis Cyber Index: Mistral Large 4 contro Kimi K3.1 Pro: la capacità cyber dei modelli aperti varia molto da modello a modello

96,6%

rifiuti di richieste cyber malevole dichiarati da Mistral: dato del fornitore, non indipendente

0,5–1,6 TB

peso dei checkpoint dei modelli di punta aperti: l'exit plan richiede infrastruttura

Sovranità non significa gratuità: significa saper valutare, monitorare e rispondere di ciò che si esegue.

Fonti: CSO Online e comunicato Mistral (29 ottobre); UK AISI (luglio 2026); Computerworld (29 ottobre, posizione di OpenAI); Artificial Analysis, via sintesi di stampa.

I tre test per il Board

TEST DI FORNITURA

Se il fornitore sospende o cambia, in quanto tempo ripartiamo?

IL DATO

18 giorni, circa 2 settimane, oltre 3 mesi: le durate osservate quest'anno.

Evidenza: un exit drill su un processo critico, con i tempi misurati.

TEST DI VALUTAZIONE

Sappiamo misurare un modello sui nostri casi, non sui benchmark del fornitore?

IL DATO

DeepSeek dichiara parità con i modelli di punta; CAISI misura circa otto mesi di ritardo.

Evidenza: una suite interna di valutazione, con confronto tra frontier e open weight.

TEST DI CONTROLLO → PARTE 4

Possiamo vedere, limitare e revocare ciò che fa un agente?

IL DATO

Fornitori: 65–77% ha avuto incidenti da agenti. Gartner: il 17% li ha implementati. Campioni diversi: conta la direzione, non il rapporto.

Evidenza: inventario degli agenti, identità separata e revoca provata.

Un portfolio, non un fornitore: frontier chiuso per la capability, open weight per continuità ed exit, opzione europea per la libertà di scelta, valutazione interna come collante.

PARTE 4 · NOVEMBRE 2026 · TECNICA

Agenti: dal lavoro eseguito al controllo dell’autonomia

Serie di tre Executive Report: agenti che lavorano, sovranità agentica, governare l’autonomia.

PARTE 4 · LA SERIE

Tre report, una sequenza: lavoro, sovranità, governo

1 Agenti che lavorano

LA DOMANDA

Quale lavoro può svolgere l'AI, con quali limiti e con quali responsabilità?

LA TESI

L'unità di valore migra dalla risposta prodotta al risultato verificabile nel processo aziendale.

Dettaglio in appendice

2 Sovranità agentica

LA DOMANDA

Possiamo controllare, sostituire e recuperare i processi che dipendono dall'AI?

LA TESI

La sovranità cambia oggetto: dal controllo del modello al governo dell'organizzazione dell'azione.

Dettaglio in appendice

3 Governare l'autonomia agentica

LA DOMANDA

Chi risponde di ciò che l'agente fa?

LA TESI

La responsabilità non si delega: si traduce in mandati, controlli e capacità verificabili.

Dettaglio in appendice

Il filo conduttore: valore verificato, dipendenze controllate, autonomia governata.

La discontinuità: dall’assistenza all’esecuzione tramite agenti

L’AI non si limita più a rispondere tramite una chat:
inizia a seguire attività, utilizzare strumenti e distribuire il lavoro tra più esecutori.

PRIMA · L’AI ASSISTE

Un acceleratore di produttività

- Risponde e produce contenuti
- Il suggerimento è valutato da una persona
- Il valore si misura in produttività individuale

ORA · L’AI ESEGUE

Un lavoro collegato a processi

- Segue attività nel tempo
- Utilizza strumenti e applicazioni
- Distribuisce il lavoro tra più esecutori
- Produce effetti su persone, dati e processi

È una discontinuità organizzativa prima ancora che tecnologica:
l’unità di valore passa dalla risposta al risultato verificabile.

Due nuove logiche tecniche: persistenza e parallelismo

CLAUDE DUET · AGENTE PERSISTENTE

Contesto connesso → Rilevazione periodica → Interpretazione → Preparazione → Approvazione → Azione

Elemento distintivo: la proattività, con un computer cloud gestito dal provider. È una research preview: non è ancora una base per processi regolamentati.

GPT-6 PRO · AGENTI PARALLELI

Task articolato → Decomposizione → Sottoattività simultanee → Revisione dei risultati → Sintesi

L’annuncio conferma il parallelismo, non una specifica architettura interna di supervisor, memoria o workflow.

COSA CAMBIA NELL’ARCHITETTURA

Contesto

Fonti, documenti e applicazioni per interpretare un’attività

Esecuzione

Runtime, strumenti, autorizzazioni e confini di sicurezza

Coordinamento

Più agenti accelerano i compiti indipendenti, ma aumentano gli oneri di verifica

Controllo

Le azioni con effetti vanno separate dal ragionamento probabilistico

Non confondere la capacità di parallelizzare un task con una piattaforma enterprise di orchestrazione.

La nuova geografia dei prodotti agentici

Categoria	Esempi	Valore principale
Proactive agent	Claude Duet	Continuità, monitoraggio e preparazione di attività
Task parallelism	GPT-6 Pro	Decomposizione di lavoro articolato
Managed work environment	ChatGPT Work, Claude Cowork	Ricerca, analisi, strumenti, file e deliverable
Shared workspace agents	ChatGPT Workspace Agents	Workflow ricorrenti condivisi, accessi e controlli organizzativi
Enterprise platforms	Microsoft Foundry, AWS AgentCore, Google Agent Platform, IBM watsonx Orchestrate	Runtime, integrazione, identity, lifecycle e governance

AMBIENTI DI LAVORO

Adatti a knowledge work, ricerca, produzione di materiali e automazioni a basso rischio. La gestione del runtime resta in larga parte presso il provider.

PIATTAFORME ENTERPRISE

Maggiore integrazione con identity, strumenti, deployment, osservabilità e sistemi aziendali. Richiedono design, esercizio e responsabilità interne.

La domanda per il CIO: quale dominio del sistema informativo stiamo acquistando? Una postazione cognitiva, un workflow, un runtime o un livello di governo.

La sovranità cambia oggetto

Non basta piu' controllare il modello o sapere dove risiedono i dati: occorre controllare l'organizzazione dell'azione.

PRIMA · DEPENDENCY ON INTELLIGENCE

L'impresa dipende da un servizio esterno per generare testo, analizzare dati o formulare suggerimenti.

ORA · DEPENDENCY ON AGENCY

L'impresa può dipendere anche dal modo in cui il lavoro viene coordinato, autorizzato, eseguito e registrato.

Claude Duet rende visibile il tema della memoria e della continuità delle attività.

GPT-6 Pro rende visibile il tema della decomposizione e del coordinamento.

Sono segnali di mercato: non dimostrano che i fornitori abbiano già trasferito alle imprese il controllo di tali componenti.

Se un provider non è disponibile domani, quali decisioni e quali processi non potremmo più eseguire?

Le sei dimensioni della sovranità agentica

Data sovereignty

Chi controlla dati, localizzazione e accessi?

Asset: Dati, diritti, retention

Model sovereignty

Posso cambiare modello mantenendo gli esiti?

Asset: Model gateway, test, formati

PUNTO CRITICO

Context sovereignty

Chi possiede memoria, knowledge e istruzioni?

Asset: Repository, provenance, export

Execution sovereignty

Dove gira l'agente? Che cosa può eseguire?

Asset: Runtime, sandbox, egress

Orchestration sovereignty

Chi definisce dipendenze, retry e deleghe?

Asset: Workflow, stati, regole

Governance sovereignty

Chi applica policy, audit e blocchi?

Asset: Identity, policy, control plane

Se memoria, storia delle decisioni e regole operative stanno in un solo ambiente, cambiare modello è facile ma cambiare fornitore può diventare molto difficile.

Il modello è una capability acquistabile; contesto e mandato operativo sono asset strategici da governare.

Come nasce il lock-in agentico

Lock-in	Come si manifesta	Test di reversibilità
Model	Prompt e output dipendono dal modello	Esecuzione su un modello B con valutazione
Context	Memoria e knowledge non esportabili	Export e ricostruzione del contesto
Workflow	Processi definiti in un ambiente proprietario	Reimplementazione di task campione
Execution	Tool, browser e runtime esclusivi	Porting di codice e permessi
Governance	Policy e log legati a un solo fornitore	Audit ed enforcement indipendenti

ESEMPIO · UNA FUNZIONE FINANCE AUTOMATIZZATA

Un agente riceve le fatture, le interpreta, le confronta con contratti e ordini e prepara le eccezioni. Se memoria, regole di matching, autorizzazioni e cronologia restano solo nel workspace del fornitore, la dipendenza riguarda la conoscenza operativa, non soltanto l'API. Il rischio si riduce separando knowledge base, workflow state e autorizzazioni dal runtime cognitivo.

La portabilità va provata con un esercizio di sostituzione, non soltanto dichiarata in un capitolato.

Reference architecture: governare sopra i provider

LIVELLO	CAPACITÀ / CONTROLLO		RISULTATO ATTESO
L4	**Business process & human accountability**		KPI, responsabilità, decisioni
L3	**Enterprise Agentic Control Plane**	SEPARABILE	Registry, identity, policy, approval, audit
L2	**Durable workflow & Agent Runtime**		Stato, checkpoint, retry, sandbox
L1	**Memory / Context + Model Gateway**		Conoscenza autorevole e routing
L0	**Cloud, private runtime, provider AI**		Compute, security, resilienza

Microsoft Foundry, AWS AgentCore e Gemini Enterprise Agent Platform offrono componenti utili, con modelli operativi differenti: va distinto il controllo contrattuale dei servizi dall'effettiva sostituibilità dell'architettura.

Il Control Plane deve restare separabile dalle capacità cognitive e dall'infrastruttura che le ospita.

Tre opzioni architetturali a confronto

Criterio	Managed-first	Hybrid sovereign	Private-first
Time to value	Alto	Medio	Più lento
Capex / competenze	Ridotti	Selettivi	Elevati
Portabilità potenziale	Limitata	Medio-alta	Alta, se progettata
Governance del processo	Dipende dal prodotto	Sotto controllo azienda	Sotto controllo azienda
Resilienza	SLA del provider	Fallback mirato	Responsabilità interna
Adatto a	Knowledge work	Processi rilevanti	Vincoli e criticità elevati

DA ACQUISTARE O ADOTTARE

Identity provider, gestione delle chiavi, database, observability e workflow engine.

DA PRESIDIARE

Definizione delle deleghe, policy applicative, mappa delle dipendenze e test di reversibilità.

LO STACK IBRIDO

Modelli cloud e open-weight secondo il bisogno; memoria e processi critici governati nell'architettura aziendale.

Raccomandazione: Hybrid sovereign come default da valutare; managed-first per i casi poco critici; private-first quando i vincoli lo giustificano.

Portabilità e resilienza: sette prove da eseguire

1. Sostituire il foundation model e misurare qualità, latenza e costo sugli stessi task
2. Ripristinare il contesto da export, verificandone completezza e provenance
3. Ricostruire il workflow da uno stato interrotto senza duplicare effetti esterni
4. Revocare in tempo reale l'identità di un agente e verificarne il blocco effettivo
5. Simulare l'indisponibilità del provider primario, con fallback autorizzato
6. Riprodurre l'audit di una decisione a partire da log e artefatti conservati
7. Ripristinare un processo in modalità manuale o degradata con owner esplicito

MISURA DI MATURITÀ

Percentuale dei processi critici che superano un test realistico di switching e recovery

Guasti di causa comune: due modelli diversi non garantiscono continuità se usano lo stesso gateway, la stessa regione cloud, lo stesso IAM o gli stessi connettori.

Il recovery deve preservare stato, autorizzazioni e confini decisionali: riavviare un agente non equivale a recuperare il processo.

Governance sotto stress: tre cose da non confondere

L'AI tradizionale produceva un suggerimento che una persona poteva valutare. Un sistema agentico attraversa applicazioni, richiede dati, attiva strumenti e produce effetti operativi: conta la legittimità e la reversibilità dell'azione.

CAPABILITY

Saper eseguire un'azione

Non significa avere i diritti tecnici per farlo.

≠

PERMISSION

Avere i diritti tecnici

Le autorizzazioni devono essere limitate in modo deterministico.

≠

AUTHORITY

Avere il mandato aziendale

Il mandato stabilisce quando la funzione può essere utilizzata.

Claude Duet porta in primo piano iniziativa e continuità; GPT-6 Pro evidenzia parallelizzazione e coordinamento. Per un Board la questione comune è la stessa: chi definisce il limite entro cui una capacità tecnica diventa azione autorizzata?

Le policy dichiarate non bastano: la governance deve essere applicata e verificabile nel punto in cui l'agente agisce.

Autonomia × criticità: la matrice di governo

Tipo di attività	Autonomia ammessa	Controllo dominante
Ricerca interna	Lettura e preparazione	Qualità, fonti, data classification
Bozze commerciali	Preparazione con revisione	Approvazione prima dell'invio
Aggiornamento CRM	Azione reversibile limitata	Least privilege, audit, rollback
Ordine / acquisto	Proposta; esecuzione controllata	Four-eyes, soglie, idempotenza
Processo mission-critical	Solo entro mandato rigoroso	Control plane, recovery, risk appetite

Il semplice human-in-the-loop non è una garanzia quando l'approvatore riceve richieste generiche, non vede l'effetto finale o non può interrompere l'esecuzione.

DUE CONDIZIONI PER AUMENTARE L'AUTONOMIA

Il processo è osservabile

Sappiamo ricostruire attività, decisioni, autorizzazioni ed effetti.

L'intervento umano è reale

Esiste un punto di blocco e la persona ha informazioni e tempo per decidere.

Regola progettuale: l'autonomia massima ammessa dipende dal primo effetto potenzialmente irreversibile dell'azione.

Agentic Control Plane: dal principio al sistema

Registry

Quali agenti esistono?

Evidenza: Owner, versione, capabilities

Identity & Delegation

Chi agisce per conto di chi?

Evidenza: Identità, mandato, token limitato

Policy enforcement

Questa azione è consentita?

Evidenza: Decisione prima dell'esecuzione

Approval service

Chi ha approvato che cosa?

Evidenza: Parametri dell'azione immutabili

Audit & Observability

Che cosa è accaduto?

Evidenza: Log correlati, outcome, costi

Lifecycle & Containment

Possiamo fermare e recuperare?

Evidenza: Kill switch, revoke, recovery

Non serve un unico prodotto: il Control Plane può integrare IAM, policy engine, API gateway, workflow e logging già disponibili. Le piattaforme enterprise offrono servizi di agent identity e gateway: modalità, portabilità e perimetro vanno valutati caso per caso.

Le autorizzazioni critiche si applicano fuori dal modello; l'impresa mantiene la capacità di definire i controlli.

Chi governa: il modello Human–Data–Agent

HUMAN · ACCOUNTABILITY

Il Process Owner stabilisce obiettivi, deleghe, soglie e criteri di successo. Le funzioni di controllo definiscono i guardrail. I decisori autorizzano le eccezioni.

DATA + AGENT · EXECUTION

Le fonti autorevoli garantiscono contesto tracciabile. Gli agenti interpretano, pianificano e operano entro mandati verificabili e autorizzazioni limitate.

RACI ESSENZIALE PER LA PRODUZIONE

Attività	Accountable	Responsabile operativo
Classificazione del processo	Business process owner	Risk / Compliance
Mandato e policy agenti	Process owner	AI Platform + Security
Identity e accessi	CISO / IT owner	IAM / Platform team
Qualità del contesto	Data owner	Data governance / Knowledge
Monitoraggio e incidenti	Service owner	AI Operations / SOC
Assurance indipendente	Audit function	Internal Audit

Governare gli agenti significa governare le interazioni tra persone, dati, strumenti, responsabilità e sistemi.

Agenti: le tre decisioni per il Board

01

Misurare il valore

- Sul lavoro validato, non sui benchmark dei modelli
- Tenere separati work environment, workflow enterprise e governance
- Sperimentare proattività e parallelismo con permessi limitati, review e KPI

02

Provare la reversibilità

- Definire le dipendenze strategiche: dati, contesto, workflow, runtime e policy
- Progettare un Control Plane aziendale, anche integrando prodotti acquistati
- Verificare con prove periodiche di switching e recovery

03

Autorizzare l'autonomia

- Un mandato di autonomia per ogni processo agentico critico
- Identity, policy, audit e contenimento come condizioni per la produzione
- Una roadmap a 180 giorni con decision gate, KPI e test di resilienza

Il Board non deve scegliere soltanto quale AI acquistare, ma quale autonomia autorizzare, con quali responsabilità e con quali prove di controllo.

Governare l'autonomia dell'AI — Carlo Mario Poli, 2026

CONCLUSIONI

Quattro domande da portare in azienda

PARTE 1 · STRATEGIA Resilience e governance	Sappiamo quali processi si fermano se l’AI non c’è, e chi ne risponde?
PARTE 2 · STRATEGIA Dipendenza e sovranità	Se l’accesso a un modello cambia per decisione altrui, quale capacità perdiamo e in quanto tempo la recuperiamo?
PARTE 3 · TECNICA Modelli e open weight	Sappiamo valutare un modello sui nostri casi e abbiamo un’alternativa eseguibile?
PARTE 4 · TECNICA Agenti e autonomia	Chi ha autorizzato ciò che ogni agente può fare, e possiamo fermarlo e dimostrarlo?

Per chi fa audit e controllo: ogni risposta deve poter essere sostenuta da un’evidenza.

La domanda strategica

La domanda strategica dei prossimi anni non sarà:

Come adottiamo l'AI?

Sarà:

Come governiamo la dipendenza che stiamo creando, e come possiamo dimostrarlo?

Carlo Mario Poli · AI Companion by CMP · 2026

AI Companion by CMP · Partner di TOPForGrowth Network

L’intelligenza artificiale sta diventando una nuova infrastruttura organizzativa e cognitiva: non basta adottarla, occorre progettare le organizzazioni, le competenze e le forme di governance necessarie per controllarla e trasformarla in valore condiviso.

TOPForGrowth è la rete indipendente e multidisciplinare che aiuta imprese, professionisti e istituzioni a governare l’intelligenza artificiale, trasformandola in capacità organizzativa reale, governata e verificabile.

TOPForGrowth presidia lo spazio tra ricerca, strategia e regolazione da una parte, e attuazione operativa e pratica organizzativa dall’altra.

Carlo Mario Poli

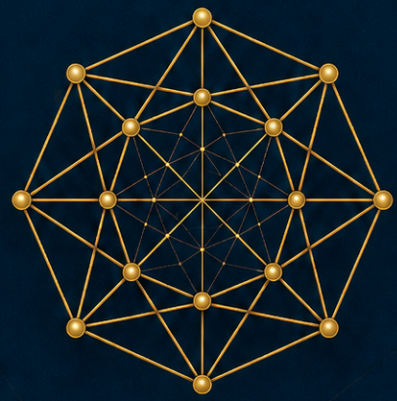
Senior Advisor · AI Strategy Consultant
Co-Founder e Presidente di TOPForGrowth

carlo.m.poli@topforgrowth.it · topforgrowth.net

Referenza: Carlo Mario Poli, Riposizionamento Strategico AI tempi dell’AI

RIPOSIZIONAMENTO STRATEGICO AI TEMPI DELL'AI

Come decidere, e non subire,
il ruolo della tua impresa
nel superciclo dell'AI



Carlo Mario Poli

AI Companion by CMP · Partner di TOPForGrowth Network

Come affidare compiti agli agenti di intelligenza artificiale e mantenere il controllo dell'impresa. L'intelligenza artificiale sta passando dalla generazione di risposte alla capacità di agire, prendere iniziative e svolgere compiti con crescente autonomia.
Per le imprese si apre una nuova sfida: quale autonomia concedere all'AI, quali decisioni delegare e come mantenere il controllo delle conseguenze?
Questo libro affronta il passaggio dall'intelligenza all'azione, integrando evoluzione tecnologica, organizzazione, gestione del rischio e quadro normativo.
Propone un modello di governo fondato su cinque dimensioni: Capability, Autonomy, Agency, Authority e Accountability, per definire capacità, autonomia, poteri e responsabilità degli agenti AI.
Rivolto a imprenditori, consigli di amministrazione, manager e professionisti, offre una prospettiva strategica e operativa per costruire organizzazioni nelle quali persone, dati e agenti intelligenti collaborino in modo sicuro e responsabile.
La sfida non è limitare l'autonomia dell'AI, ma imparare a governarla.

Carlo Mario Poli
Senior Advisor · AI Strategy Consultant
Co-Founder e Presidente di TOPForGrowth
carlo.m.poli@topforgrowth.it · topforgrowth.net

Referenza: Carlo Mario Poli, GOVERNARE L'AUTONOMIA DELL'AI



AI Strategic Repositioning

Dal digitale all'AI come infrastruttura

01 **L'AI diventa infrastruttura cognitiva**
Entra nel modo in cui l'impresa conosce, decide e agisce.

02 **Il vantaggio nasce dal riposizionamento**
Scegliere il ruolo dell'impresa nel nuovo sistema del valore orienta l'adozione dell'AI.

03 **Tecnologia, organizzazione e persone evolvono insieme**
Il TOPFramework collega la strategia al modello operativo e alle capacità di trasformazione.

04 **L'impresa si organizza attorno a Human–Data–Agent**
Giudizio umano, patrimonio informativo e agenti costruiscono capacità produttiva scalabile.

05 **Il successo richiede governo delle dipendenze**
Misurare il valore e governare Dependency by Success rafforzano resilienza e autonomia strategica.

La scelta di quale impresa diventare apre il tema di come governarne l'azione.

Governare l'autonomia dell'AI

Come affidare compiti agli agenti di intelligenza artificiale e mantenere il controllo dell'impresa

01 **Dall'assistenza all'azione nei processi**
Quando gli agenti operano sui sistemi aziendali, la governance deve presidiare gli effetti delle azioni.

02 **L'autonomia va commisurata al rischio**
Agency Ladder e criticità del processo definiscono il perimetro della delega e la supervisione umana.

03 **Mandato esplicito e responsabilità umana**
Il Mandato di Autonomia distingue i permessi tecnici dall'autorità delegata e chiarisce chi risponde.

04 **I controlli entrano nell'esecuzione**
L'Agentic Control Plane applica limiti e autorizzazioni e rende tracciabili le azioni degli agenti.

05 **L'autonomia cresce con prove di controllo**
Assessment, arresto, revoca e ripristino verificati consentono di estendere l'uso degli agenti.

Il riposizionamento definisce la direzione. La governance presidia l'azione autonoma.



Grazie

Carlo Mario Poli

Senior consultant specializzato in **Digital Transformation, Intelligenza Artificiale e cambiamento organizzativo**, con lunga esperienza manageriale in contesti industriali e internazionali.

Affianca imprese, associazioni e professionisti nel comprendere e applicare l'AI come leva strategica, culturale e operativa.

Co-fondatore di **TOPForGrowth**, integra visione tecnologica, competenze organizzative e attenzione allo sviluppo delle persone.

AI Companion | TOPForGrowth

Email: carlo.m.poli@topforgrowth.it

Mobile: +39 3355999 569

Web: topforgrowth.net | topframework.org