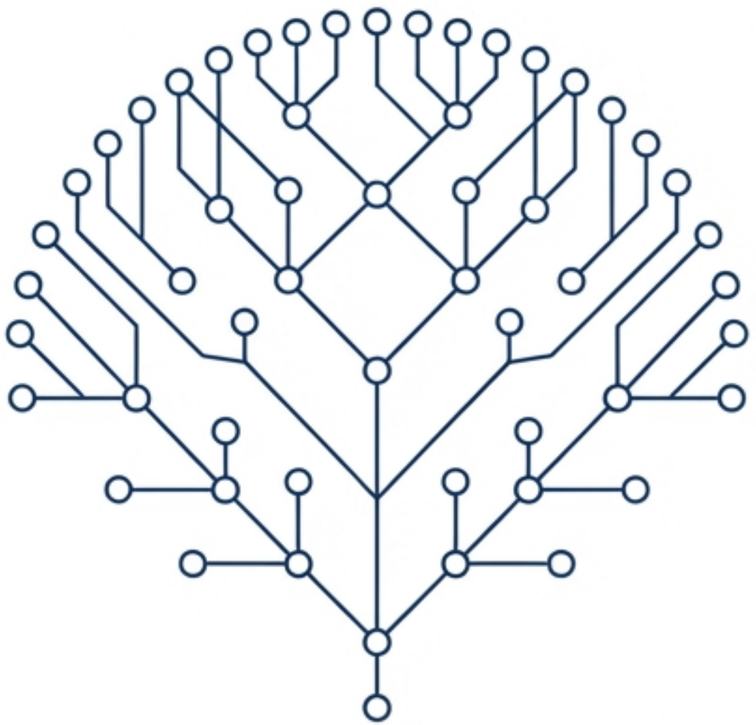
Analisi Quantitativa del Rischio Cyber: Il Metodo FAIR



Metodologia, Ontologia e Applicazione nel Cyber Risk Assessment

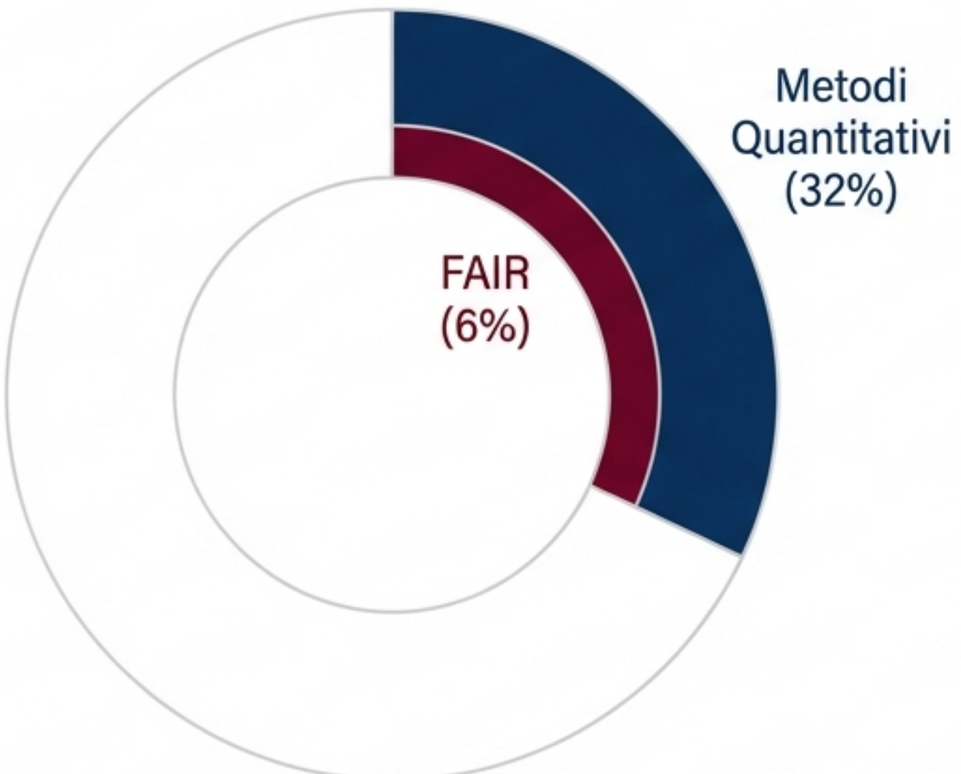
MODULO 8 - CYBER RISK ASSESSMENT QUANTITATIVO

Il Contesto di Mercato e l'Adozione dei Metodi Quantitativi

Dati di Mercato (Rapporto Clusit 2023): Il 32% delle organizzazioni adotta metodi quantitativi per la stima del rischio cyber. All'interno di questo segmento, il metodo FAIR (Factor Analysis of Information Risk) detiene una quota dichiarata del 6%.

Analisi: La stima del 6% è verosimilmente al ribasso. L'uso diffuso di categorie generiche (es. NIST SP 800-30 o norme ISO) spesso nasconde implementazioni FAIR non esplicitate.

Cenni Storici: Proposto nel 2015 da Jack Freund e Jack Jones. Il metodo precede temporalmente HTMA, pur condividendo la struttura fondamentale in quattro fasi.



Panoramica del Processo di Valutazione FAIR

01

Definizione dello Scenario

Identificazione e decomposizione obbligatoria del rischio in sottoscenari specifici.

02

Stima dei Fattori (PERT)

Valutazione dei fattori dell'ontologia FAIR utilizzando la stima a tre valori (Min, Likely, Max).

03

Simulazione Monte Carlo

Generazione degli scenari probabilistici attraverso iterazioni multiple (1.000 - 10.000).

04

Interpretazione Risultati

Analisi degli output statistici (percentili, curve di eccedenza) per il supporto decisionale.

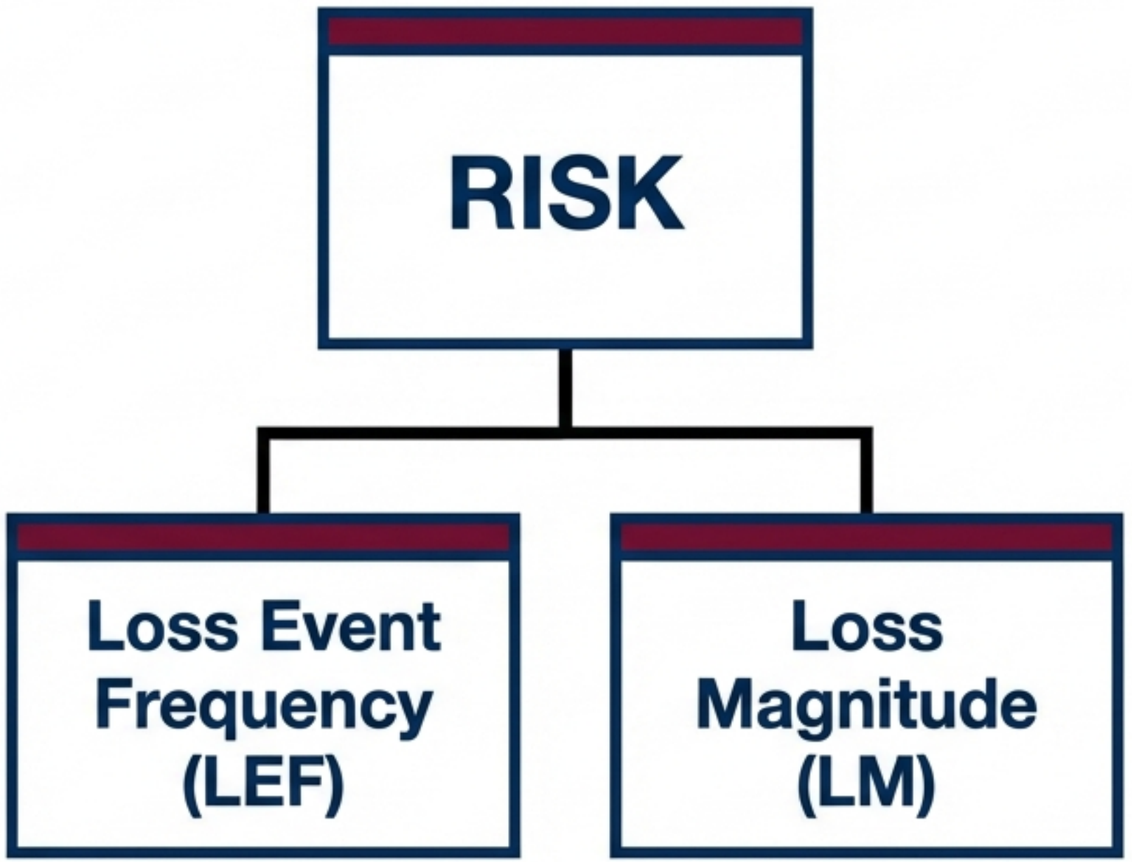
Step 1: Definizione e Decomposizione dello Scenario

Il primo passo richiede l'individuazione della situazione specifica che espone l'organizzazione al rischio. La decomposizione è mandatoria.

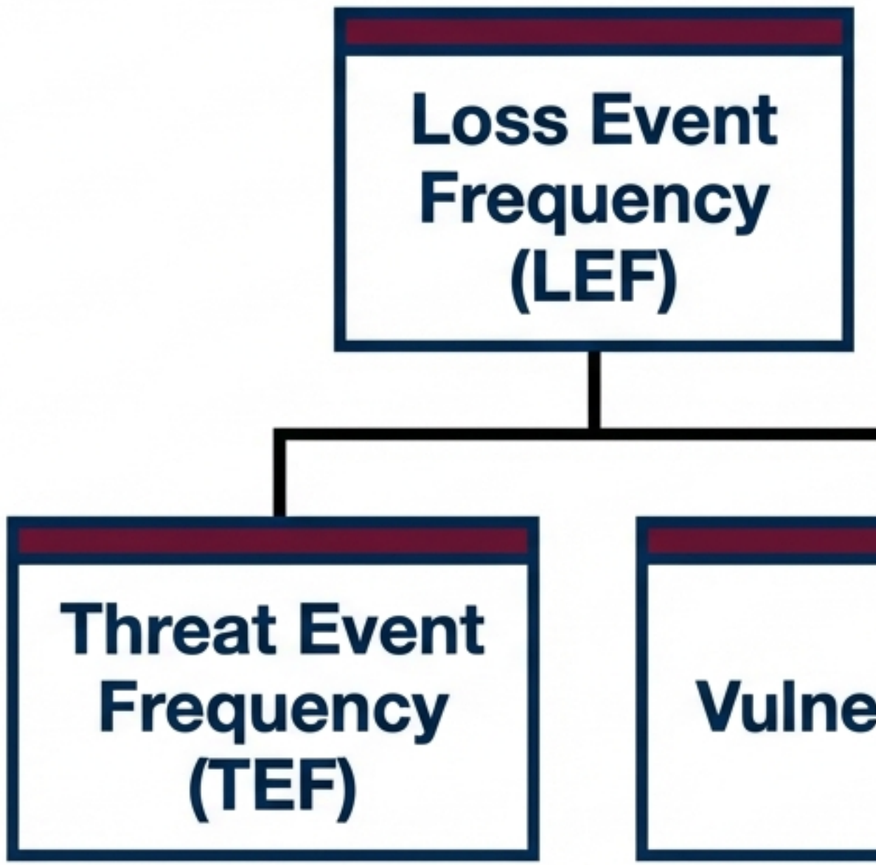
L’Ontologia del Rischio: Struttura e Definizioni

Definizione: In informatica, un’ontologia è una rappresentazione formale, condivisa ed esplicita di un dominio. Nel metodo FAIR, il Rischio è la radice di un albero gerarchico che standardizza il linguaggio.

Distinzione Critica:
Frequenza ≠ Probabilità
La frequenza indica *quante volte* si prevede che un evento accada in un intervallo di tempo (es. 2 ransomware/anno). Non è una probabilità espressa tra 0 e 1.



Analisi della Frequenza (Loss Event Frequency) Lato Sinistro dell'Ontologia

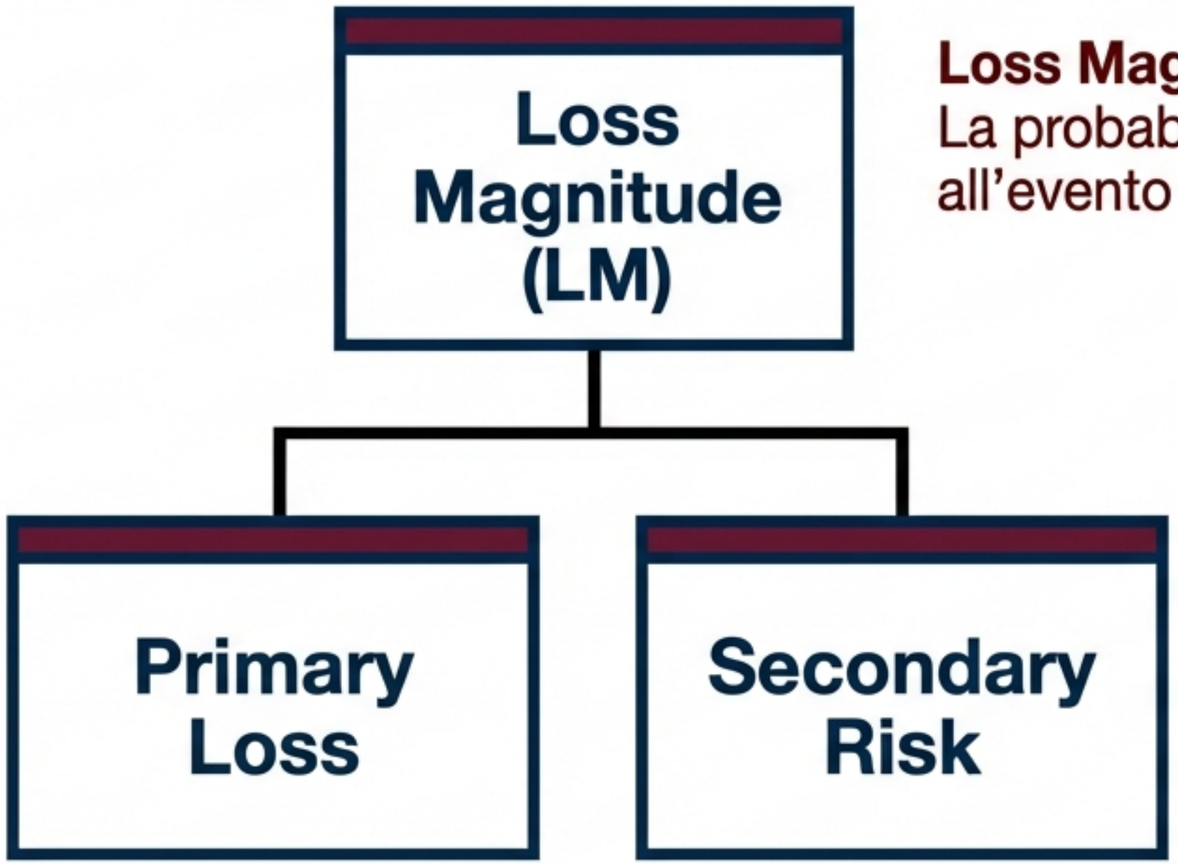


Threat Event Frequency (TEF)
La frequenza con cui gli agenti di minaccia *tentano* di attaccare l'organizzazione.
Nota: il tentativo è distinto dal successo.

Vulnerability
La probabilità che un determinato attacco abbia successo. Rappresenta la suscettibilità del sistema rispetto alla minaccia specifica.

Nota Operativa:
Si consiglia la stima diretta del LEF quando possibile; in alternativa, si decompone nei fattori TEF e Vulnerability.

Analisi dell’Impatto: Primary Loss e Secondary Risk Lato Destro dell’Ontologia



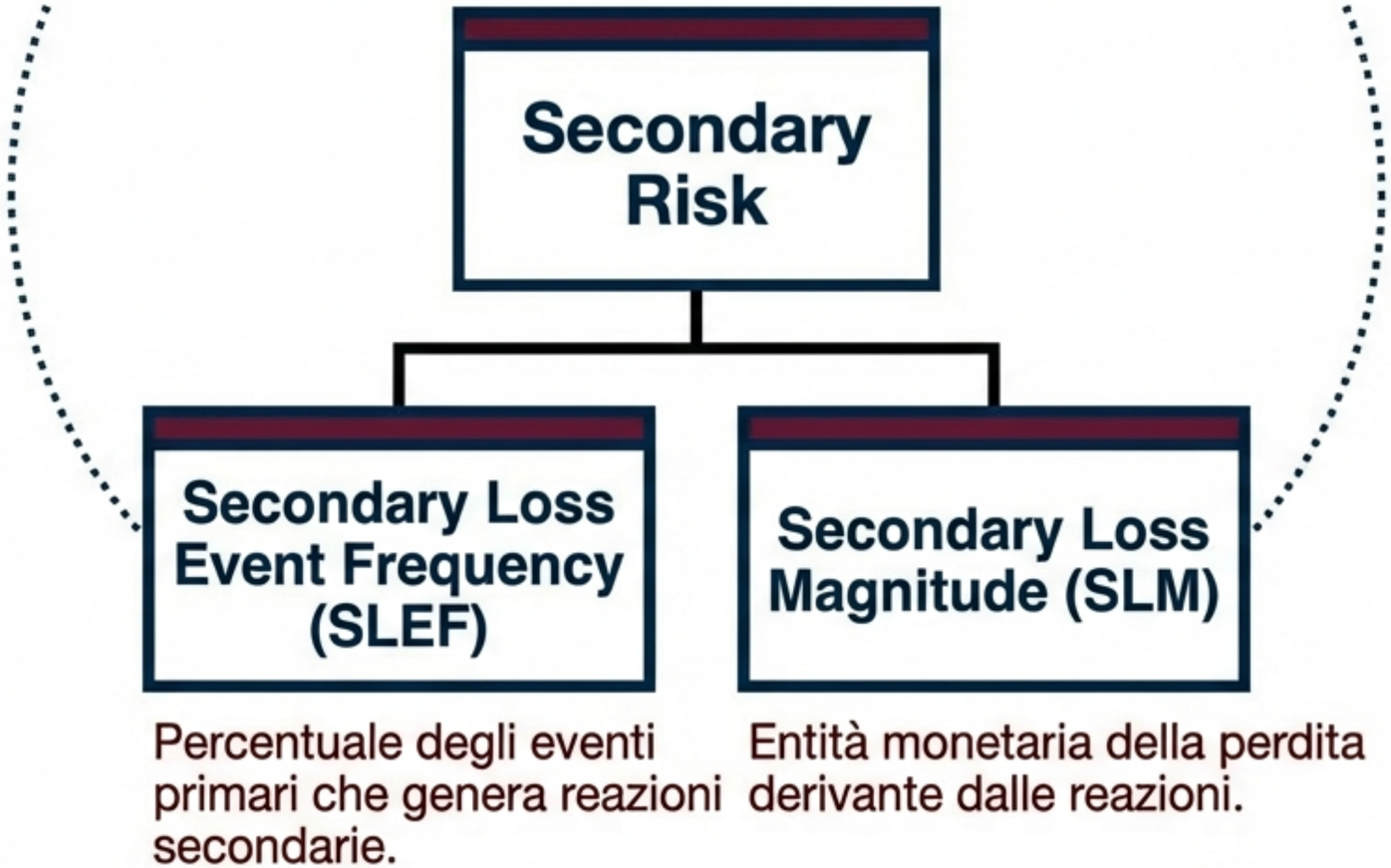
Loss Magnitude
La probabile entità della perdita monetaria associata all’evento considerato.

Primary Loss
La perdita monetaria che l’organizzazione subisce come conseguenza *diretta* dell’evento (es. interruzione operativa).

Secondary Risk
L’esposizione economica dovuta alla reazione degli **stakeholder secondari** all’evento primario. Non è una semplice somma, ma un nuovo fattore di rischio derivato.

La Ricorsività del Rischio Secondario

Il Rischio Secondario è trattato come un'equazione di rischio nidificata.
Gli stakeholder (clienti, regolatori, media) agiscono come nuovi agenti di minaccia in risposta all'incidente iniziale.



Le 6 Forme di Perdita nel Modello FAIR

Perdite Primarie (Tipiche)

- **Productivity:** Riduzione della capacità operativa (es. mancata produzione, stipendi a vuoto).

- **Response:** Costi di gestione incidente (investigazione, forensics).

- **Replacement:** Costi per rimpiazzare risorse fisiche o personale.

Perdite Secondarie (Tipiche)

- **Competitive Advantage:** Perdita di proprietà intellettuale o informazioni di mercato.

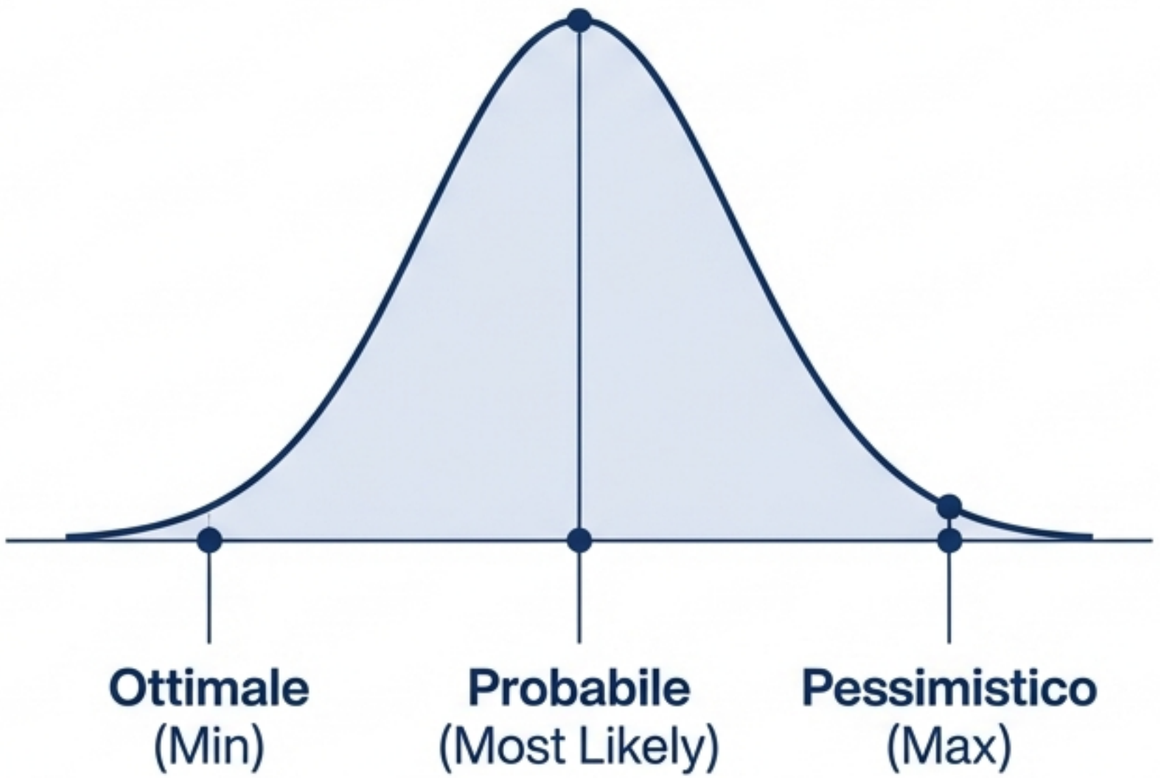
- **Fines & Judgments:** Sanzioni legali, multe, costi di cause giudiziarie.

- **Reputation:** Riduzione quota di mercato, calo azionario, churn clienti, costo del capitale.

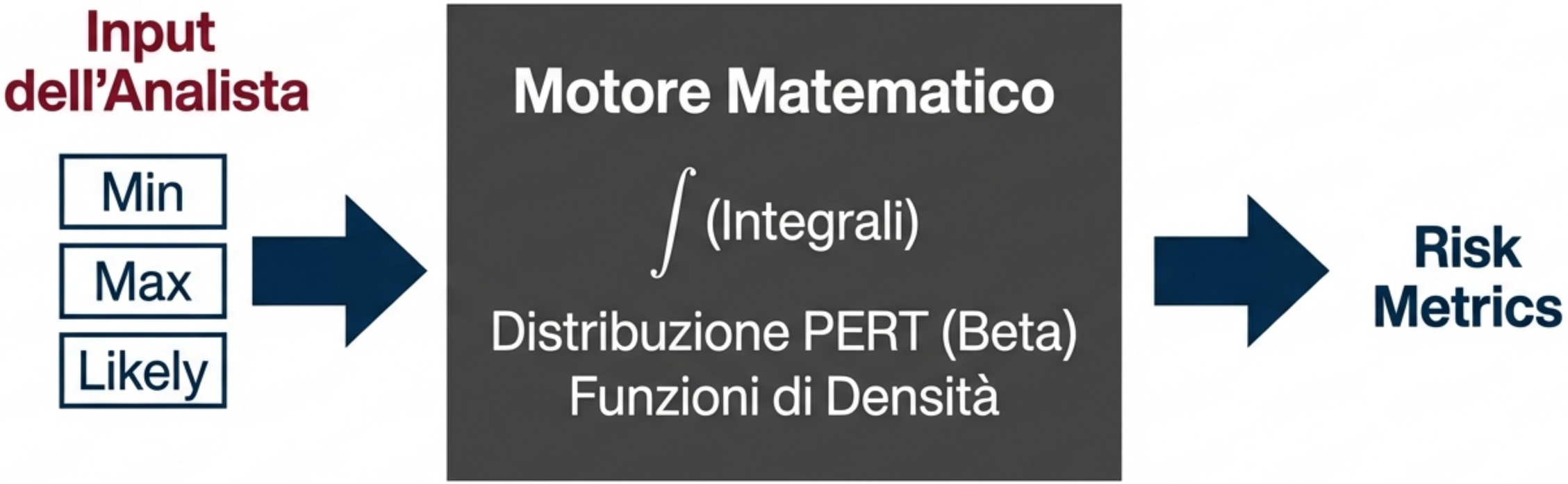
Step 2: Stima dei Fattori tramite Tecnica PERT

Program Evaluation and Review Technique (PERT)

Rispetto a una stima ‘single point’, PERT gestisce l’incertezza richiedendo tre valori per ogni fattore. FAIR richiede un volume di input elevato: fino a 6 forme di perdita devono essere stimate, oltre ai fattori di frequenza.



Il Motore Matematico: Distribuzioni e Complessità



Sebbene la matematica sia nascosta all'utente ('Black Box'), il calcolo è computazionalmente oneroso, utilizzando integrali complessi al posto di semplici somme aritmetiche.

Step 3: La Simulazione Monte Carlo

Un algoritmo iterativo che esegue il calcolo del rischio migliaia di volte (1.000 – 10.000 iterazioni) utilizzando 5 variabili aleatorie per scenario.

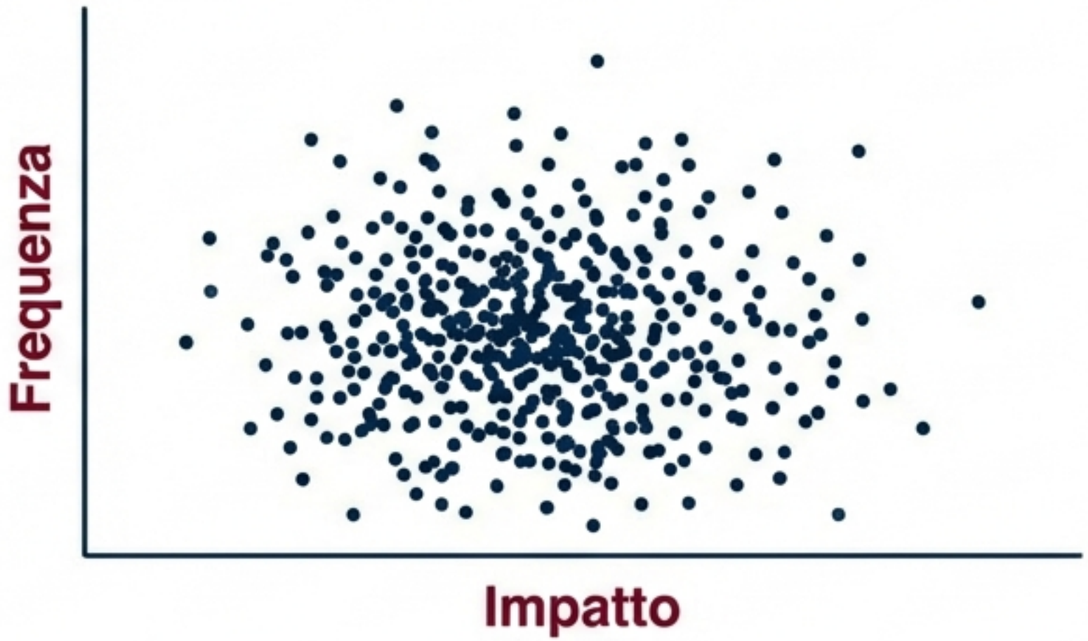
$$\text{Perdita Totale} = (\text{Freq}_{\text{Prim}} \times \text{Impatto}_{\text{Prim}}) + (\text{Freq}_{\text{Sec}} \times \text{Impatto}_{\text{Sec}})$$

Input Variabili:

1. Frequenza Perdita Primaria
2. Impatto Perdita Primaria
3. Frequenza Perdita Secondaria
4. Impatto Perdita Secondaria
5. (Variabili derivate PERT)

Step 4: Interpretazione degli Output

Scatter Plot: Confronto Frequenza vs. Impatto per ogni iterazione.



Loss Exceedance Curve: Probabilità di eccedere una certa soglia di perdita.

Key Metrics					
Min	Mean	Most Likely	Max	10th Percentile (Best Case)	90th Percentile (Worst Case)

Conclusioni: Complessità e Granularità

Complessità

FAIR è significativamente più granulare e complesso di metodi come HTMA. Richiede stime approfondite (fino a 6 forme di perdita) e la gestione di decomposizioni ricorsive.

Valore dell'Ontologia

L'ontologia offre uno standard rigoroso e difendibile per definire i termini del rischio, eliminando l'ambiguità soggettiva tipica delle analisi qualitative.

Applicabilità

Ideale per organizzazioni con maturità elevata (Esperti Calibrati) che necessitano di metriche finanziarie dettagliate per giustificare investimenti di sicurezza.