



METODOLOGIA OCTAVE® ALLEGRO

Un Framework Architetture per la Valutazione
del Rischio focalizzata sulle Informazioni

Vincenzo Calabrò

L'Evoluzione della Valutazione del Rischio

Approcci Tradizionali

- Formato “Essay” (narrativo e discorsivo)
- Flessibile ma incline a incoerenze
- Richiede elevato impiego di risorse
- Ambito degli asset generico

Il Modello Allegro

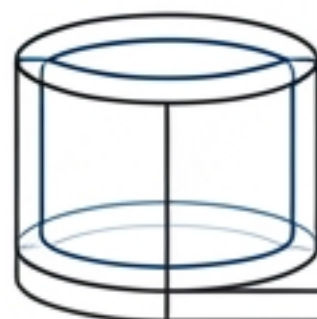
- Formato “Fill-in-the-blank” (strutturato e oggettivo)
- Ottimizza facilità d'uso, adozione e ripetibilità
- Riduce drasticamente l'impegno di risorse e i requisiti di formazione
- Ambito rigorosamente focalizzato sugli asset “informativi”

OCTAVE Allegro definisce un metodo strutturato in **8 fasi** per valutare i rischi concentrandosi esclusivamente sul **valore** e sui **container** delle informazioni.

L'Equazione Architetturale del Rischio

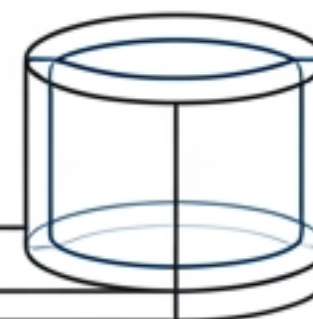
Condizione: Minaccia

— Cosa potrebbe minacciare la resilienza operativa dell'organizzazione.



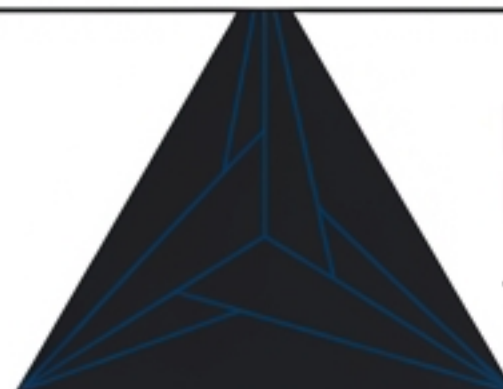
Conseguenza: Impatto

— Come il rischio realizzato impatterà l'organizzazione.



Fattore di Incertezza: Probabilità

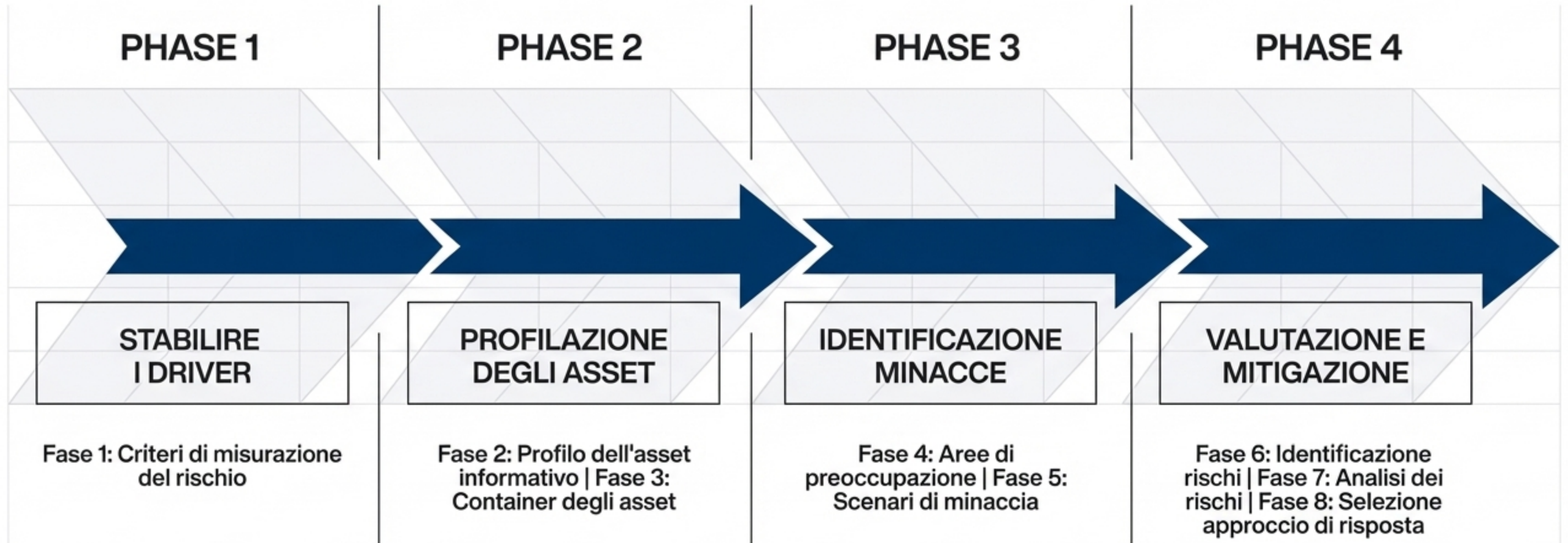
— La verosimiglianza che la minaccia si materializzi.



Rischio

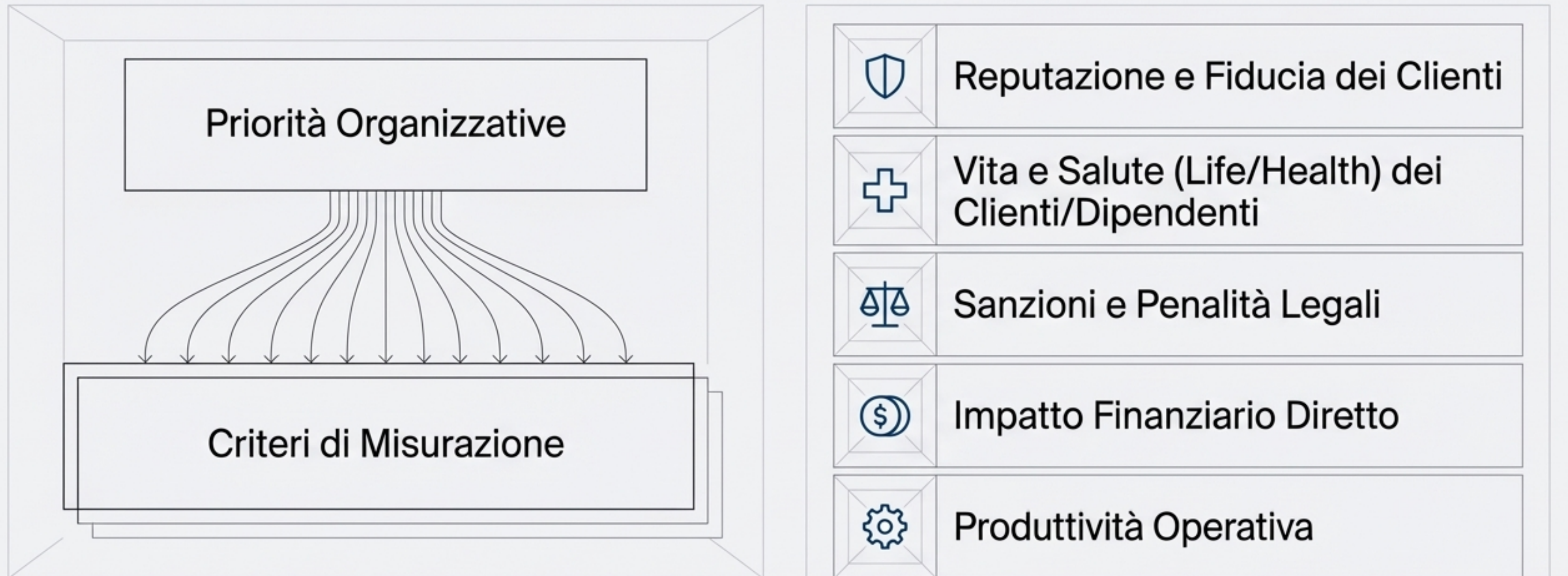
[MINACCIA / CONDIZIONE] + [IMPATTO / CONSEGUENZA] = RISCHIO OPERATIVO

Il Processo Strutturato a 8 Fasi



Fase 1: Stabilire i Driver e i Criteri

La valutazione deve basarsi su driver organizzativi oggettivi, non su percezioni tecniche.



Gerarchia degli Oggetti di Rischio (Fasi 2-3)

SERVIZI.

(Attività limitate che l'organizzazione esegue per fornire un prodotto/servizio, per uso interno o esterno).

PROCESSI DI BUSINESS.

(I flussi operativi che supportano i servizi).

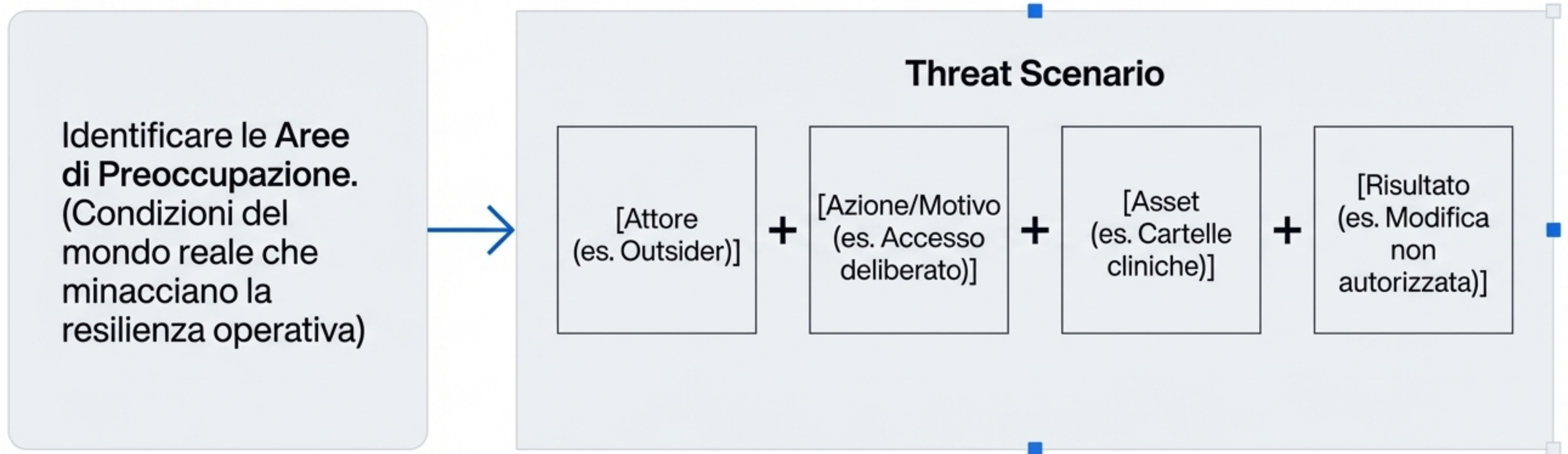
ASSET INFORMATIVI.

(I dati e le informazioni critiche generate o utilizzate dai processi).

ASSET CONTAINERS.

(Il focus tecnico: Dove risiedono le informazioni? Chi vi ha accesso? Quali sistemi le elaborano?).

Dall'Area di Preoccupazione allo Scenario di Minaccia (Fasi 4-5)



Se non è possibile sviluppare una dichiarazione di impatto, l'area di preoccupazione potrebbe non essere plausibile.

Matrice Diagnostica: Risultati e Requisiti di Sicurezza

		CIA Triad		
Threat Outcomes		Riservatezza (Confidentiality)	Integrità (Integrity)	Disponibilità (Availability)
	Divulgazione (Disclosure)	✓		
	Modifica (Modification)		✓	
	Perdita/Distruzione (Loss/Destruction)			✓
	Interruzione (Interruption)			✓

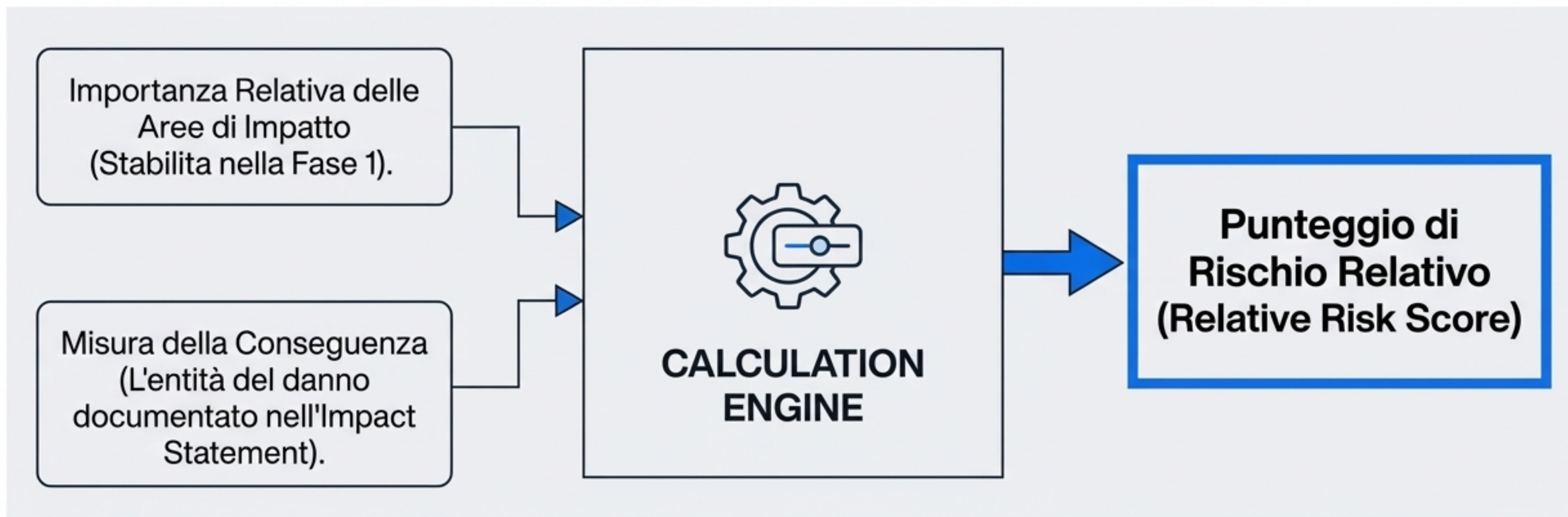
Se hai già considerato il risultato della minaccia (**Outcome**), hai automaticamente effettuato una determinazione iniziale sui requisiti di sicurezza violati.

Anatomia di un "Impact Statement"

Una dichiarazione descrittiva che dettaglia specificamente come un'organizzazione è colpita quando una minaccia si realizza.

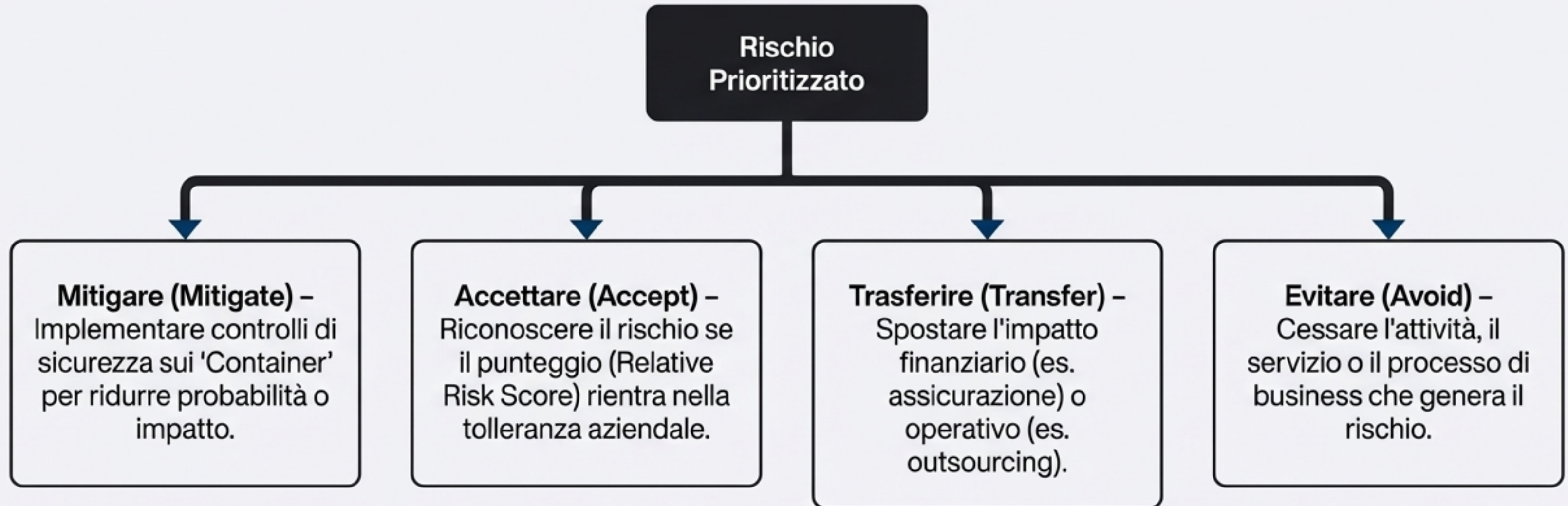


Valutazione e Scoring: Il 'Relative Risk Score' (Fasi 6-7)



Questo punteggio quantitativo determina la priorità assoluta. I rischi che hanno un impatto severo nelle aree di importanza critica per l'organizzazione ottengono priorità di mitigazione immediata.

Fase 8: Selezione dell'Approccio di Risposta



La decisione è guidata in modo inequivocabile dai driver stabiliti nella Fase 1.

Sintesi della Metodologia Allegro

Focus Informativo

(Sposta l'attenzione dall'infrastruttura tecnologica astratta al valore tangibile dei dati e dei loro container)

Oggettività Diagnostica

(Sostituisce le narrazioni soggettive con matrici strutturate 'fill-in-the-blank' e requisiti CIA)

Priorità Basata sul Business

(Allinea rigorosamente gli investimenti in mitigazione con i driver organizzativi tramite il Relative Risk Score)