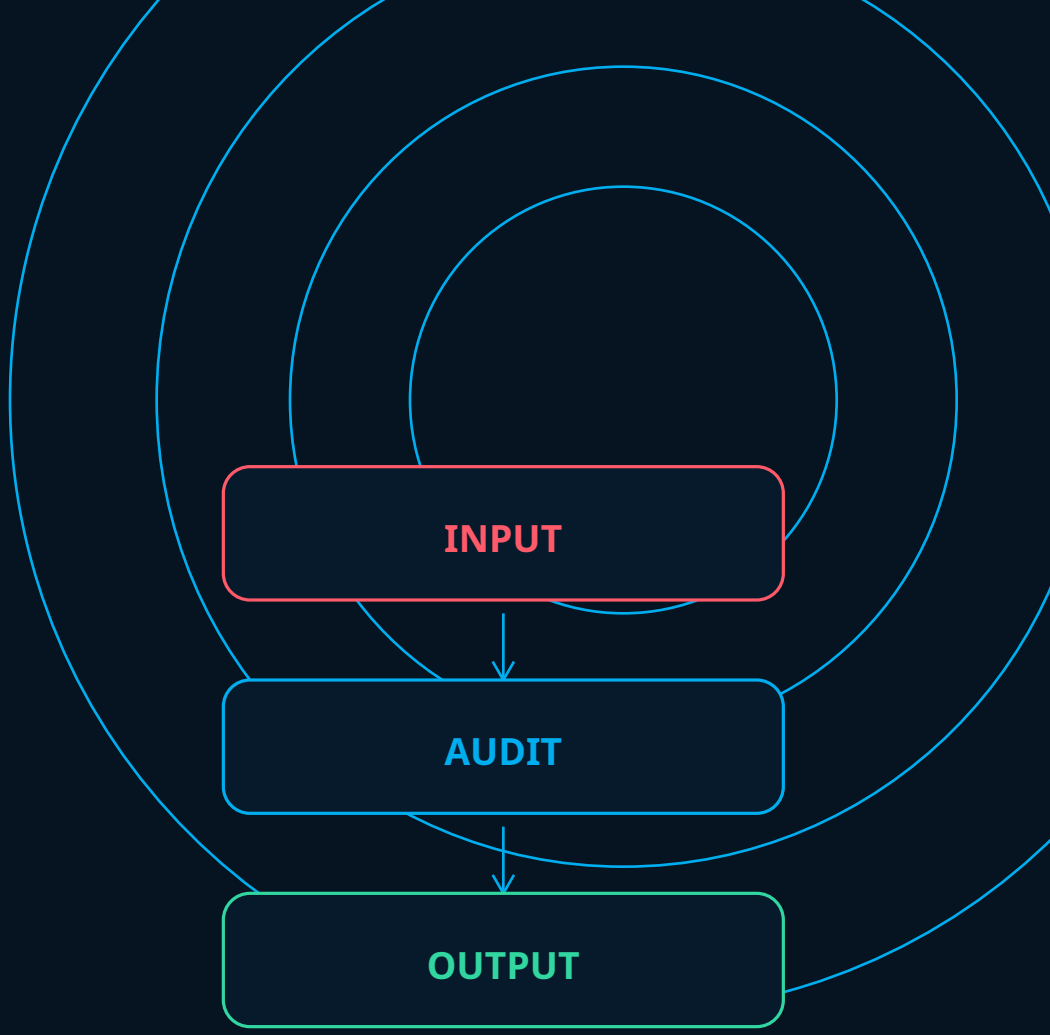
ControlPrompt **Audit**

Audit rapido per richieste AI rischiose

Controllo operativo per prompt, documenti, screenshot, landing, email e workflow prima della generazione o pubblicazione.

audit operativo | claim prudenti | privacy risk



Da input fragile a richiesta più chiara, controllabile e difendibile.

L'AI entra nei team senza controllo sufficiente.

Il risultato: richieste disordinate, output disallineati e decisioni difficili da difendere.

1 **Richieste vaghe**

Prompt scritti in modo veloce, incompleto o ambiguo.

2 **Output incoerenti**

Risultati diversi tra persone, tool e contesti d'uso.

3 **Controllo debole**

Nessun filtro chiaro su claim, dati mancanti o rischio.

Senza uno standard minimo, l'AI scala rumore prima di scalare valore.

Output incoerenti, claim fragili, controllo debole.

Quando manca un layer di controllo, i problemi non si vedono subito: si moltiplicano nel tempo.

1 **Messaggi incoerenti**

Tono, struttura e qualità cambiano da un caso all'altro.

2 **Promesse fragili**

Claim, numeri o formulazioni forti senza base sufficiente.

3 **Dati non pubblicabili**

Screenshot e documenti possono contenere dati personali o riservati.

4 **Decisioni poco difendibili**

Difficile spiegare perché un output è corretto, utile o pubblicabile.

Il problema non è solo generare. È generare in modo controllabile.

Un audit operativo prima dell'output AI.

ControlPrompt Audit trasforma una richiesta vaga o rischiosa in istruzioni più chiare, vincolate e verificabili.

Security Gate: prima se c'è rischio

Evals: dopo su casi reali

PromptOps: se cambia qualcosa

Non sostituisce il modello: migliora il modo in cui il modello viene istruito.

Da richiesta debole a istruzione controllata.

Il valore non è scrivere di più. E guidare meglio il modello.

Before

Fammi un prompt per vendere meglio il prodotto. Non conosco target, prezzo o settore.

- dati mancanti
- troppo generico
- falsa precisione

After

Crea una richiesta di vendita credibile. Se mancano dati, non inventarli: usa limiti espliciti.

- più controllato
- riutilizzabile
- più prudente

ControlPrompt non inventa precisione: riduce rischio e aumenta controllo operativo.

Riduce i punti di fragilità più comuni.

Il sistema non promette di risolvere tutto. Interviene dove il rischio operativo e più frequente.

1 **Dati mancanti**

Evita di riempire vuoti con dettagli inventati.

2 **Claim non supportati**

Riduce promesse, prove o numeri non sostenibili.

3 **Privacy risk**

Evidenzia dati sensibili, segreti o informazioni non pubblicabili.

4 **Criteri assenti**

Rende più chiaro quando un output può considerarsi sufficiente.

5 **Ambiguità**

Chiarisce pubblico, formato, vincoli, contesto e obiettivo.

6 **Falsa specificità**

Abbassa precisione apparente quando mancano dati reali.

Meglio meno specifico ma vero, che più specifico ma fragile.

Per chi usa AI in modo operativo.

Applicazioni pratiche per team e professionisti che hanno bisogno di chiarezza, coerenza e controllo.

Casi d'uso

Marketing e Sales

brief, copy, offerte, landing e messaggi più controllati

Trust e compliance

claim, linguaggio prudente e richieste sensibili

Documenti e sintesi

strutturazione, revisione e standard operativi

Workflow executive

richieste rapide per decisioni interne più chiare

Per chi è

team marketing e commerciale

controllo su contenuti e promesse

operations e knowledge team

processi ripetitivi e materiali interni

agenzie e consulenti

before/after e output cliente più difendibili

funzioni trust o governance

richieste sensibili, policy e revisione

Non è un altro tool AI: è un controllo prima della generazione.

Dal singolo caso a un processo controllato.

Tre layer leggeri aiutano a non trasformare casi reali in output rischiosi o non verificabili.

1. Prima

Security Gate
Controlla privacy, dati sensibili, credenziali, prompt injection e claim rischiosi.

2. Dopo

Evals & Regression
Trasforma casi reali in esempi riutilizzabili e criteri per non peggiorare.

3. Quando cambia

PromptOps Log
Registra modifiche importanti, limiti noti e stato reale del materiale.

Test interni non sono benchmark. I casi reali non sono validazione di mercato.

Si parte piccolo, si valida, si estende solo se utile.

Un percorso semplice per introdurre controllo operativo nelle richieste AI del team.

1 ControlPrompt Audit

mini-analisi iniziale
mappa rischi ricorrenti
versione migliorata
before/after prudente

2 Workflow Pilot

1 caso d'uso prioritario
workflow controllato
criteri di successo
demo before/after

3 Materiali per il team

standard di richiesta
linee guida interne
materiali operativi
adozione progressiva

Obiettivo: passare da uso occasionale dell'AI a richieste più coerenti e difendibili.

Prenota un AI Request Audit iniziale.

Partiamo da un caso reale e valutiamo dove il controllo può migliorare chiarezza, coerenza e rischio.

1 Invia un caso

prompt, documento, screenshot, landing o workflow

→

2 Analizziamo

ambiguità, dati mancanti, claim e rischi

→

3 Restituiamo

diagnosi, versione migliorata e limiti residui

Parti da un caso reale. I materiali sensibili vengono trattati in forma prudente e anonimizzata.

Apri il form Tally

https://tally.so/r/0Q1xVP