L’AI A SUPPORTO DELLA SICUREZZA AZIENDALE

Soluzioni Operative per la Gestione del Rischio e il Rafforzamento della Governance

Convegno AI e Cyber Risk

Maggio 2026

REPLY

AGENDA

- AI GOVERNANCE
- FOCUS SULLA CYBERSECURITY

AI GOVERNANCE

Rischi AI emergenti

CONTESTO NORMATIVO E RESPONSABILITÀ

Un nuovo profilo di rischio

EU AI Act

Feb 2025
Utilizzi Proibiti dell'AI

Ago 2025
Regole per modelli AI di uso generale (GPAI)

Ago 2026 (Dic 2027 / Ago 2028 se Digital Omnibus)
Obblighi completi per sistemi ad alto rischio

AI Lifecycle

Rischi AI

L'AI introduce rischi diversi da quelli tradizionali: emergono durante l'utilizzo reale, non solo prima del rilascio.
Occorre quindi controllo continuo e un modello di responsabilità condiviso tra fornitore e utilizzatore.

Conformità

Diritti fondamentali

Oltre ai classici temi di Data Governance e CyberSecurity occorre valutare l'impatto sui diritti fondamentali dell'uomo.
Per i casi ad alto rischio sono richieste misure specifiche (FRIA, monitoring, logging e supervisione umana).

AI Observability

Trasparenza

Nuove aree di monitoraggio e verifica continua per garantire Fairness, Trasparenza, Spiegabilità e Accountatbility:

- Errori decisionali difficili da prevedere.
- Output non controllabili e di difficile spiegazione.

CyberSecurity

Aumento attacchi

Nuova superficie di attacco:

- Manipolazione del comportamento dei modelli.
- Alterazione dei dati di addestramento e input.

Uso dell'AI per condurre attacchi sofisticati e produrre deepfake.

FRAMEWORK DI AI GOVERNANCE

Tre livelli integrati che costituiscono un **percorso di conformità AI**

01
Governance
- Policy e regole aziendali
- Ruoli e responsabilità definiti
- AI Committee dedicato
- Inventory sistemi AI

02
Gestione del Rischio
- Classificazione per AI Act
- Valutazione impatti sul business
- Valutazione di conformità e prioritizzazione interventi risk-based

03
Gestione della Sicurezza
- Controlli tecnici mirati
- Test e monitoraggio continuo
- Gestione operativa del rischio

1
Ruoli e Responsabilità AI
Definire RACI e ownership

2
Framework documentale AI
Politiche e procedure

3
Livello di Governance
Comitato e supervisione

4
Livello di Gestione del Rischio
Valutare e classificare

Principio cardine
I tre livelli si integrano con i framework esistenti di Risk Management e Cybersecurity — nessun silo AI isolato.

La governance AI non è un progetto — è un processo continuo. I tre livelli devono lavorare insieme nel tempo.

RUOLI E RESPONSABILITÀ AI

Una chiara attribuzione di responsabilità e poteri decisionali previene colli di bottiglia e rischi di non conformità

Strategico

Comitato AI

Supervisione a livello di Consiglio, approvazione delle policy, autorità di escalation

Operativo

Responsible AI Officer

Responsabile della governance operativa quotidiana, coordinamento interfunzionale

Tecnico

Responsible AI Champions

Focalizzato su Compliance, rischio AI e cybersicurezza per l'applicazione dei principi di conformità e sicurezza by design, supervisione del threat modeling

- Responsabili di business
- Responsabilità sui casi d'uso e valutazione dell'impatto
- IT & DevOps
- Integrazione di sistema e controlli di rilascio
- Data & AI Office
- Ciclo di vita del modello e qualità dei dati
- Cybersicurezza
- Controlli di rischio e attività di AI red teaming
- Compliance, DPO e Ufficio legale
- Mappatura regolamentare e supervisione FRIA
- **Matrice RACI esplicita**
- Meccanismi formali di escalation a ogni livello

FOCUS SULLA CYBERSECURITY

Le strategie di difesa

EVOLUZIONE DEL RISCHIO AI

Modelli sempre più potenti e con meccanismi di reasoning, evoluzione agentica

- Rischi comportamentali e decisionali
  - Non valutabili solo ex-ante: emergono durante l'operatività reale dei sistemi
- Amplificazione del rischio da autonomia agenti
  - Agentic AI introduce rischi sistemici non lineari e difficili da contenere
- Gap tra intended purpose e comportamento reale
  - I sistemi generativi e agentici divergono dall'intento dichiarato in modi non prevedibili
- Incidenti non riconoscibili come attacchi classici
  - Si manifestano come decisioni non difendibili o violazioni di accountability

Implicazione strategica

Servono modelli di valutazione basati su **comportamento effettivo** e impatto osservato, non solo sull'intento dichiarato.

CYBERSECURITY E AI GOVERNANCE

Compliance e security by design

Nuove Superfici di Attacco

- Prompt Injection
- Manipolazione diretta del comportamento AI
- Data Poisoning
- Corruzione dei dati di training e fine-tuning
- AI Supply Chain Compromise
- Modelli e componenti di terze parti non verificati
- Incidenti senza exploit classici
- Output dannosi senza violazione tecnica rilevabile

Evoluzione Necessaria

- Governance comportamentale
- Dal perimetro infrastrutturale al governo delle capacità operative AI
- Sicurezza by design nel ciclo di vita AI
- Integrazione strutturale, non aggiunta a posteriori
- AI Red Teaming e runtime monitoring
- Testing attivo e monitoraggio continuo come pratiche standard

Shift strategico

Da **difesa perimetrale** a governance comportamentale dell'AI

STRATEGIA DI DIFESA DEL CISO E NEXT STEPS

Un piano di azioni concrete

Fase 1

AI Asset Inventory

Censimento completo e dinamico di sistemi AI, modelli e dataset in produzione e sviluppo fin dalla fase di Idea/Concept

Fase 2

Autonomy Governance

Classificazione e limiti operativi per use case AI complessi e soprattutto per agenti AI, rivalutazione continua

Fase 3

Zero Trust esteso all'AI

Principi Zero Trust applicati a modelli, dati e pipeline AI per ridurre rischi di manipolazione e accessi non autorizzati

Fase 4

Incident Preparedness

Tassonomie AI-specifiche, playbook, telemetria dedicata, esercitazioni per rispondere efficacemente a incidenti AI complessi

Fase 5

Allineamento a Framework

Standardizzare su NIST AI RMF e ISO/IEC 42001, integrazione con risk management esistente

Come prepararsi

AI Governance **continua e adattiva**

Team di esperti e **formazione continua**

Strumenti a supporto dell'AI Governance

Agenti AI a supporto di compliance e security

AI GOVERNANCE TOOLS

Tools di mercato e Agente AI sviluppato da Reply come acceleratore

Valutazioni manuali

- Basate su Excel, Forms, Teams ed email
- Avvio rapido
- Evidenze frammentate
- Scalabilità e controllo limitati

Strumenti personalizzati

- Su portali esistenti o piattaforme low-code
- Allineati ai processi interni
- Più controllo e accountability
- Richiedono ownership e manutenzione

Strumenti di mercato

- Selezione software più lunga
- Soluzioni leader: IBM, OneTrust, ServiceNow
- Compliance più strutturata
- Reporting robusto e integrazione elevata

Le esigenze

Processo di AI Governance

- Evitare duplicazioni informative tra team
- Triage rapido di idee e iniziative
- Stimare valore, impatto e compliance
- Aggiornare le valutazioni lungo l'evoluzione del caso d'uso
- Ridurre tempi di analisi e produrre evidenze verificabili

La soluzione

AI Governance Accelerator Agent

- Precompila questionari e raccoglie evidenze disponibili
- Individua priorità e fattori di rischio chiave
- Genera una valutazione precompilata su documenti e codice
- Trasferisce output nello strumento di governance
- Supporta reporting, accountability e remediation

THANK YOU

Laura Bertalero – Spike Advisory Reply

Email: l.bertalero@reply.it

Mob: +39-346-2411525