Auditorium
Internal Audit & Governance Knowledge Center

Associazione Italiana
Internal Auditors



SPERIMENTAZIONE SUL CAMPO DI UN AGENTE AI IN UN AUDIT REALE

Paolo Patruno
Head of I.A. Function and 231 Model Supervisory Board Member di BH Italia - Berkshire Hathaway Group

Il primo articolo ha descritto la costruzione del Synthetic Prompt: le istruzioni generate dall'AI a partire dal meta-prompt dell'Auditor e dalle fonti autorizzate, sottoposte a verifica e approvazione prima dell'utilizzo. Questo secondo contributo ne esamina la sperimentazione su un incarico reale, attraverso il confronto con il percorso ordinario di Audit.

La sperimentazione binaria

Il metodo è stato testato sul campo durante un Audit, facendo correre lo stesso incarico su due binari paralleli:

- da una parte, l'esecuzione tradizionale, svolta secondo la metodologia ordinaria della Funzione Internal Audit
- dall'altra, un'esecuzione AI-augmented, guidata dal Prompt Sintetico.

Le condizioni di partenza erano identiche: stesso perimetro, stesso programma di lavoro, stesse popolazioni da analizzare, stessi criteri di campionamento e medesime evidenze operative.

L'obiettivo di questa prima fase era valutare la qualità e l'affidabilità del percorso supportato dal Synthetic Prompt, sia durante il processo di Audit sia sul risultato finale. Il confronto non assumeva in partenza la superiorità di uno dei due approcci: doveva verificare se l'esecuzione AI-augmented mantenesse il rigore metodologico del percorso standard e dove potessero emergere errori, omissioni, estensioni non supportate, incoerenze o attività da rifare.

Per questo sono stati inseriti punti di controllo lungo tutto il processo: dalla definizione del perimetro e delle richieste documentali all'analisi delle evidenze, dall'esecuzione dei test alla predisposizione delle carte di lavoro, fino all'identificazione delle eccezioni, alla valutazione dei potenziali Audit issue, alla formulazione delle azioni di mitigazione e all'allineamento del reporting finale.

La valutazione ha riguardato qualità, completezza, coerenza, affidabilità e tracciabilità degli output, considerando anche il lavoro necessario alla review.

La qualità dei deliverable finali è stata considerata insieme alla tenuta del percorso che li aveva prodotti: un risultato formalmente ordinato non sarebbe stato sufficiente se ottenuto attraverso passaggi non supportati dalle evidenze o incoerenti con il programma di lavoro.

Nella fase iniziale, il parallel run ha comportato più lavoro, non meno. Questo maggiore sforzo ha consentito di osservare il modello lungo l'incarico e di confrontare i due percorsi senza assumere la rapidità di produzione degli output come misura della loro qualità. Il lavoro necessario per la review resta parte della valutazione complessiva della sperimentazione.

I risultati della sperimentazione

L'Agente ha offerto il contributo più significativo nell'organizzazione delle evidenze, anche quando ricevute in modo frammentato dai risk/action owner, tra solleciti e chiarimenti successivi. Ha mantenuto una tracciabilità puntuale tra programma di Audit, evidenze acquisite, carte di lavoro, rilievi e report, rendendo ricostruibile il collegamento tra procedure, riscontri e conclusioni.

L'impegno professionale si è concentrato, come previsto, nella configurazione e nell'affinamento della RAG a supporto dell'incarico e nella revisione del meta-prompt e del Synthetic Prompt, prima dell'approvazione e dell'avvio operativo. Durante l'esecuzione, l'Auditor ha verificato la correttezza delle analisi dell'Agente riesaminando un sottoinsieme del campione già selezionato per l'Audit, con una sensibile riduzione del lavoro di controllo.

I controlli svolti non hanno evidenziato errori macroscopici. Il reporting ha richiesto un intervento redazionale per contenere ripetizioni e ridondanze e rendere la comunicazione più asciutta ed executive, preservando chiarezza, concretezza e completezza delle risultanze.

Questa prima fase ha privilegiato qualità e affidabilità degli output. La stima prudenziale del risparmio è di quasi un terzo dei man-days abitualmente necessari per gestire un engagement end-to-end. La valutazione resta preliminare: il proseguimento della sperimentazione introdurrà KPI quantitativi per misurare il tempo effettivamente liberato lungo l'intero ciclo dell'incarico.

Limiti, governance e possibile scalabilità

La sperimentazione descritta è un Proof of Concept. I risultati ottenuti richiedono ulteriori verifiche prima di poter essere estesi ad Audit, organizzazioni e contesti differenti.

Le performance dipendono dalla qualità e completezza del corpus documentale, dalla configurazione della RAG, dalla selezione degli input, dalla disciplina di utilizzo, dalla stabilità del modello e dalla complessità dell'engagement.

Un impiego più ampio richiede un perimetro di governo preciso: dati trattabili, profili di accesso, interazioni da registrare e tempi di conservazione. Devono inoltre essere disciplinati sicurezza, proprietà intellettuale, versionamento, gestione degli incidenti e competenze degli utilizzatori, con responsabilità chiaramente attribuite.

L'auto-generazione del Prompt Sintetico presenta rischi specifici: istruzioni circolari, requisiti omessi, gerarchie delle fonti errate e un'apparente completezza dovuta al solo livello di dettaglio. Occorre quindi verificare copertura, coerenza e correttezza delle istruzioni. La separazione tra generazione, validazione ed esecuzione resta il controllo centrale; nel Proof of Concept, il confronto con il percorso ordinario costituisce un ulteriore presidio per individuare divergenze, omissioni e risultati non supportati.

Tra le possibili evoluzioni rientrano la connessione tramite API ai database aziendali, per acquisire i dati necessari alle verifiche, e collegamenti dedicati ai risk/action owner. Attraverso questi ultimi, i responsabili potrebbero ricevere direttamente le richieste dell'Agente e caricare documenti, risposte e chiarimenti, mantenendo l'associazione con le richieste originarie e con le procedure del programma di Audit. Queste integrazioni andrebbero progettate entro il perimetro autorizzativo e di tracciabilità dell'incarico.

Un ulteriore sviluppo sarebbe affiancare all'Agente esecutore un **Supervisor AI Agent**, operativo in parallelo e con un mandato critico e antitetico rispetto al percorso guidato dal Synthetic Prompt. La revisione riguarderebbe la struttura del meta-prompt, il Synthetic Prompt generato, le attività svolte durante l'engagement e gli output finali. Il contraddittorio dovrebbe mettere alla prova le ipotesi adottate, ricercare elementi contrari e segnalare omissioni, deviazioni dal programma di lavoro o conclusioni non sostenute dalle evidenze. L'Auditor valuterebbe gli esiti del riesame, mantenendo la responsabilità delle decisioni professionali.

Il framework deve rimanere tool-agnostic, preservando la natura metodologica del Prompt Sintetico e l'indipendenza da uno specifico fornitore o piattaforma. La sua adozione strutturata, comprese le eventuali integrazioni e funzioni di supervisione, andrebbe formalizzata nella metodologia di Internal Audit e ricondotta al processo aziendale di approvazione, registrazione, monitoraggio e riesame degli AI use case.

La valutazione richiederebbe il coinvolgimento, oltre alla Funzione Internal Audit, delle competenze Legal, Compliance, Data Protection e Information Security. L'inquadramento del caso d'uso, le condizioni di accesso ai sistemi e le salvaguardie applicabili dovrebbero essere definiti prima di procedere all'estensione operativa del modello.

