



# Dati, Conoscenza e Modelli Cognitivi per la Sicurezza Bancaria

---

Dal contrasto alla criminalità predatoria  
alla gestione integrata del rischio

10.12.2025

Stati Generali della Sicurezza - Palazzo Altieri - Roma

**Dott. Phd Amir Topalovic**  
**AISMA**





## IL CONTESTO CHE CAMBIA:

Le minacce sempre più ibride: fisiche, digitali, organizzative, comportamentali.

La complessità **non deriva solo dagli attacchi, ma dalla frammentazione della conoscenza** tra SOC, fraud, IT, risk, compliance, HR ...

In questo scenario diventa necessario un: **sistema cognitivo multi-dipartimentale dell'organizzazione**

- assorbire dati e know-how da tutte le piattaforme aziendali
- unificare contesto fisico + digitale + rischio + compliance
- preservare la conoscenza operativa
- potenziare sicurezza e risk management
- supportare ogni livello decisionale





# Contrastare le complessità richiede un'**architettura cognitiva**, non una somma di tecnologie

Bisogna abilitare l'organizzazione a:

- **Comprendere** ciò che accade nella dimensione fisica, digitale, procedurale e normativa.
- **Correlare** eventi, anomalie, pattern e comportamenti.
- **Decidere rapidamente** su basi coerenti e verificabili.
- **Standardizzare il reasoning operativo.**

---

Questa capacità si chiama **soglia cognitiva d'impresa**: la banca non usa l'AI, diventa un sistema intelligente essa stessa





# QUESTIONE DI METODO:

## 1. Costruzione dei dati

Ingestion controllato, pulizia, deduplica, tagging semantico, riduzione del debito informativo. AISMA assorbiamo e strutturiamo ciò che l'organizzazione già possiede.

---

## 2. Modellazione cognitiva

Costruzione dell'**ontologia** dell'impresa:

- minacce fisiche e digitali,
- procedure, ruoli, responsabilità, normative di riferimento,
- asset, eventi, eccezioni,
- KRI e indicatori di rischio.

La **mappa mentale ufficiale dell'organizzazione, unica e condivisa.**

---

## 3. Reasoning verificabile

Pipeline deterministiche con retrieval controllato, validazione formale, explainability, human-in-the-loop.

Solo dopo questa architettura si introducono automazioni affidabili, integrate nei processi.



# Aree di impatto nella sicurezza fisica, logica e nel risk management

## Sicurezza fisica

- logiche di automazione tra eventi simili e tra filiali;
- identificazione pattern predatori;
- recupero informazioni accelerate.

## Sicurezza logica

- correlazione alert IT + comportamenti + procedure;
- procedure di riduzione dei falsi positivi;
- mappatura e aggiornamento delle minacce.

## Risk Management

- KPI cross-domain (fisico + digitale + umano);
- KRI più accurati e predittivi;
- reportistica avanzata;
- compliance e audit





# Governance & AI Act Compliance

## Una pipeline di esecuzione completa:

- explainability
- audit trail
- versionamento
- tracciabilità decisionale
- controlli formali
- risk scoring
- rilevamento anomalie
- enforcement delle policy

La pipeline è progettata per essere **AI Act Tier-3 compliant.**





## USE CASE: Sistema di Intelligence Cognitiva

**Crystal Box** – soluzione di **architettura cognitiva ad alta criticità** progettata per supportare le operazioni ricorsive di polizia giudiziaria.

*Sistema on-premise, auditabile, zero-trust.*

### Funzionalità:

- apprendimento e ricostruzione storica di grandi volumi di dati e documenti;
- correlazione tra eventi fisici, digitali e pattern comportamentali;
- network & timeline analysis;
- anomaly detection;
- predictive Intelligence;
- supporto all'automatizzazione delle procedure secondo c.p.p.;
- reasoning chain certificata.



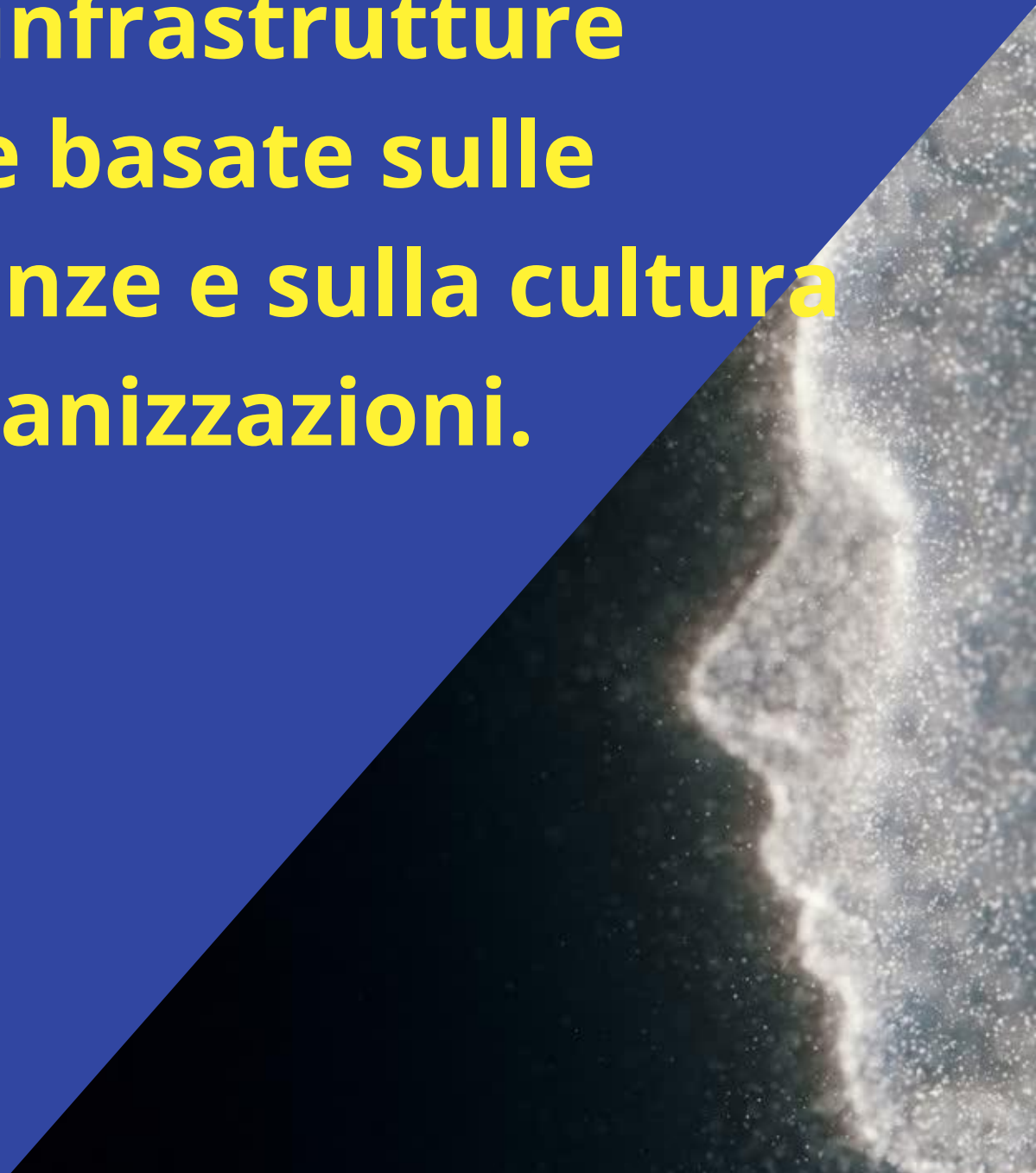
# CONCLUSIONI

Per contrastare la criminalità predatoria e governare il rischio serve:

- trasformare la banca in **un'impresa cognitiva**, non in un utilizzatore di AI;
- adottare un **linguaggio unico per sicurezza e rischio** (ONTOLOGIA di dominio);
- integrare la dimensione fisica, digitale e comportamentale in un solo modello;
- validare casi ad alta criticità.

AISMA non fornisce strumenti:

**realizza infrastrutture cognitive basate sulle competenze e sulla cultura delle organizzazioni.**





# GRAZIE

---

**AISMA Srl**

*centro di ricerca & trasferimento tecnologico*

[www.aisma.it](http://www.aisma.it)

**Dott. Phd Amir Topalovic**

CEO

mail: [amir.topalovic@aisma.it](mailto:amir.topalovic@aisma.it)