IRAM2: Metodologia Avanzata per la Gestione del Rischio

Un'analisi strutturale e metodologica per esperti di Information Security e Risk Management.

Il fallimento degli approcci tradizionali all'ISRM

I framework di rischio tradizionali faticano a tradurre le vulnerabilità tecniche in impatti di business concreti, lasciando le aziende esposte e i budget mal spesi.

50%

delle grandi organizzazioni britanniche fallisce in un'efficace gestione dei rischi

72.7%

dei professionisti fatica a comunicare i rischi tecnologici ai leader aziendali

Il cambio di paradigma: Dal difetto tecnico all'impatto di business

IRAM2 (Information Risk Assessment Methodology 2) sposta l'asse della valutazione dalla speculazione qualitativa al rigore strutturato, mettendo il business al centro.

Approccio Tradizionale

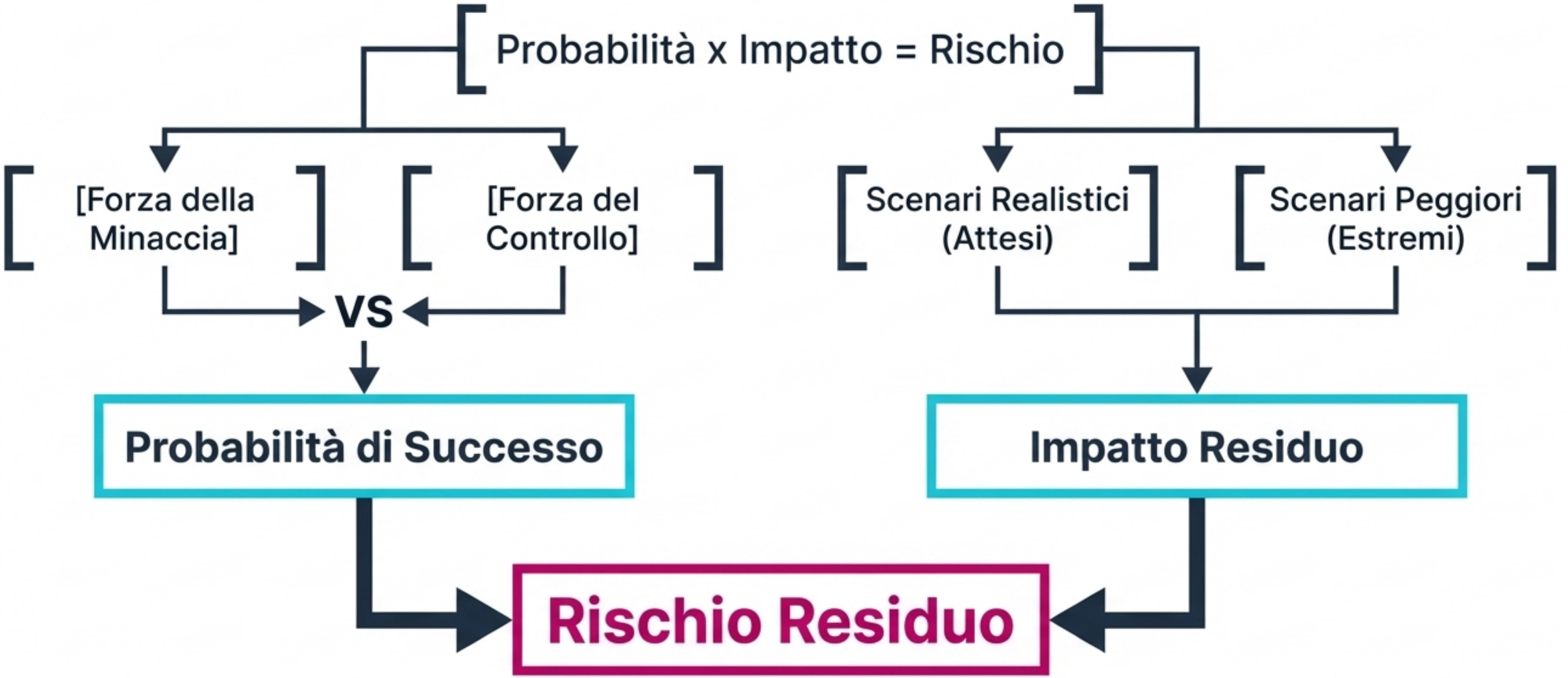
- IT-centrico, focalizzato sui difetti tecnici
- Valutazioni basate su speculazioni qualitative (guesswork)
- Disconnesso dagli obiettivi aziendali

Paradigma IRAM2

- Business-centrico, architettura strutturata e rigorosa
- Focalizzato su minacce e impatti reali
- Nativamente integrato con l'Enterprise Risk Management (ERM)

L’equazione espansa del rischio IRAM2

La scomposizione delle variabili di base in sotto-componenti misurabili per eliminare la soggettività nella valutazione.



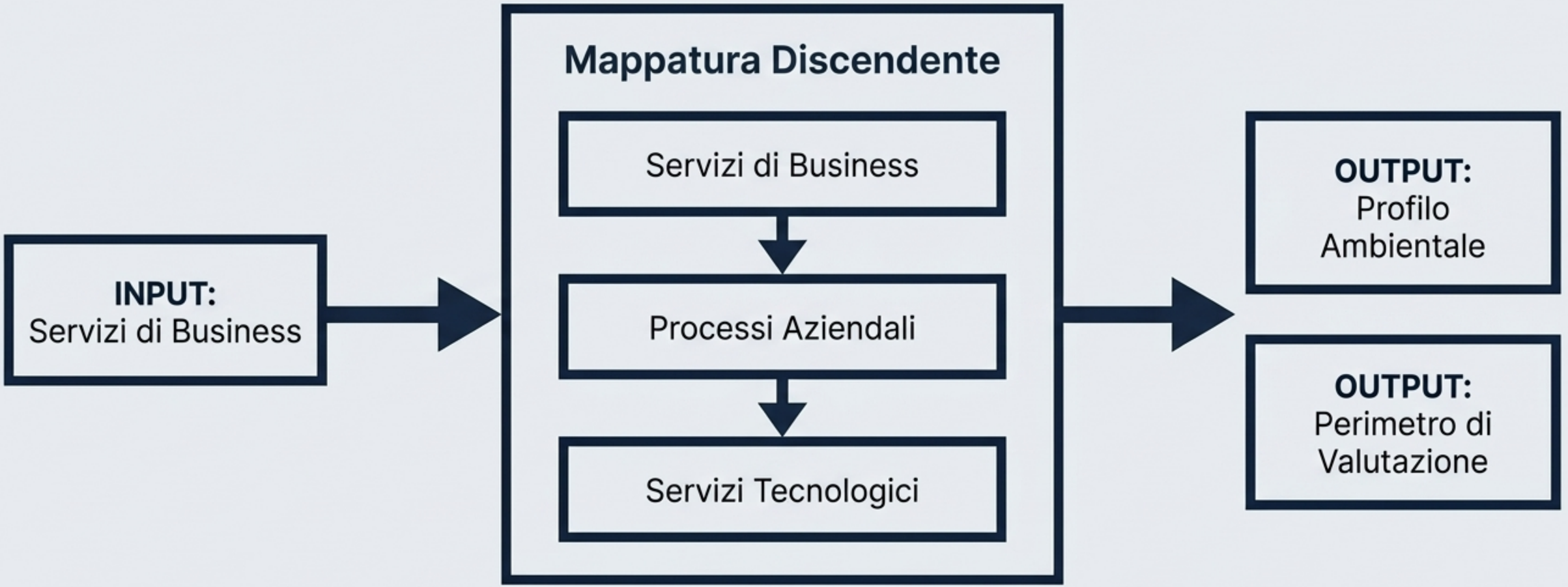
L’architettura a 6 fasi

Un processo sequenziale e modulare che trasforma il contesto ambientale in un piano di trattamento strategico e quantificabile.

Objectives	Steps
Definizione dell'Ambito (Scoping)	- Definizioni contesto dell'ambito - Business impact assessment - Identificati preiranzione - Ambito rivulnerabilita del scoping
Business Impact Assessment (BIA)	- Identificunzo da pianii di contesoio in mandare - Comprensa il trattamento strategico - Analyzizo tiola vulnerabilità - Drnaicraziore iis.rsessmenti
Profilazione delle Minacce (Threat Profiling)	- Profilazione delle minacce - Profilazione matibuce - Profilazione titranczeret.nponpa dell minacce
Valutazione delle Vulnerabilità (Vulnerability Assessment)	- Valutazione delle vulnerabilità - Valutazione del calinito - Valutazione utti delle vulnerabilità (vulnerabllità assessment)
Valutazione del Rischio (Risk Evaluation)	- Valutazione del rischio - Valutazione del rischio interndi - Rischio empoegsi - Valutazione del rischio e quantificale
Trattamento del Rischio (Risk Treatment)	- Trattamento del rischio - Trattamento del rischio insencine - Trattamento del rischio

Fase A: Definizione dell’Ambito (Scoping)

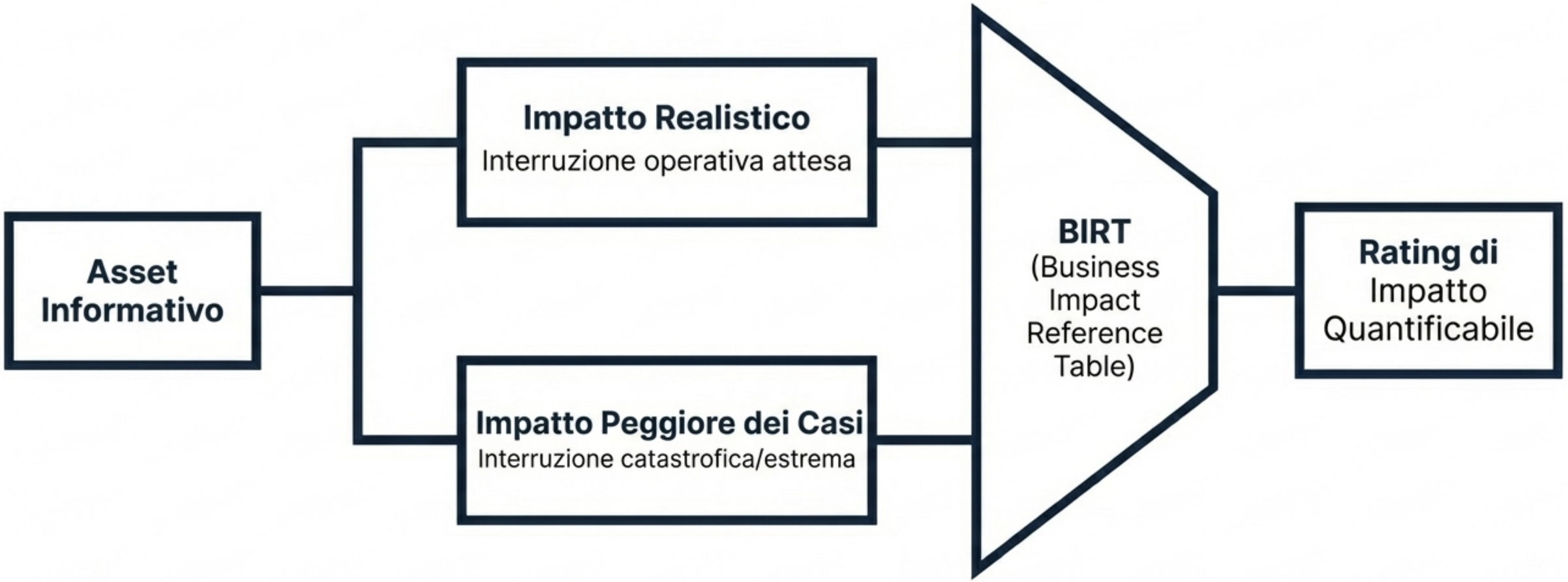
Partire dai servizi di business per mappare le dipendenze tecnologiche, garantendo che l'analisi sia rilevante per gli obiettivi aziendali.



A B C D E F

Fase B: Business Impact Assessment (BIA)

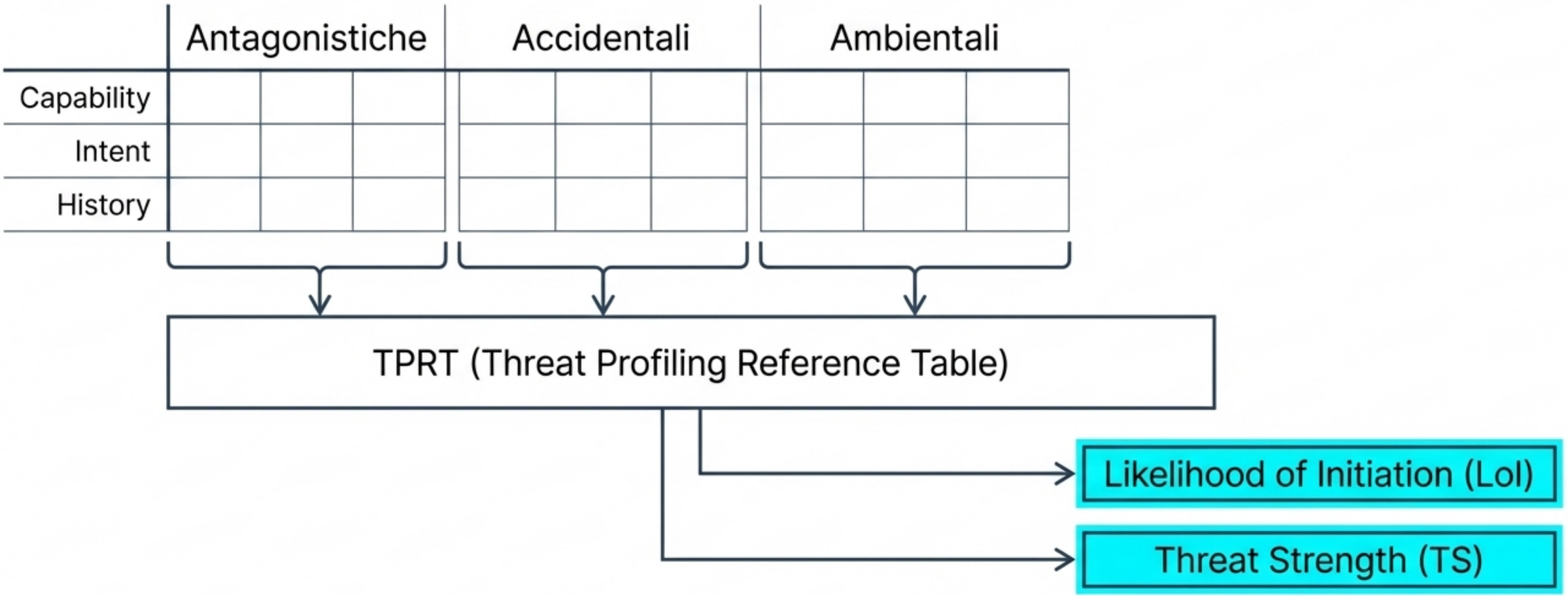
Valutare gli impatti su Riservatezza, Integrità e Disponibilità (CIA) separando scenari probabili da conseguenze catastrofiche.



A B C D E F

Fase C: Profilazione delle Minacce

Quantificare la motivazione, la capacità e l'intento per calcolare l'effettiva forza di ciascun attore ostile.



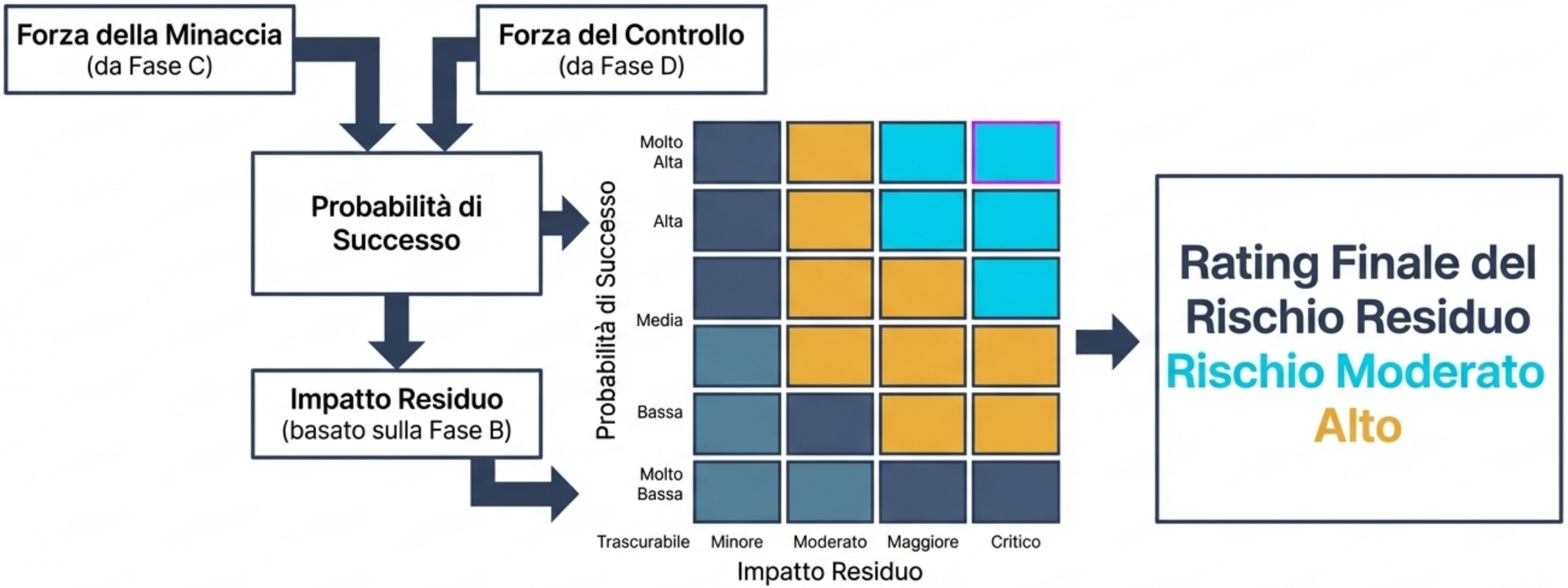
A B C D E F

Fase D: Valutazione delle Vulnerabilità

Misurare l'efficacia difensiva reale filtrando i 167 controlli ISF attraverso la pertinenza alla minaccia e la qualità dell'implementazione.

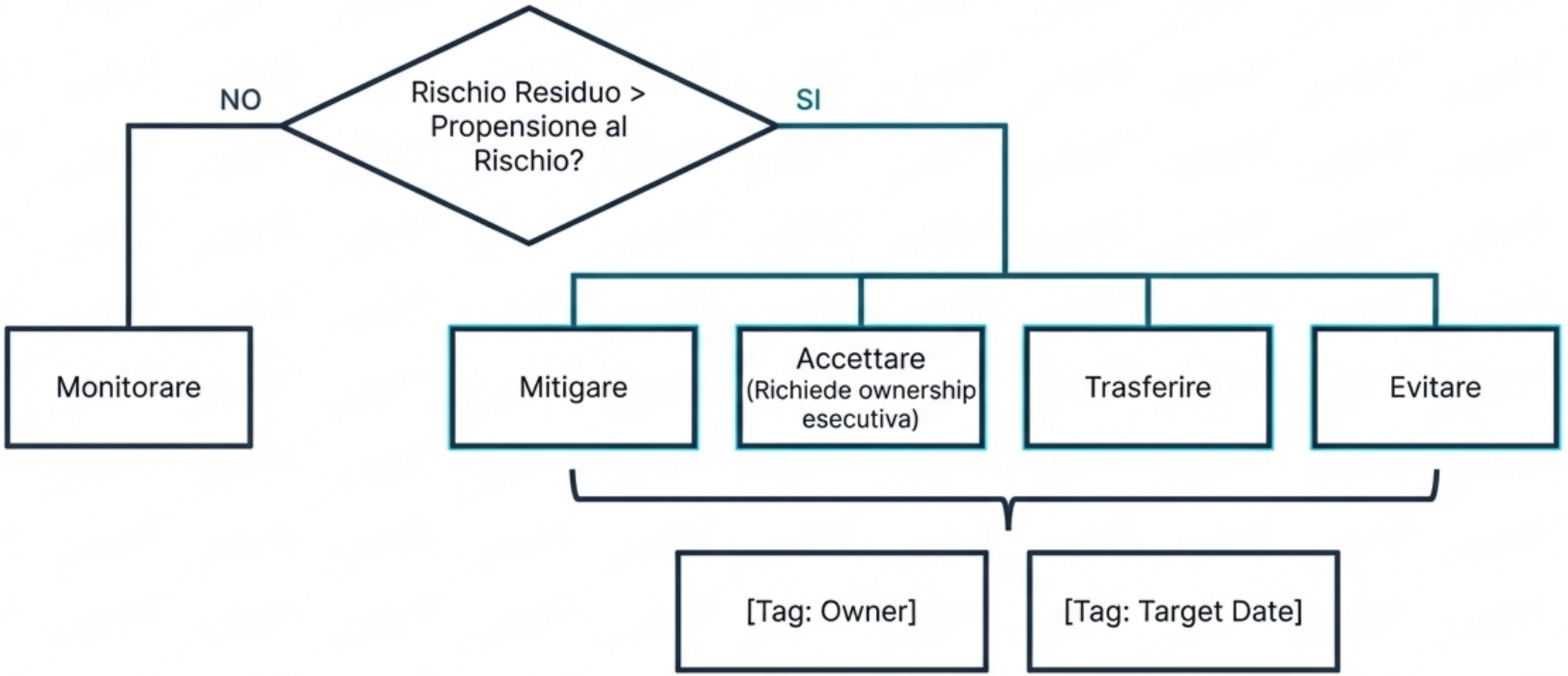
Fase E: Valutazione del Rischio

La sintesi delle metriche calcolate in una singola valutazione del rischio residuo, pronta per il processo decisionale esecutivo.



Fase F: Trattamento del Rischio

Il ponte verso l'azione: allineare il rischio residuo con la propensione al rischio aziendale (Risk Appetite) assegnando precise responsabilità.



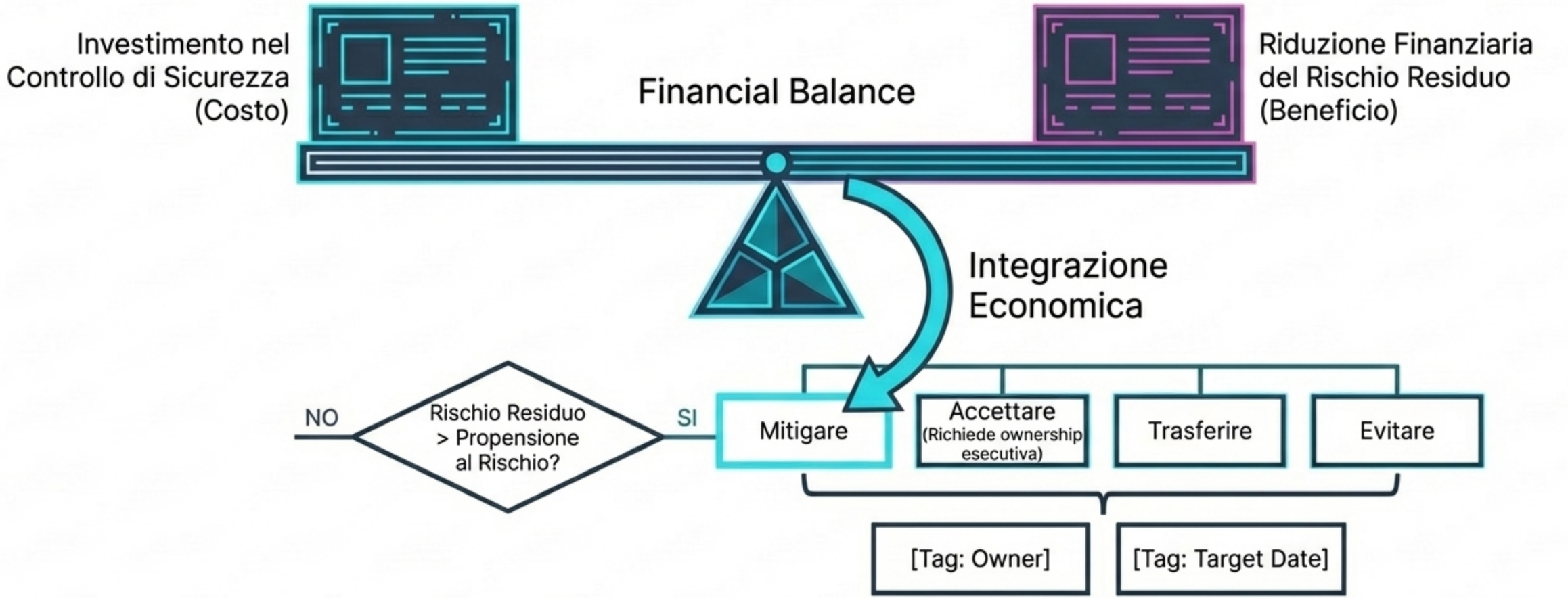
Framework Comparativo: IRAM2 nel panorama globale

Posizionamento diagnostico della metodologia ISF rispetto agli standard di settore ISO e NIST.

Dimensioni	IRAM2	ISO/IEC 27005	NIST SP 800-30
Approccio	Misto, Top-down & Bottom-up	Top-down Management	Bottom-up Tecnico
Complessità	Alta - Rigore strutturato	Media - Linee guida generiche	Alta - Dettaglio tecnico
Focus Principale	Business / Enterprise	Sistemi di Gestione (ISMS)	Governativo / Sistemi IT
Azione	Prescrittivo (‘Come fare”)	Descrittivo (“Cosa fare”)	Analitico

Il Metodo Ibrido: Integrare CBA (Cost-Benefit Analysis)

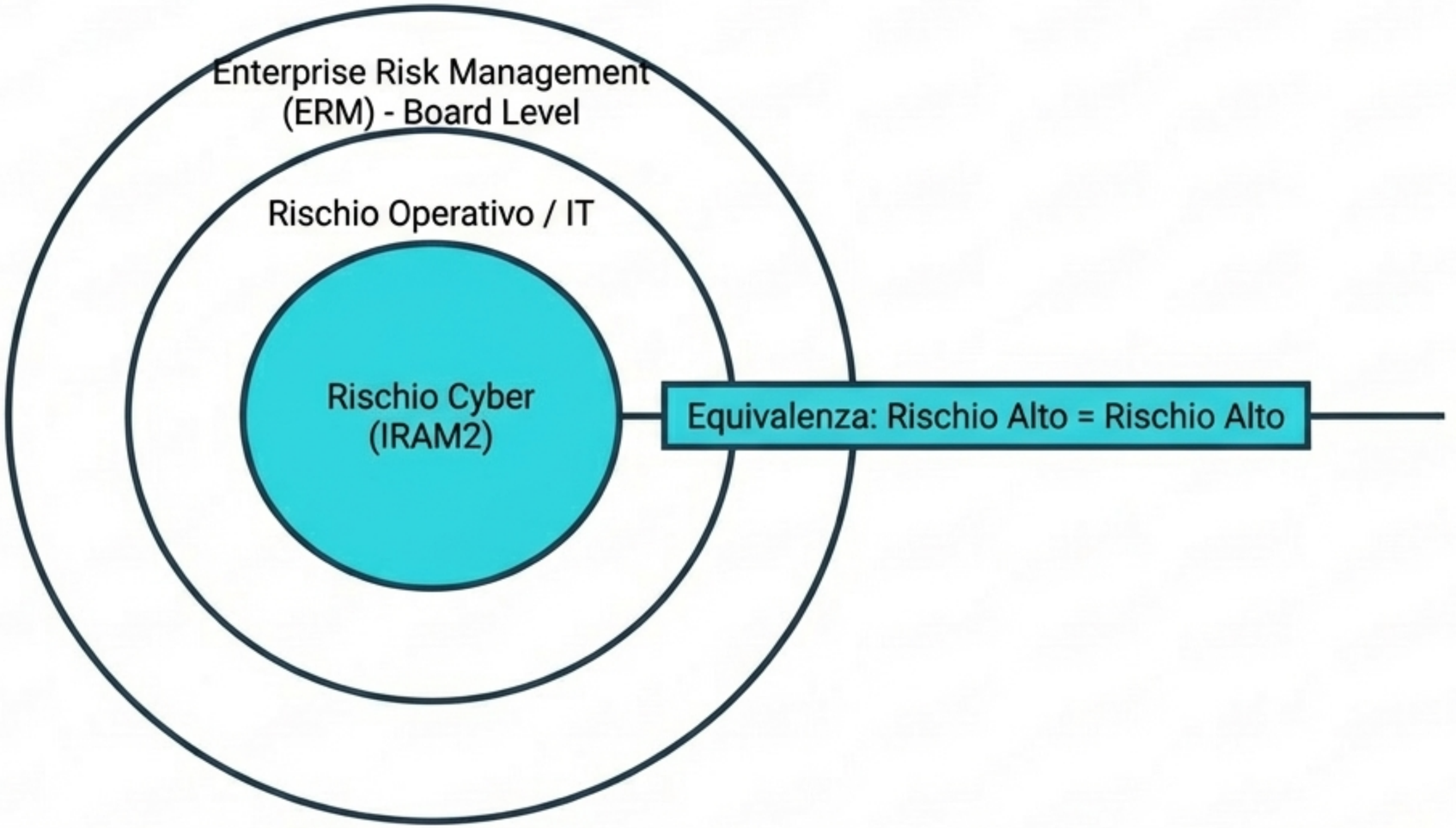
L'integrazione dell'analisi costi-benefici nelle Fasi E e F trasforma i dati sul rischio residuo nel ROI per i controlli di sicurezza.



A B C D E F

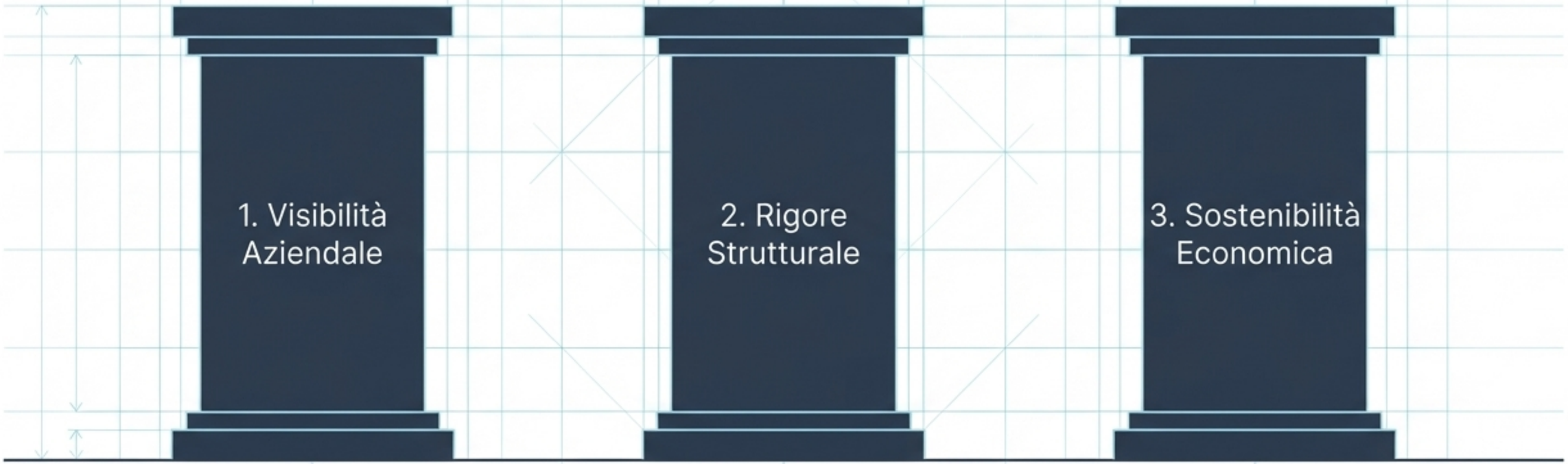
Sintesi Strategica: L'integrazione nell'Enterprise Risk Management

IRAM2 standardizza la tassonomia del rischio cyber, permettendo al CdA di ponderare i rischi informatici allo stesso livello dei rischi finanziari o operativi.



L’Imperativo della Resilienza

IRAM2 guida le organizzazioni dall'incertezza soggettiva a una gestione del rischio visibile, controllabile ed economicamente sostenibile.



Traduzione inequivocabile del rischio IT in impatto sul business.

Sostituzione delle speculazioni con metriche derivate e difendibili.

Giustificazione degli investimenti di sicurezza tramite integrazione ERM e CBA.