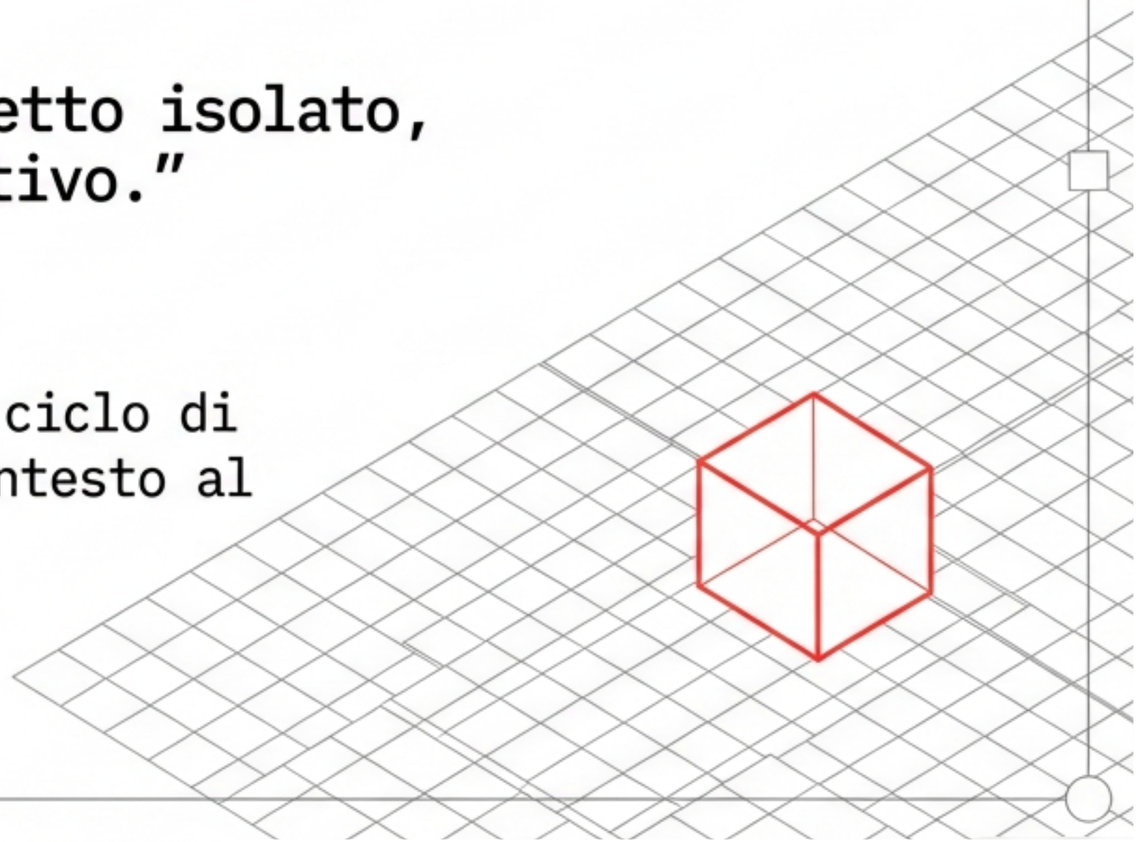
Pianificare il Processo di IT Risk Management

Metodologie, Framework e Strategie di Governance per i Sistemi Informativi

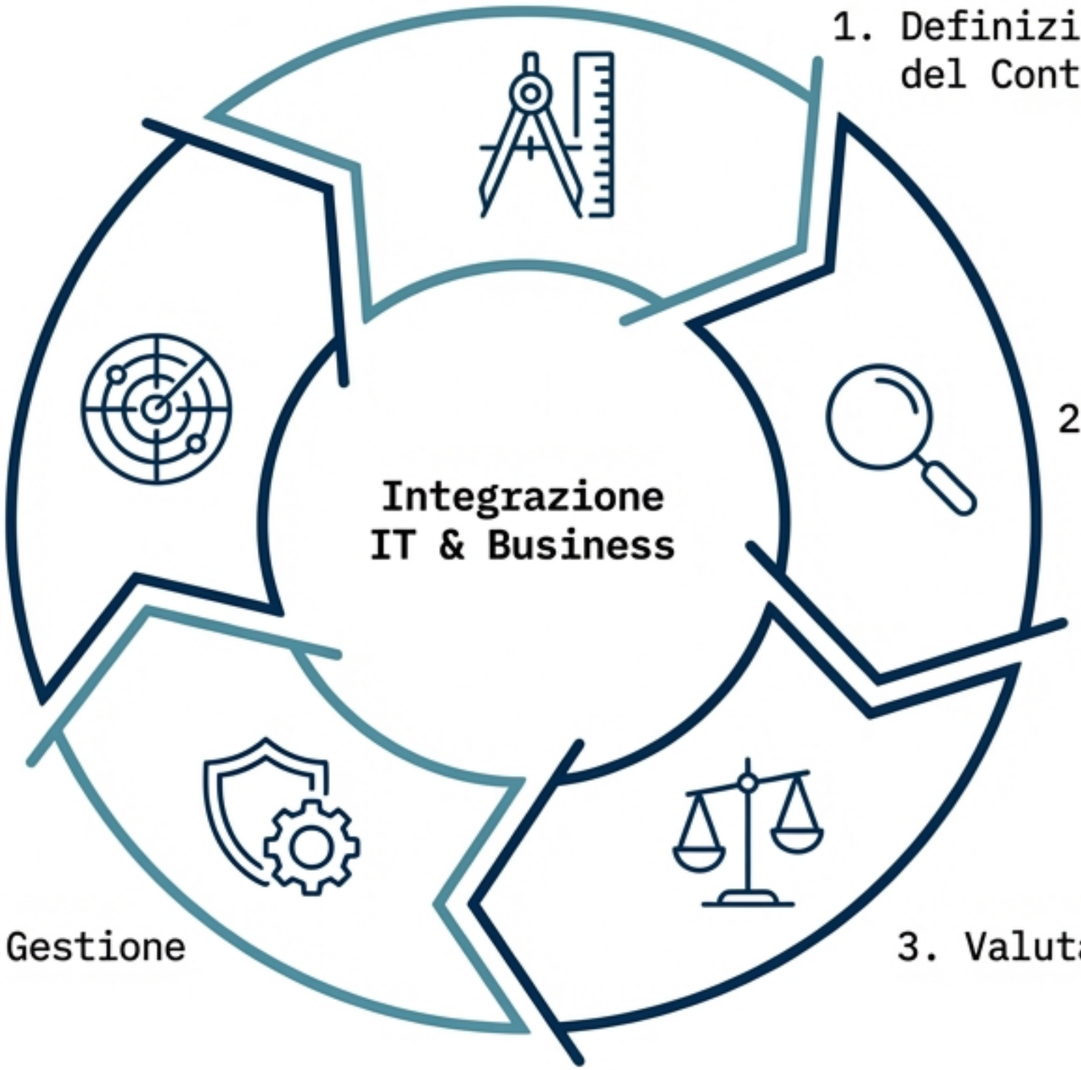
“L’IT Risk Management non è un progetto isolato, ma un processo continuativo e iterativo.”

Obiettivo: Comprendere come i framework internazionali (es. COBIT) strutturano il ciclo di vita del rischio, dalla definizione del contesto al monitoraggio del rischio residuo.



CORSO DI IT GOVERNANCE & MANAGEMENT // MODULO 01

Il Ciclo di Vita: Un Processo Continuativo



Ciclicità

La gestione del rischio non è un'attività "una tantum". Il processo deve evolvere parallelamente ai cambiamenti del contesto aziendale (nuovi asset, nuovi progetti, nuove minacce).

La Fase di Pianificazione

Definire le Regole del Gioco prima di iniziare.

Fonti Informative	Log di sistema, report incidenti, audit passati.
Tecniche di Identificazione	Brainstorming, analisi scenari, interviste strutturate.
Ruoli e Responsabilità	Definizione matrice RACI (Risk Owner vs. Control Owner).
Cadenza Temporale	Frequenza di aggiornamento del registro dei rischi.
Soglie di Attenzione	Livelli di tolleranza che richiedono escalation immediata.
Reportistica	Standard di comunicazione verso gli stakeholder.

Il Ruolo del Framework COBIT

1996

Audit & Controllo

Oggi (COBIT 2019)

Enterprise Governance & Management

Lo Standard

Fonte principale per l'IT Governance.
40 processi che coprono l'intero ciclo di vita del dato e della tecnologia.

Struttura Processo

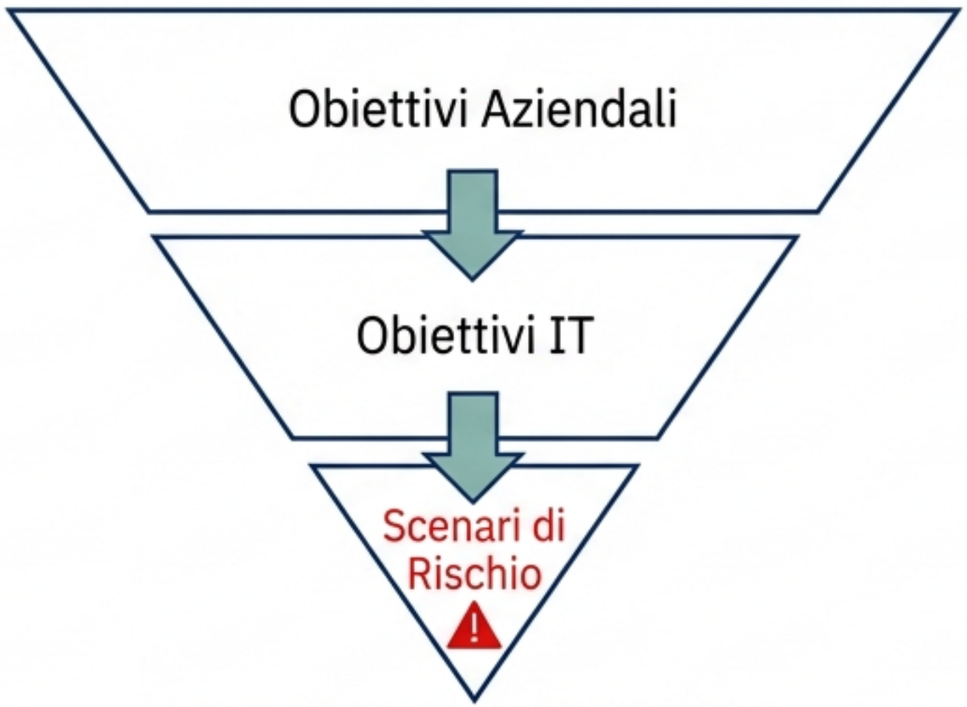
Ogni processo include: Obiettivi IT/Business, Management Practices, Metriche (KPI/KGI), Matrice RACI, Input/Output.

Valore Generato

Oltre la compliance (es. SOX).
Standardizzazione operativa, allineamento Business-IT e linguaggio comune.

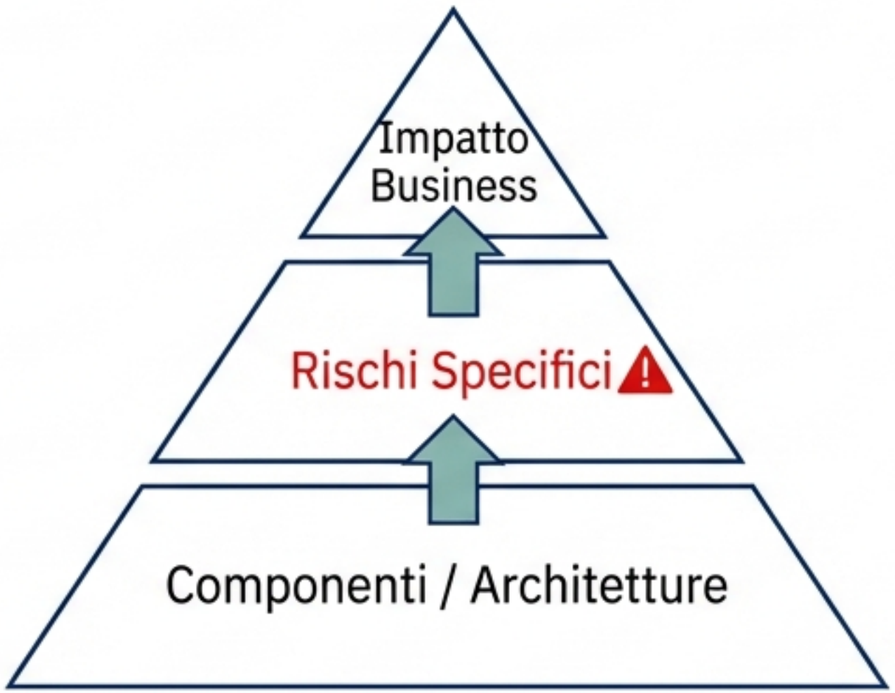
Approcci all'Identificazione

Top-Down (Strategico)



Attori: Senior Management

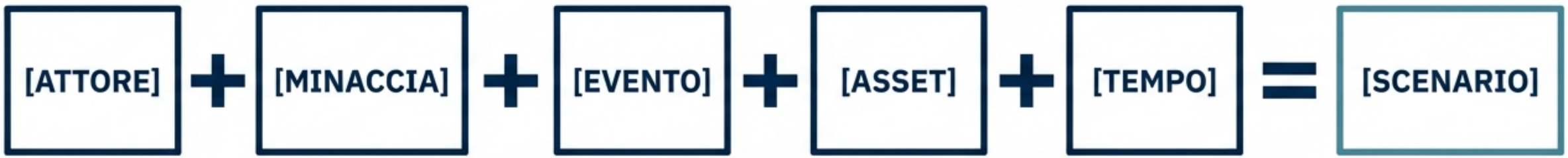
Bottom-Up (Tecnico/MAP)



Attori: Tecnici IT

Best Practice: Combinare i due approcci per garantire copertura strategica e operativa.

Strumenti: Costruire “Scenari di Rischio”



Interno (Staff), Esterno (Competitor), Terze parti.

Errore, Dolo, Guasto, Disastro.

Disclosure, Interruzione, Modifica, Furto.

Dati, Processi, Infrastruttura, App.

Durata, Frequenza, Rilevamento.

Esempio: Un utente interno (Attore) per errore (Minaccia) causa la disclosure (Evento) di dati sensibili (Asset) con effetto prolungato (Tempo).

Analisi: Quantitativa vs. Qualitativa

Statistica e Dati Empirici.

PRO: Oggettività.

CONTRO: Richiede serie storiche di dati (spesso indisponibili). Rischio "Overconfidence".

Etichette Descrittive (Alto/Medio/Basso).

PRO: Veloce, applicabile senza dati storici.

CONTRO: Soggettiva. "Risk beauty is in the eye of the beholder".

Approccio Ibrido: Usare dati storici per giustificare le etichette qualitative.

Psicologia del Rischio: Bias ed Euristiche

Perché il giudizio umano fallisce nella valutazione.

Bias di Negligenza (Probability Neglect)

Paura sproporzionata per eventi rari ma drammatici (es. squalo) rispetto a rischi comuni (es. incidenti domestici).

Bias della Disponibilità (Availability)

Sovrastima di eventi recenti o con forte risonanza mediatica.

Bias della Vicinanza (Proximity)

Sottostima dei problemi percepiti come geograficamente o temporalmente lontani.

Soluzione: Processi collaborativi e guidati.

La Matrice di Valutazione: Evidence-Based

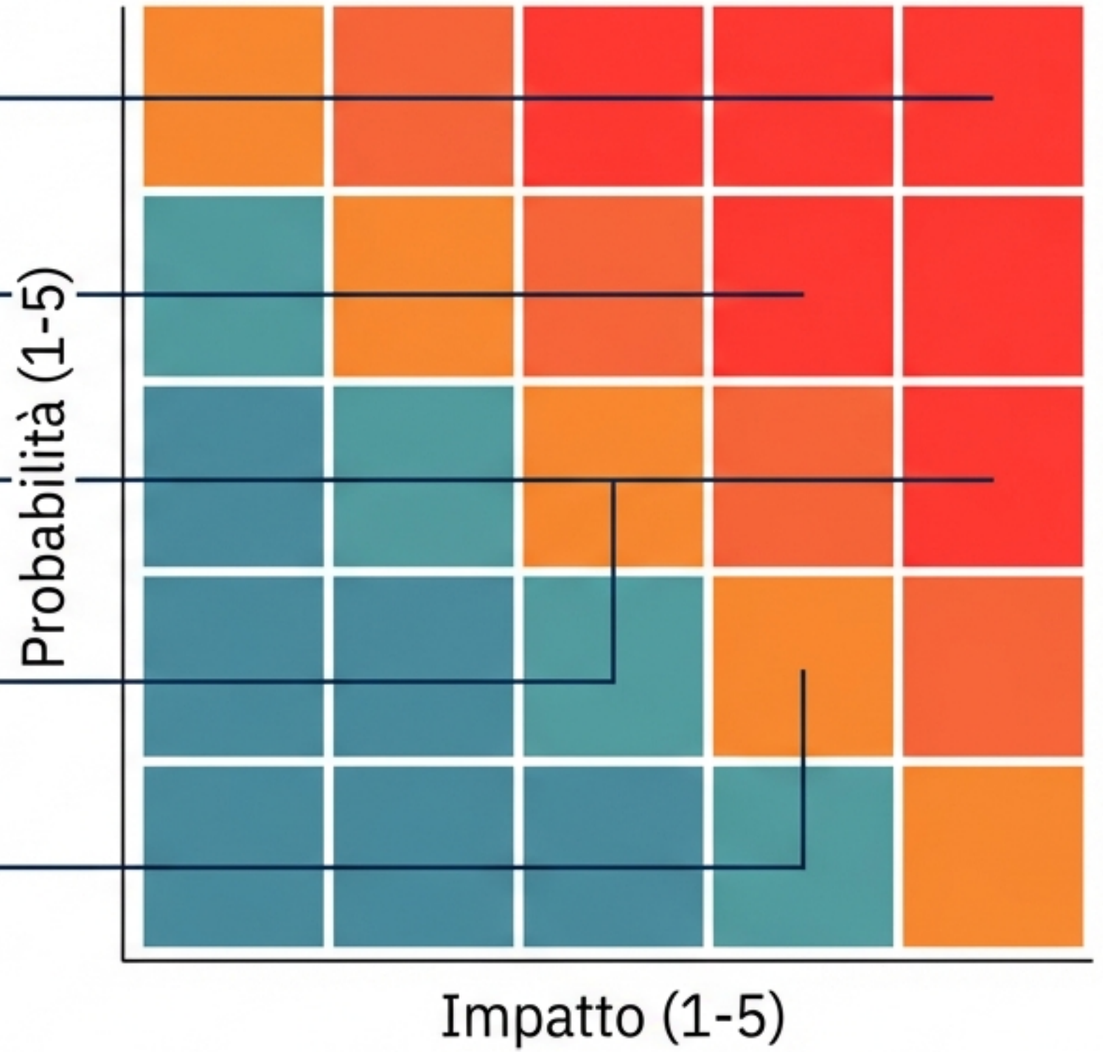
Posizionare il rischio richiede dati, non solo percezioni.

Help Desk / Ticketing:
Volume problematiche utente.

Log di Sistema:
Tracciamento attività.

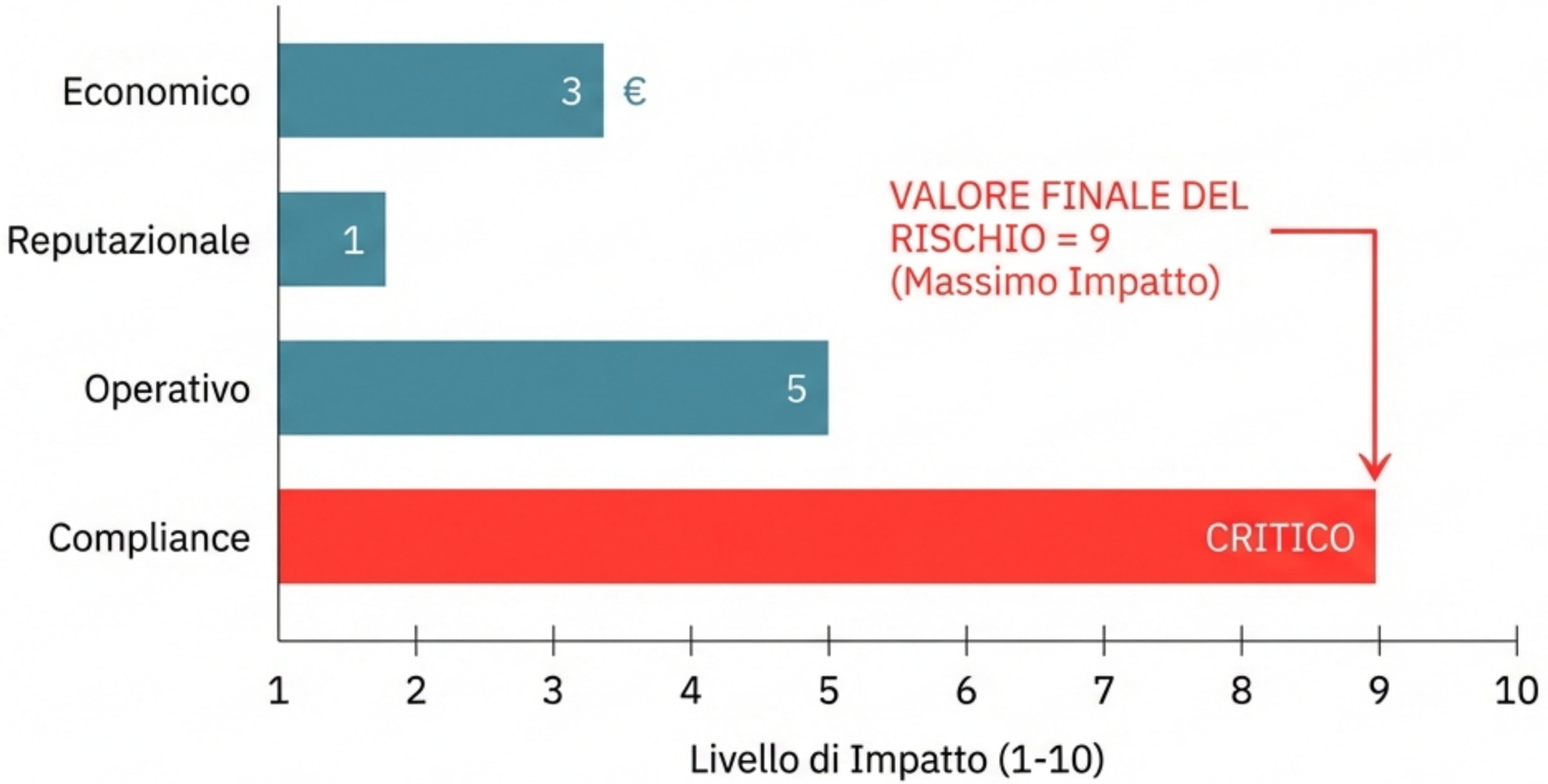
Change Management:
Frequenza modifiche e failure rate.

Disponibilità:
Uptime storico infrastrutture.



Scale di Impatto e Tolleranza

Il principio del “Maximum Impact Rule” nella valutazione.



Governance Rule:

Le soglie (es. €1M = Critico) sono definite dal Board/ERM in base alla Risk Tolerance, non dall’IT Manager.

Strategie di Gestione (Risk Response)

AVOID (Evitare)

Desc: Non intraprendere l'attività.
Es: Dismettere Data Center a rischio.

TRANSFER (Trasferire)

Desc: Spostare su terze parti.
Es: Assicurazioni, Outsourcing.

MITIGATE (Ridurre)

Desc: Agire su Probabilità o Impatto.
Es: Controlli, Backup, Formazione.

ACCEPT (Accettare)

Desc: Tollerare formalmente.
Es: Decisione tracciata e approvata.

Strategie Temporanee

Quando la decisione finale richiede tempo.

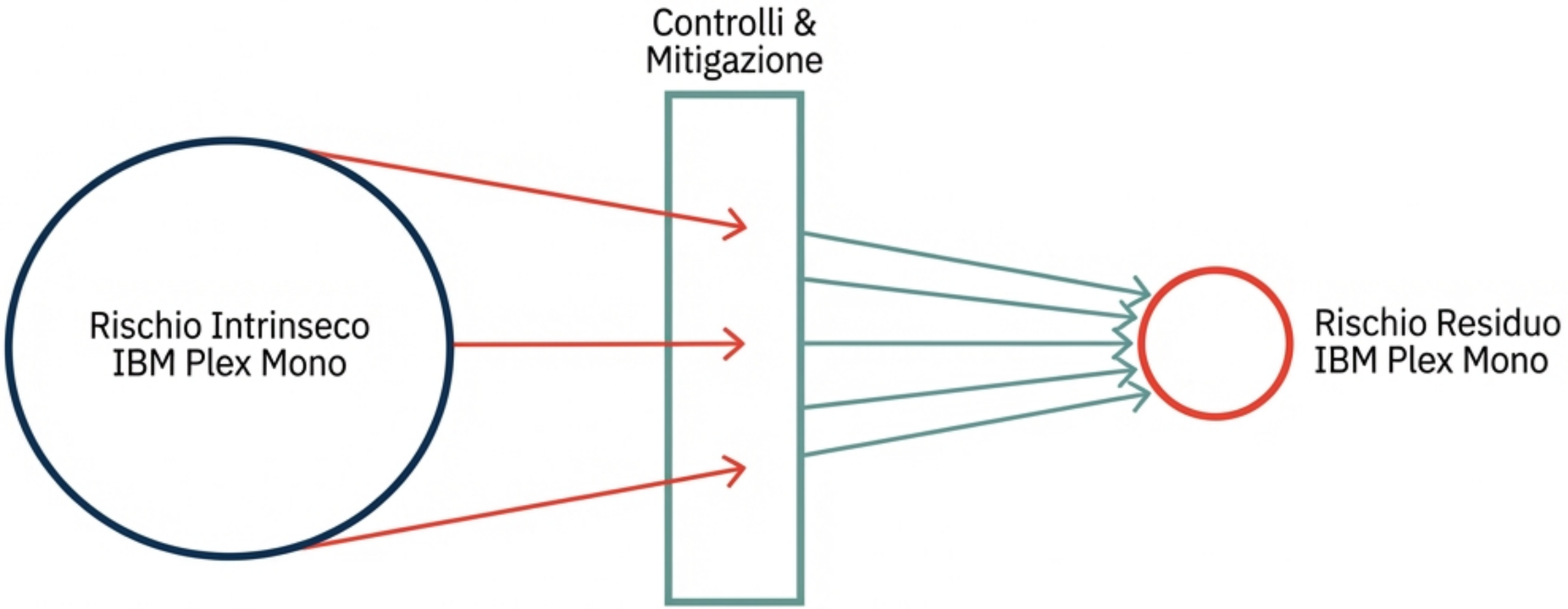
OSSERVARE (Passivo)

Per rischi minori o per valutare trend nel tempo (peggioramento/miglioramento).

INVESTIGARE (Attivo)

Ricerca attiva delle cause radice per raccogliere dati mancanti e decidere.

Il Rischio Residuo e il Monitoraggio



- **Definizione*:** Il rischio che permane dopo l'implementazione dei controlli.
- **Azione Richiesta***: Monitoraggio continuo per intercettare cambiamenti nel contesto.
- **Audit***: Verifica indipendente (IS Audit) dell'efficacia dei controlli.

Conclusioni: IT Risk Management come Leva Strategica

La gestione del rischio IT abilita l'azienda a perseguire i propri obiettivi in un ambiente controllato.