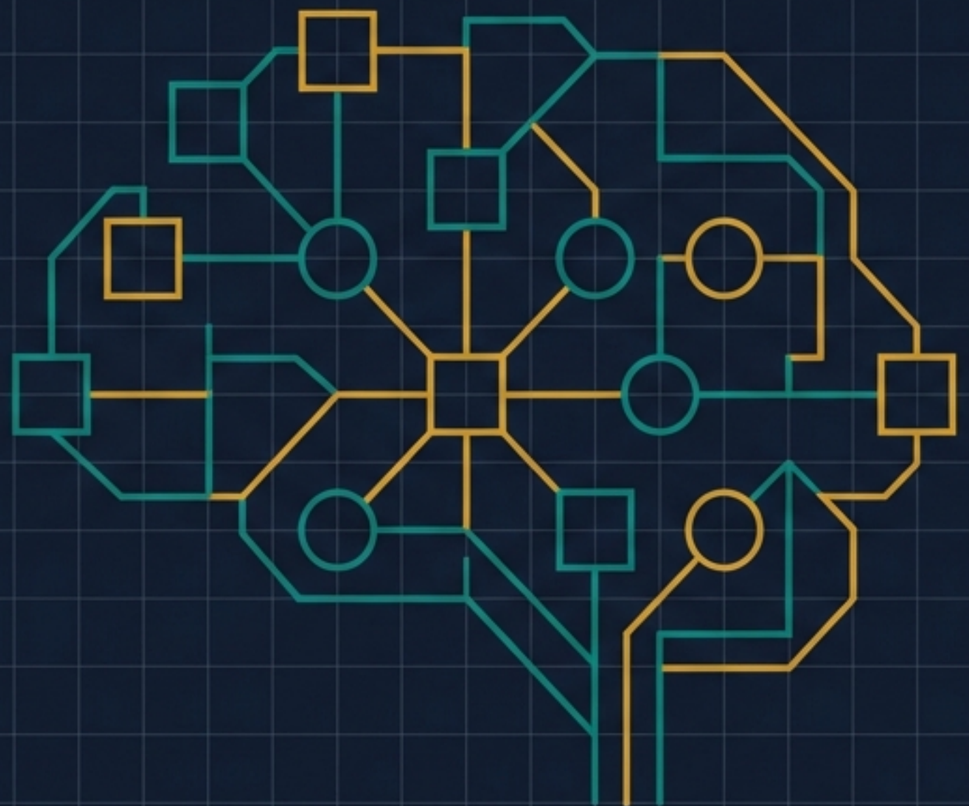


FAIR: L’Anatomia del Rischio Cyber

Masterclass sull’analisi quantitativa, l’ontologia del rischio e la modellazione finanziaria

Per CISO, Risk Manager e IT Auditor

Il Cambio di Paradigma: Da Qualitativo a Quantitativo

	Approccio Qualitativo (Tradizionale)	Approccio Quantitativo (FAIR)
Unità di Misura	Scale ordinali (Alto/Medio/Basso)	Valori monetari (€) e frequenze temporali
Precisione	Illusoria (numeri arbitrari come 1-5)	Probabilistica (intervalli di confidenza BetaPERT)
Output Principale	Mappe di calore (Heat Maps) soggettive	Curve di eccedenza delle perdite (LEC)
Comunicazione	Ambigua (rischio rosso)	Finanziaria (10% di probabilità di perdere >1M€)

Key Insight: Il modello FAIR trasforma le vulnerabilità tecniche in probabilità di perdita monetaria, consentendo decisioni basate su dati difendibili e un calcolo reale del RosI (Return on Security Investment).

L'Ontologia FAIR: Scomporre il Rischio

Rischio = Probabile Frequenza x Probabile Entità

(di una perdita futura)

Loss Event Frequency (LEF):
Quante volte la minaccia causerà un danno in un anno.

Loss Magnitude (LM):
L'impatto finanziario totale per ogni singolo evento.

Nota: La tassonomia standard (Open FAIR) impedisce la confusione tra minacce, vulnerabilità e impatto, fornendo un modello logico rigoroso.

L’Asse della Frequenza: Loss Event Frequency (LEF)

Loss Event Frequency (LEF)

Threat Event Frequency (TEF) [X] **Vulnerability (Vuln)**

La frequenza dei tentativi. Deriva da:

- **Contact Frequency:** Frequenza di contatto tra minaccia e asset (Casuale, Regolare, Intenzionale).
- **Probability of Action:** Probabilità che la minaccia agisca (basata su valore, sforzo e rischio percepito).

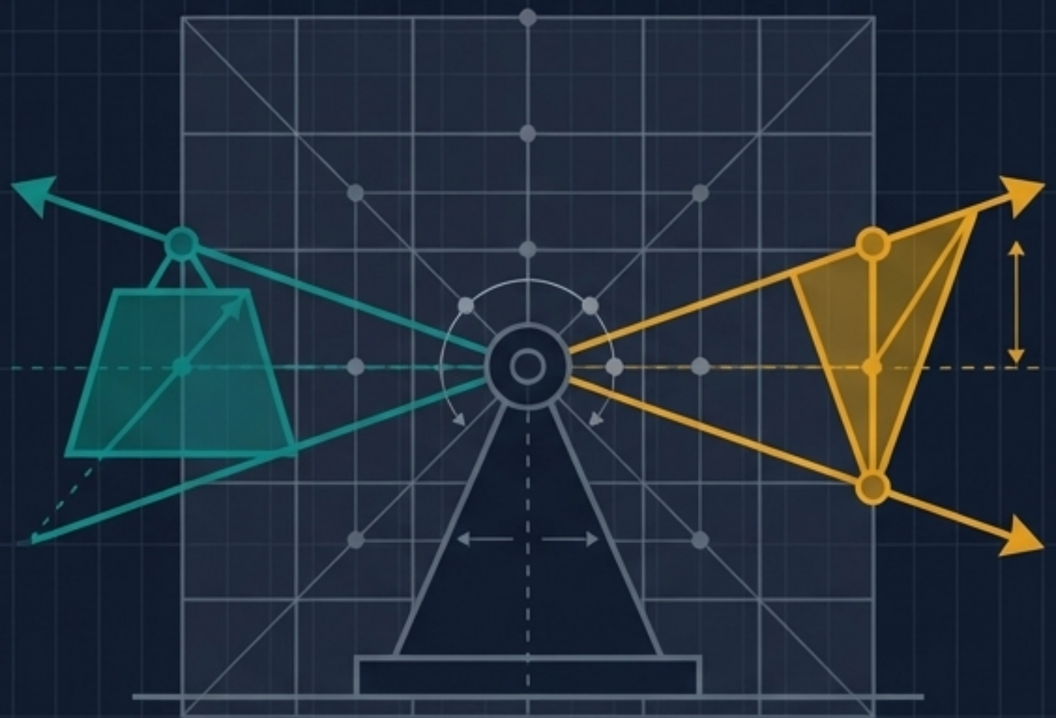
- La probabilità che il tentativo abbia successo e si trasformi in una perdita.

Key Takeaway: Un evento di minaccia (es. invio di phishing) diventa un evento di perdita (es. ransomware eseguito) SOLO se l’asset è vulnerabile.

Dinamiche della Vulnerabilità: Forza vs. Resistenza

Forza della Minaccia

- **Threat Capability (TCap):** Competenze, risorse e tempo dell'attaccante (es. APT vs Script Kiddie). Misurato su un Continuum a percentili.

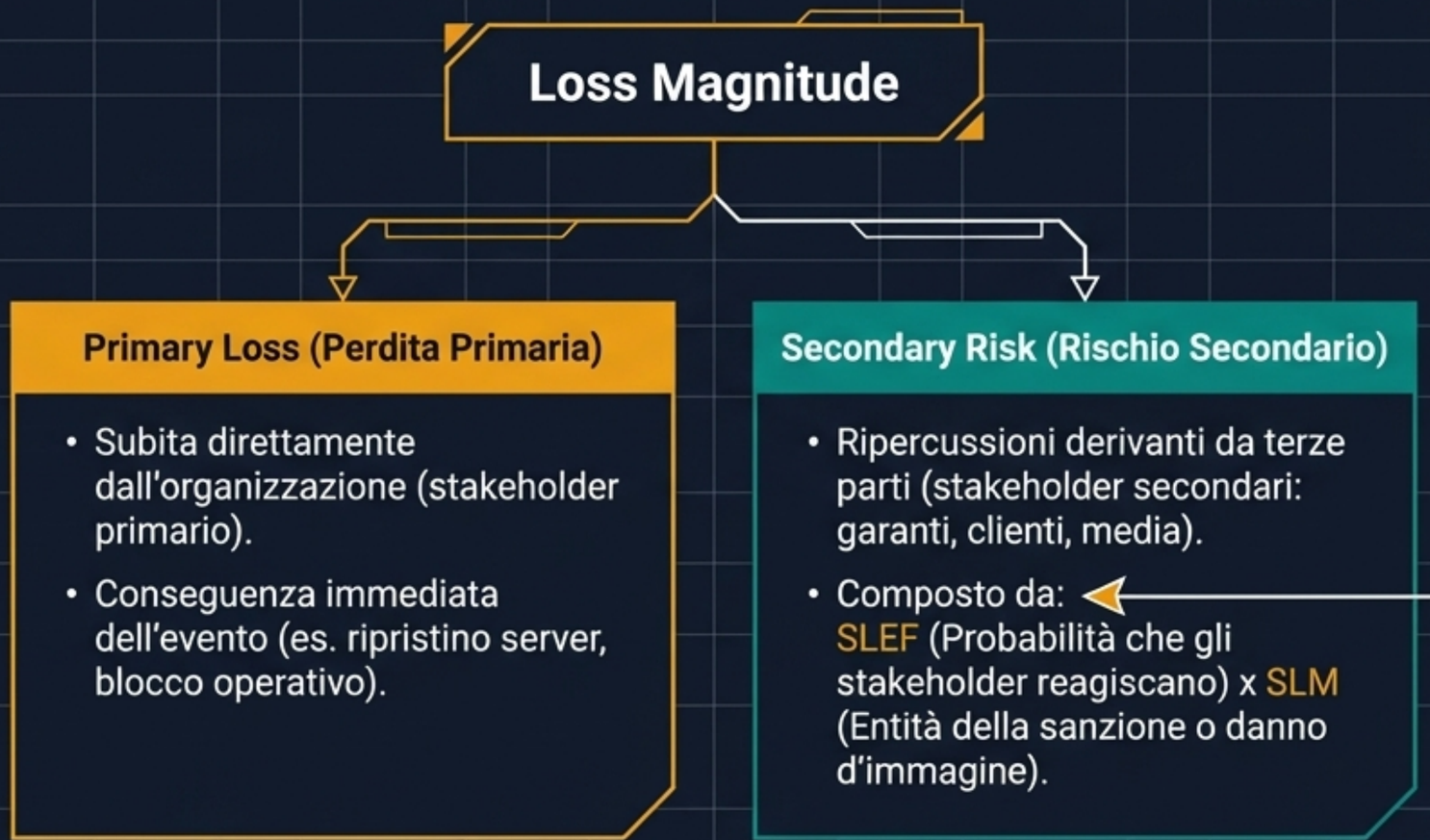


Resistenza dei Controlli

- **Control Strength (CS):** Il livello di difficoltà imposto dai controlli resistivi (es. crittografia, MFA).

In FAIR, la vulnerabilità **NON** è un difetto del software. È una percentuale probabilistica (es. 10%) che la forza applicata dalla minaccia superi la resistenza dei controlli implementati.

L'Asse dell'Impatto: Loss Magnitude (LM)



La Tassonomia delle Perdite: Le 6 Forme Economiche

Produttività (Primary)

Tempo e output persi per interruzione.

Risposta (Primary)

Costi di indagine, contenimento ed esperti forensi.

Sostituzione (Primary)

Sostituzione di asset fisici o logici (es. server danneggiati).

Sanzioni e Giudizi (Secondary)

Multe normative (GDPR), cause legali.

Vantaggio Competitivo (Secondary)

Furto di proprietà intellettuale (IP).

Reputazione (Secondary)

Erosione del brand, perdita di clienti e fiducia a lungo termine.

Ognuna di queste categorie viene quantificata finanziariamente per alimentare il motore di simulazione.

Gestire l’Incertezza: La Stima BetaPERT

Il Problema

I dati empirici perfetti non esistono nella cybersecurity.

La Soluzione

Stime calibrate basate sul giudizio di esperti, trasformate in distribuzioni statistiche.

[O] Ottimistico (Min)
Il valore minimo plausibile.

[M] Più Probabile
Il valore atteso (ha un peso maggiore: 4x).

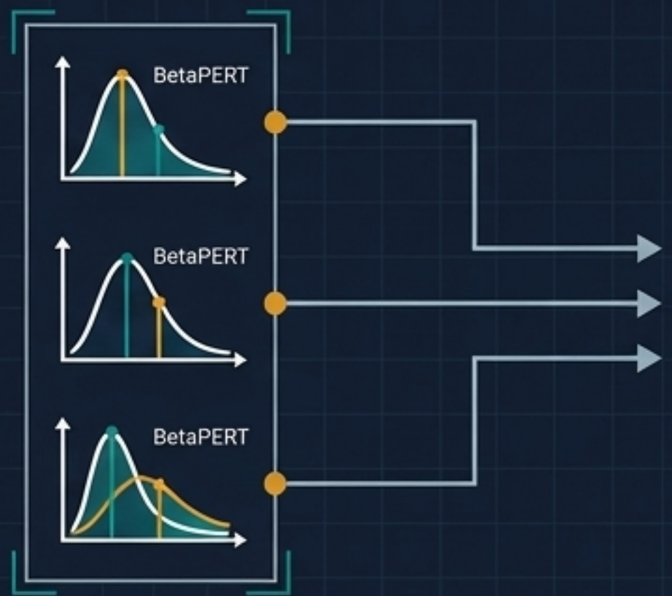
[P] Pessimistico (Max)
Il peggior scenario plausibile.

$$E = (O + 4M + P) / 6$$

Questo approccio cattura la variabilità e riduce l'incertezza senza richiedere una precisione impossibile.

Il Motore di Calcolo: Simulazione Monte Carlo

1. Input: Inserimento delle stime a 3 punti (Frequenza e Impatto).

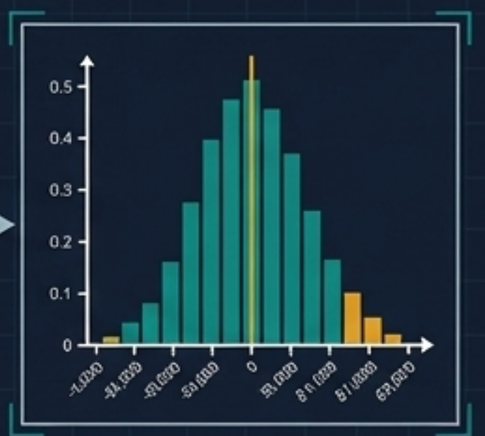


2. Simulazione: Motore Monte Carlo (10,000+ Iterazioni)

Il sistema esegue migliaia di scenari ipotetici, estraendo casualmente valori dalle distribuzioni fornite.

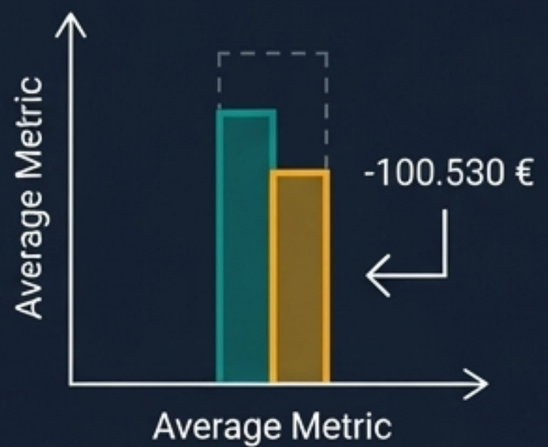
3. Aggregazione: I risultati vengono combinati matematicamente.

4. Output: Generazione di un quadro completo delle probabilità di perdita, evidenziando la media e gli scenari estremi.



Interpretazione degli Output: ALE e LEC

Annualized Loss Expectancy (ALE)

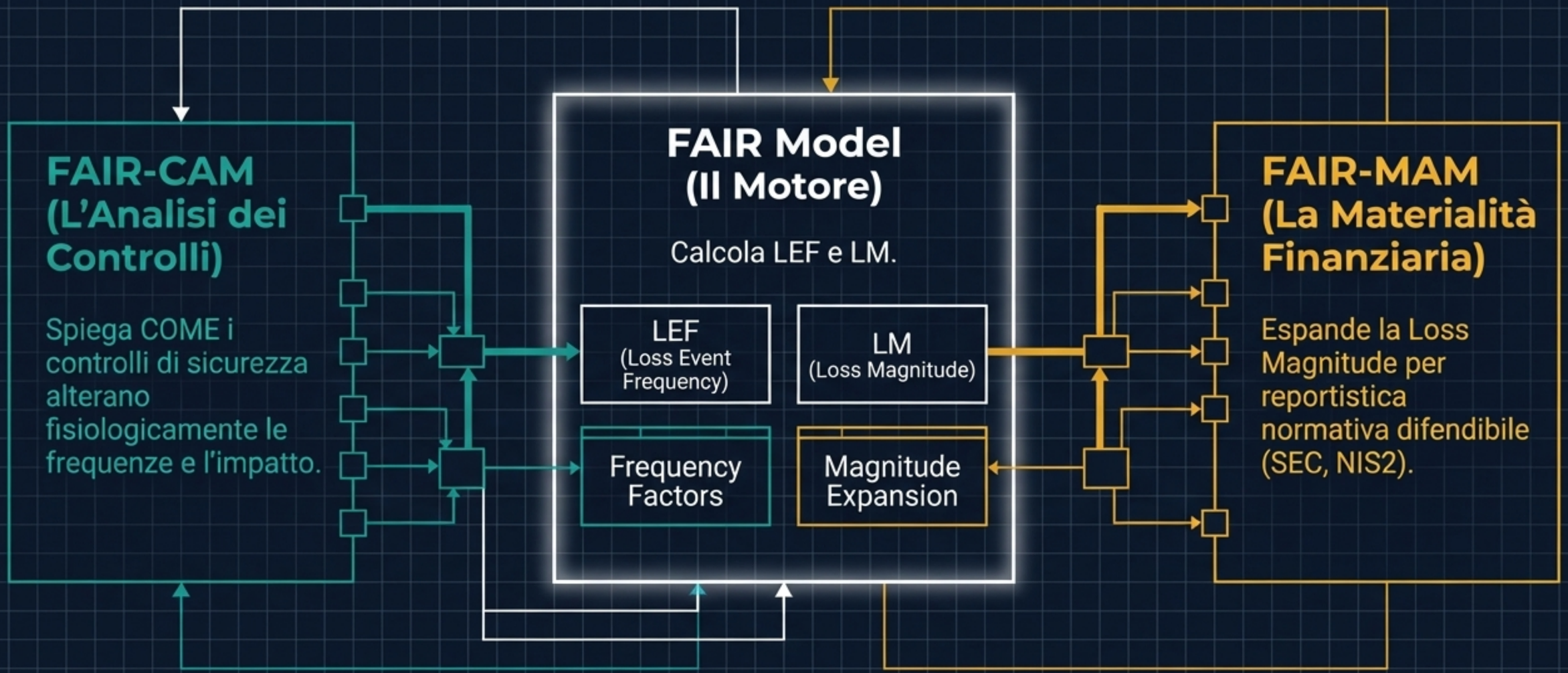


- Rappresenta il costo medio annuo atteso per uno scenario.
- **Uso Strategico**: Utile per il budgeting e il calcolo del RoSI, ma non cattura gli eventi catastrofici rari.

Loss Exceedance Curve (LEC)

- Mostra la probabilità che le perdite superino una determinata soglia finanziaria.
- **Uso Strategico**: Fondamentale per confrontare l'esposizione al rischio con l'appetito al rischio aziendale (es. 'C'è il 5% di probabilità di perdere più di 10M€').

L’Ecosistema FAIR Integrato



FAIR-CAM: Analitica Fisiologica dei Controlli

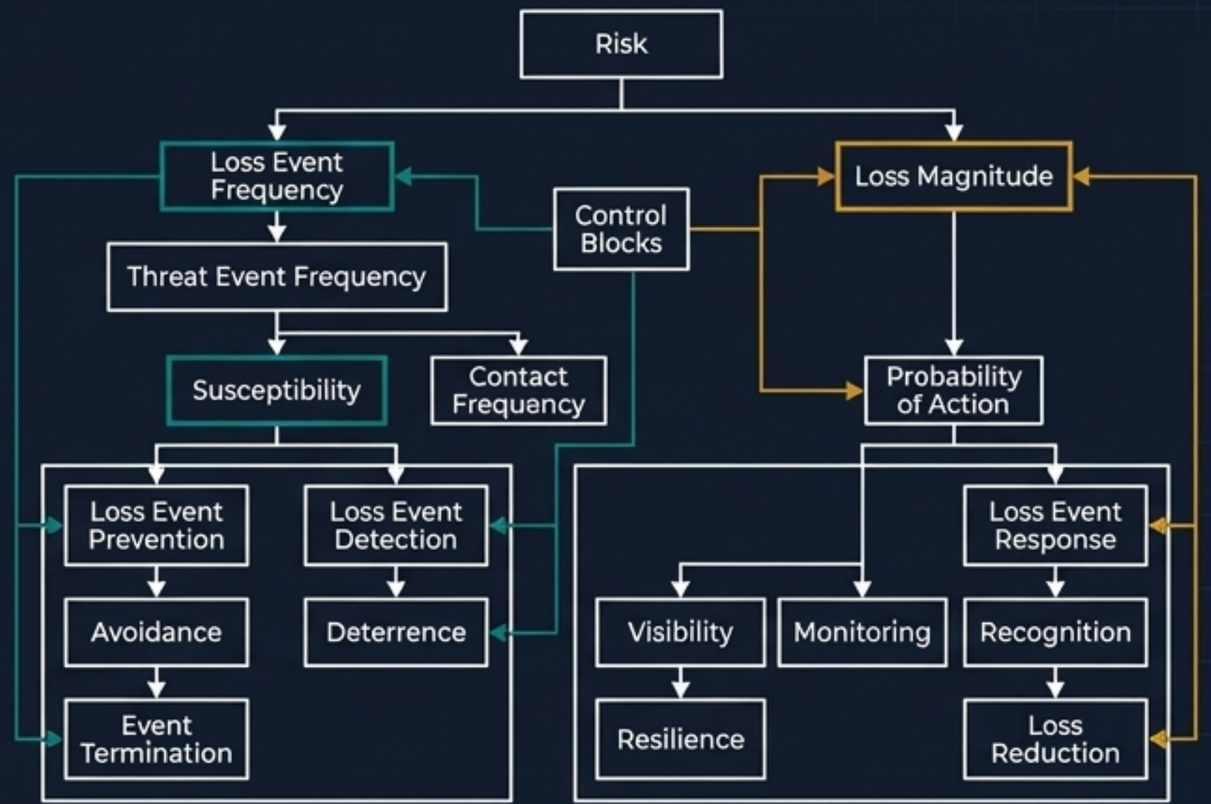
I framework tradizionali descrivono COSA sono i controlli (anatomia).
FAIR-CAM misura COME funzionano (fisiologia).

Le 3 Categorie di Controlli

Loss Event Controls
Agiscono direttamente su Frequenza o Impatto (Prevenzione, Deterrenza, Risposta).
Es. Un WAF riduce la Susceptibility.

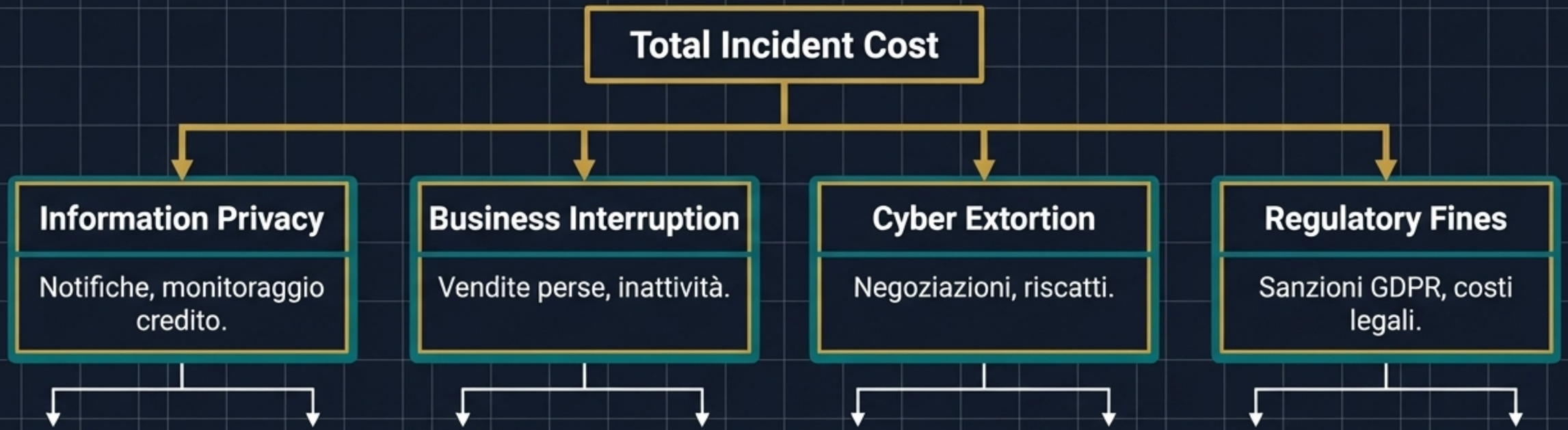
Variance Management Controls
Garantiscono l'affidabilità nel tempo dei controlli primari. Es. Patch management.

Decision Support Controls
Forniscono dati per gestire il rischio.
Es. Threat intelligence, Asset management.



FAIR-MAM: Valutazione della Materialità (Compliance SEC & NIS2)

Espande il ramo destro dell'ontologia (Loss Magnitude) in una tassonomia ultra-dettagliata di 10 moduli e **26 sottoctategorie** per **difendere le stime** di fronte a garanti e investitori.



Valore: Permette alle aziende di determinare rapidamente (es. in 4 giorni per la SEC) se un incidente ha superato la soglia legale di 'materialità".

L’Implementazione: Le 4 Fasi dell’Analisi FAIR

Conclusione: Il Valore Strategico dell'Approccio FAIR

Trasparenza Glass-Box

Abbandona i punteggi opachi. Le assunzioni sono visibili, testabili e matematicamente difendibili.

Allineamento al Business

Traduce bit e byte nella lingua universale del consiglio di amministrazione: l'esposizione finanziaria.

Ottimizzazione del RoSI

Permette di smettere di gestire il rischio basandosi sulla paura, giustificando gli investimenti in modo economicamente efficiente.

Non si può gestire in modo efficace ciò che non si può misurare oggettivamente.