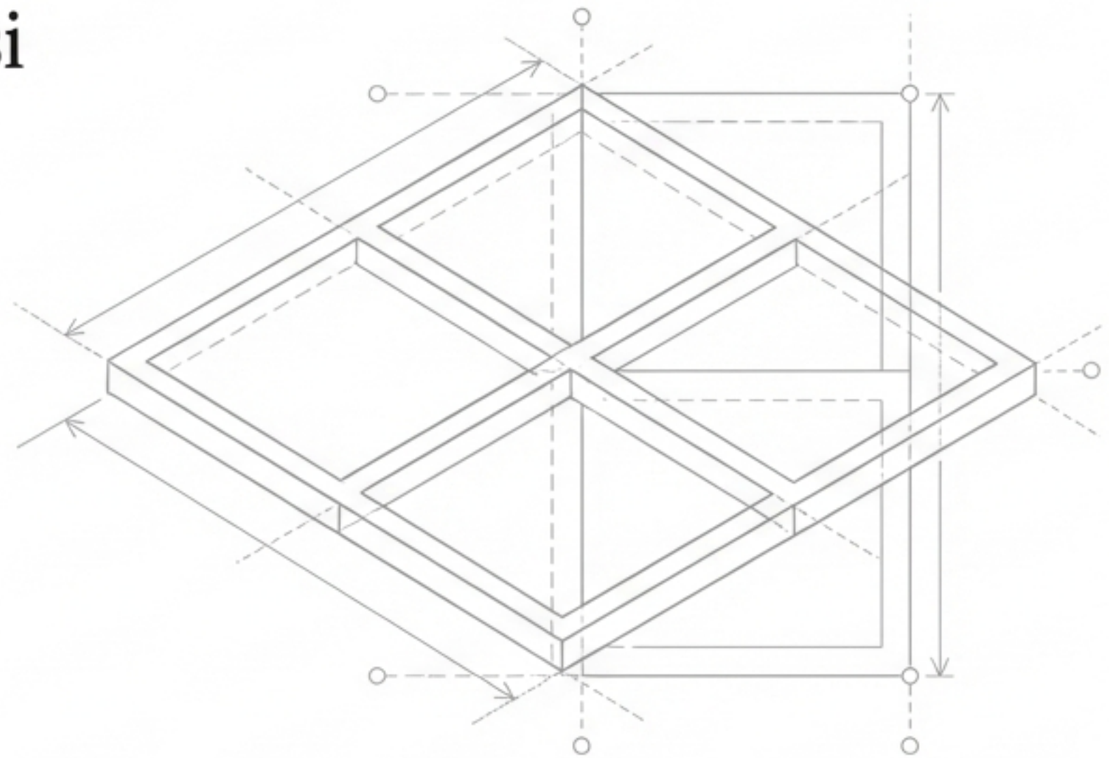
La Gestione del Rischio IT: Tassonomia e Domini

Metodologie di identificazione e analisi per i sistemi informativi aziendali



Definizione e Perimetro del Processo

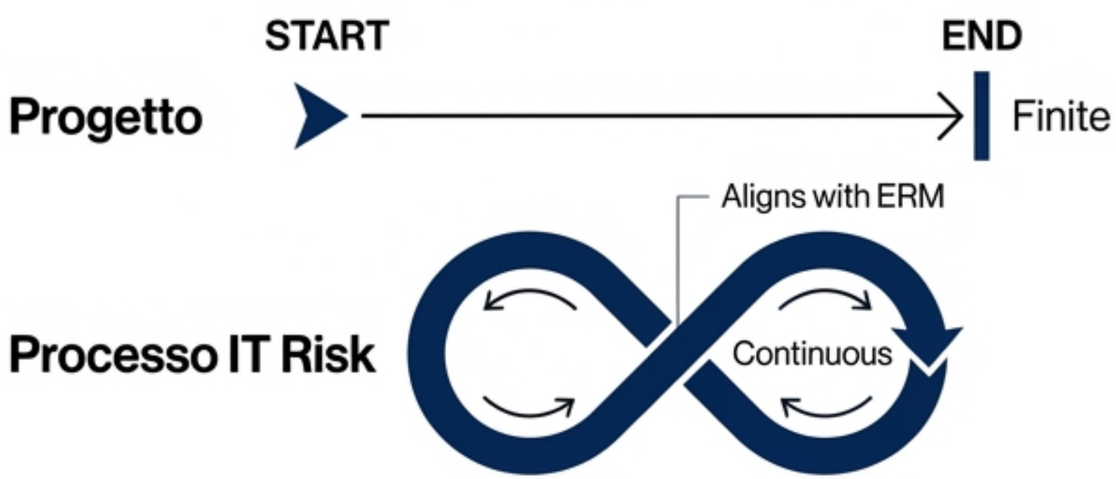
L'IT Risk Management è un processo continuo, allineato all'Enterprise Risk Management (ERM), non un'iniziativa progettuale temporanea.

Obiettivi Duali:

1. Mitigazione: Prevenire o ridurre l'impatto di eventi negativi.
2. Valore: Massimizzare le opportunità offerte dalle tecnologie digitali (ICT).

Perimetro:

- Persone, Tecnologie, Risorse Finanziarie, Dati, Processi Operativi, Governance.



La Necessità di una Tassonomia Strutturata

Basato sulla classificazione Forrester Research (2009)

Rischi Non Strutturati → **Tassonomia Lens**
Filtro e Classificazione
→ **Rischi Strutturati**
Organizzazione per Categorie

Completezza
Helvetica Now Display

Garantire che nessun ambito di rischio venga trascurato durante l'identificazione.

Granularità
Helvetica Now Display

Permette la segmentazione in sottodomini per analisi approfondite.

Reportistica
Helvetica Now Display

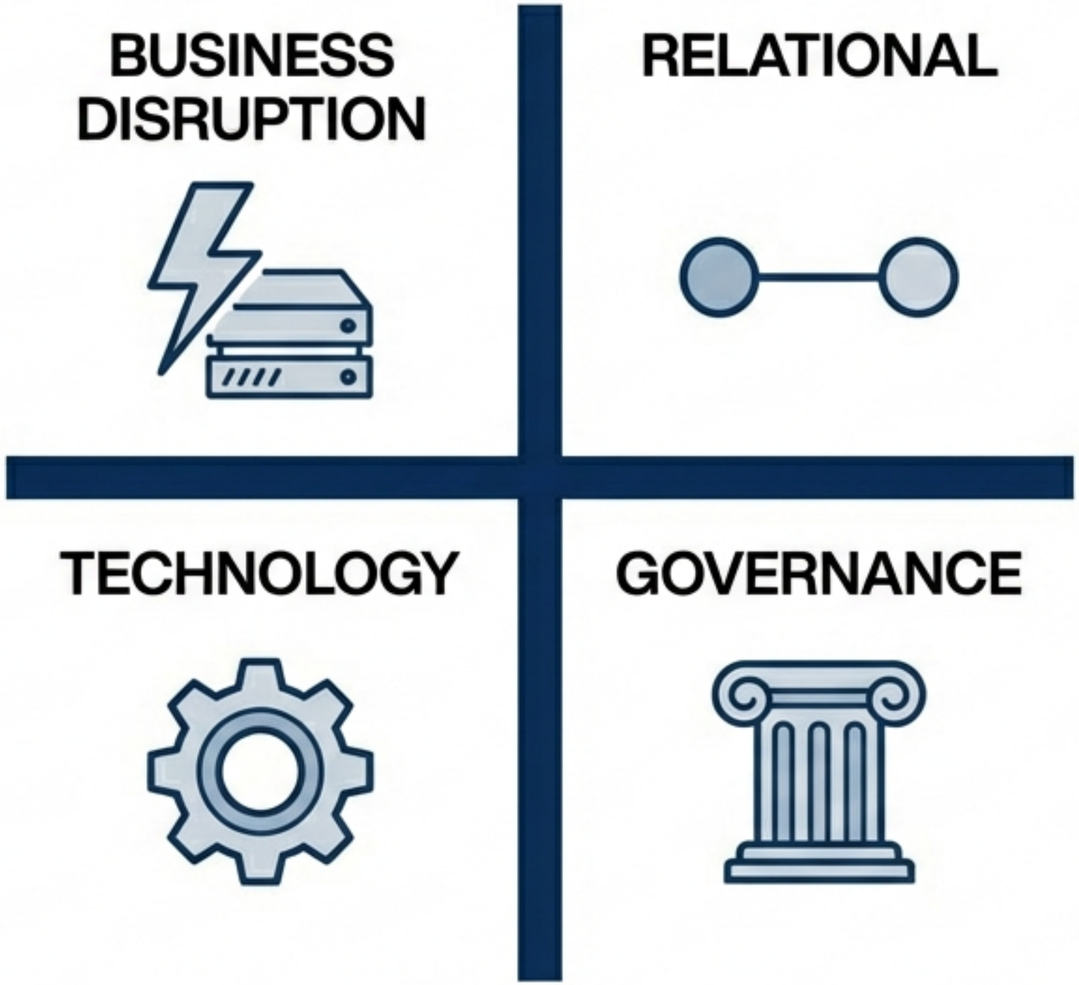
Fornisce una logica per rappresentare il rischio in ampiezza e profondità.

Comunicazione
Helvetica Now Display

Crea un linguaggio comune comprensibile al di fuori dell'IT (es. Board, Audit).

www.vincenzocalabro.it

Il Framework Forrester: I 4 Domini del Rischio



Questi domini fungono da macro-aggregazioni per la classificazione dettagliata dei rischi.

Dominio 1: Business Disruption

Rischi che causano l’inoperatività parziale/totale del sistema informativo o la perdita di informazioni sensibili.

Cause Scatenanti (Triggers):

- Eventi avversi naturali (disastri).
- Attacchi esterni imprevisti alla rete aziendale.
- Inadeguata protezione del patrimonio dati.

Impatto:

- Interruzione della continuità operativa aziendale.

Dominio 2: Relational (Rischi Relazionali)

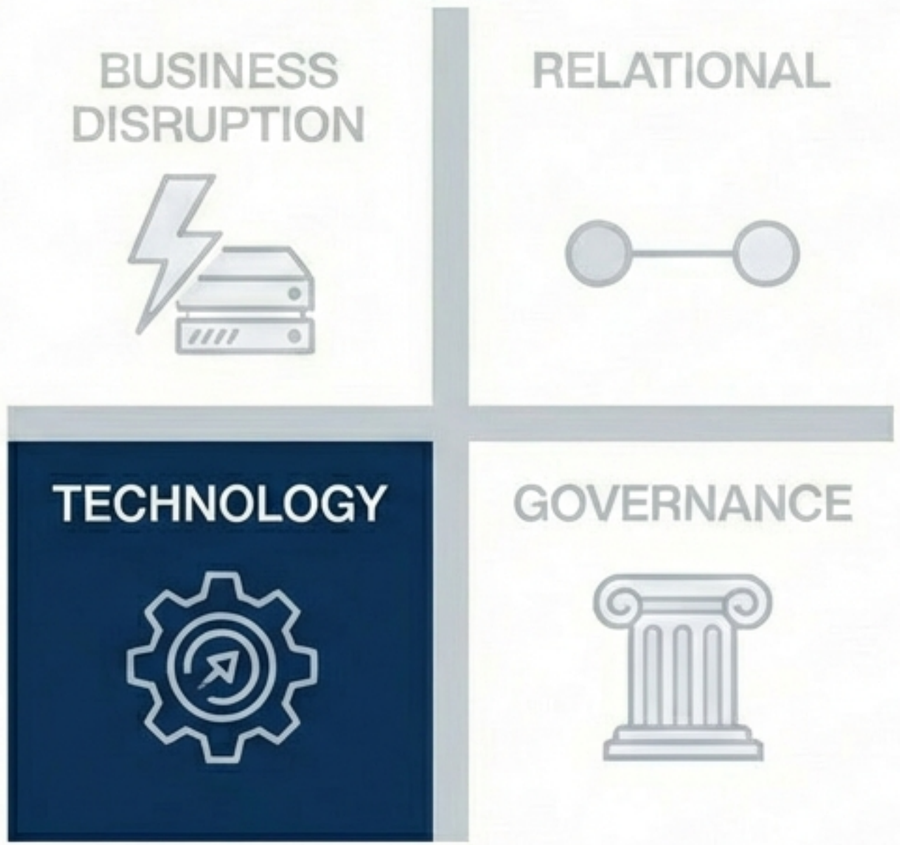
Rischi derivanti dalle interazioni tra il sistema informativo e altre entità (interne o esterne).

Aree Chiave:

- Fornitori & Outsourcing: Gestione delle terze parti (es. System Integrator).
- Clienti: Interazione digitale e servizi erogati.
- Compliance: Rispetto delle normative e regolamenti esterni.

Dominio 3: Technology (Rischi Tecnologici)

Rischi connessi alle scelte architetturali e alla gestione operativa.

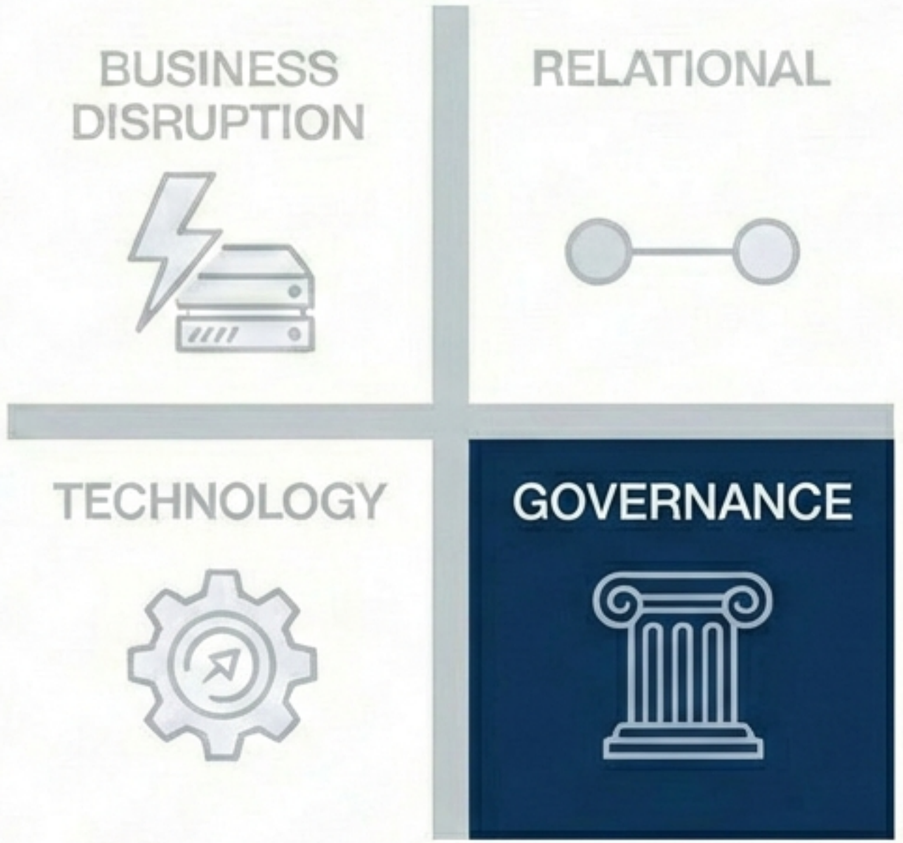


Aree Chiave:

- Architettura: Obsolescenza, scalabilità, scelte di design.
- Operations: Capacity management, performance dei sistemi.
- Change & Project Management: Rischi legati alla gestione dei progetti IT (tempi, costi, delivery).

Dominio 4: Governance (Rischi di Governo)

Rischi connessi alle scelte manageriali e strategiche dei sistemi informativi.



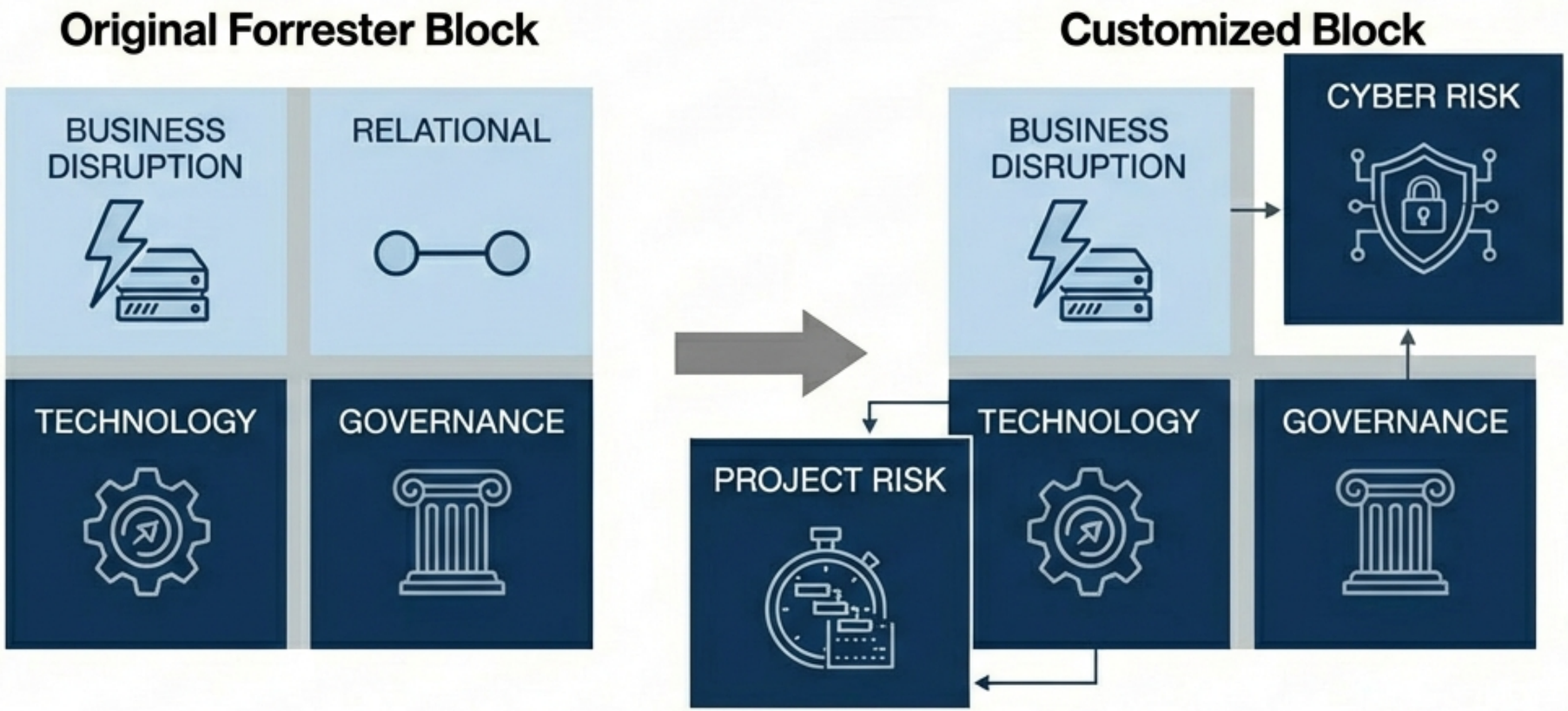
Aree Chiave:

- Strategia: Disallineamento tra IT e obiettivi aziendali.
- Organizzazione: Struttura dell'IT, definizione dei ruoli.
- HR Management: Competenze, gestione delle risorse umane in ambito tecnico.

www.vincenzocalabro.it

Adattamento Critico della Tassonomia

Le tassonomie non vanno adottate in modo acritico, ma adattate al contesto specifico.

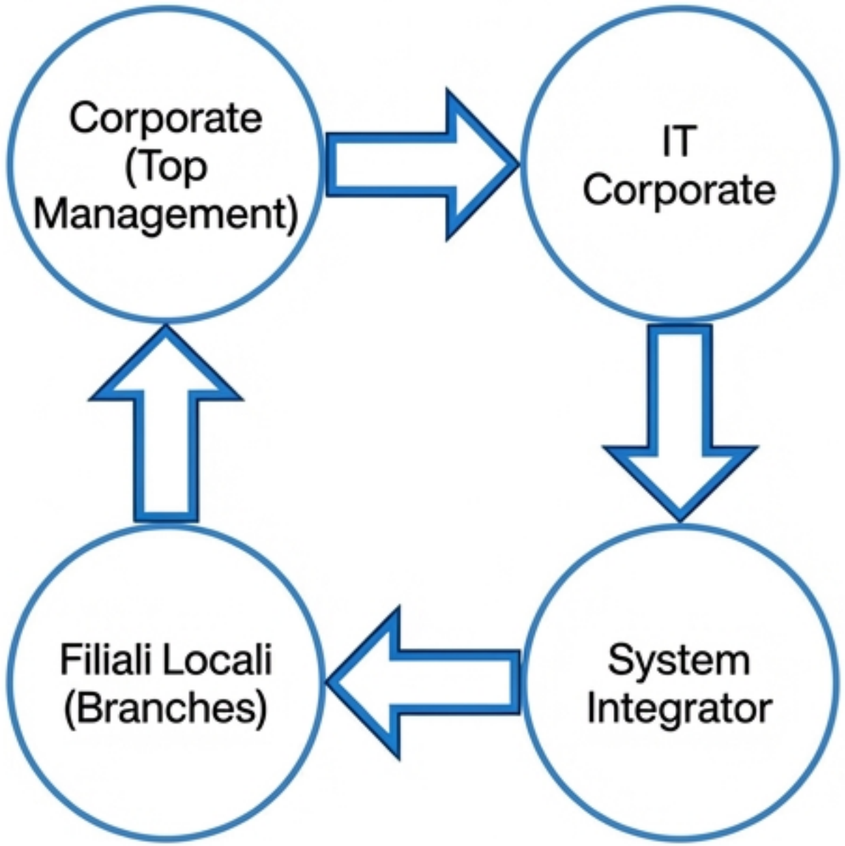


1. “Project Risk”: Se l’azienda è project-intensive, il rischio di progetto (da Technology) diventa un dominio autonomo.

2. “Cyber Risk”: Security e Online Risk (da Business Disruption) meritano un dominio dedicato nel contesto moderno.

La tassonomia guida l’identificazione, ma deve evolvere con l’azienda.

Caso Studio USIS: “Uno Stallo alla Messicana”



Azienda: Acme Oil & Gas (Divisione USIS)
Scenario: Consolidamento ERP e standardizzazione processi
Outcome: Progetto bloccato, tempi sforati, budget a rischio

Analisi degli Attori e degli Obiettivi

Attore	Obiettivo Esplicito	Obiettivo Implicito
Corporate	Market share	Centralizzazione del potere
IT Corporate	Standardizzazione ERP	Allineamento politico / Cambio Governance
System Integrator	Implementazione Kernel Standard	Profitto (Minimizzare personalizzazioni)
Filiali Locali	Specificità di Business	Difesa dell'autonomia locale

Diagnosi: Mappatura dei Rischi nel Caso USIS

FALLIMENTO PRIMARIO: GOVERNANCE RISK

Issue: Strategia 'Cavallo di Troia'. L'IT usato per imporre cambiamenti organizzativi senza ingaggio politico.
Risultato: Resistenza passiva e attiva delle filiali.

FALLIMENTO CONSEGUENTE: TECHNOLOGY/PROJECT RISK

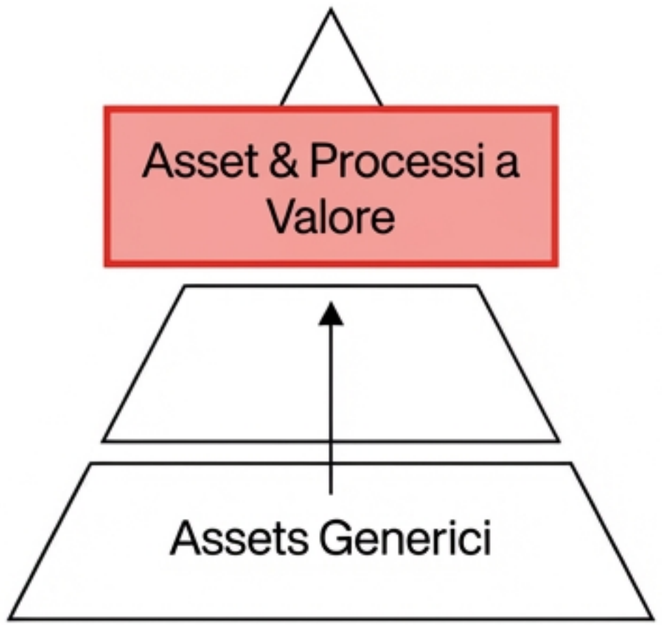
Issue: Sottostima della complessità. Go-live in 20 giorni irrealistico.
Risultato: Esplosione delle Change Requests (2400 gg) e saturazione del System Integrator.

Focus Verticale: Cyber Risk Management

Landscape delle Minacce

- **Interne:** Phishing mirato ai dipendenti.
- **Esterne:** Brand Abuse, Furto dati (Loyalty).

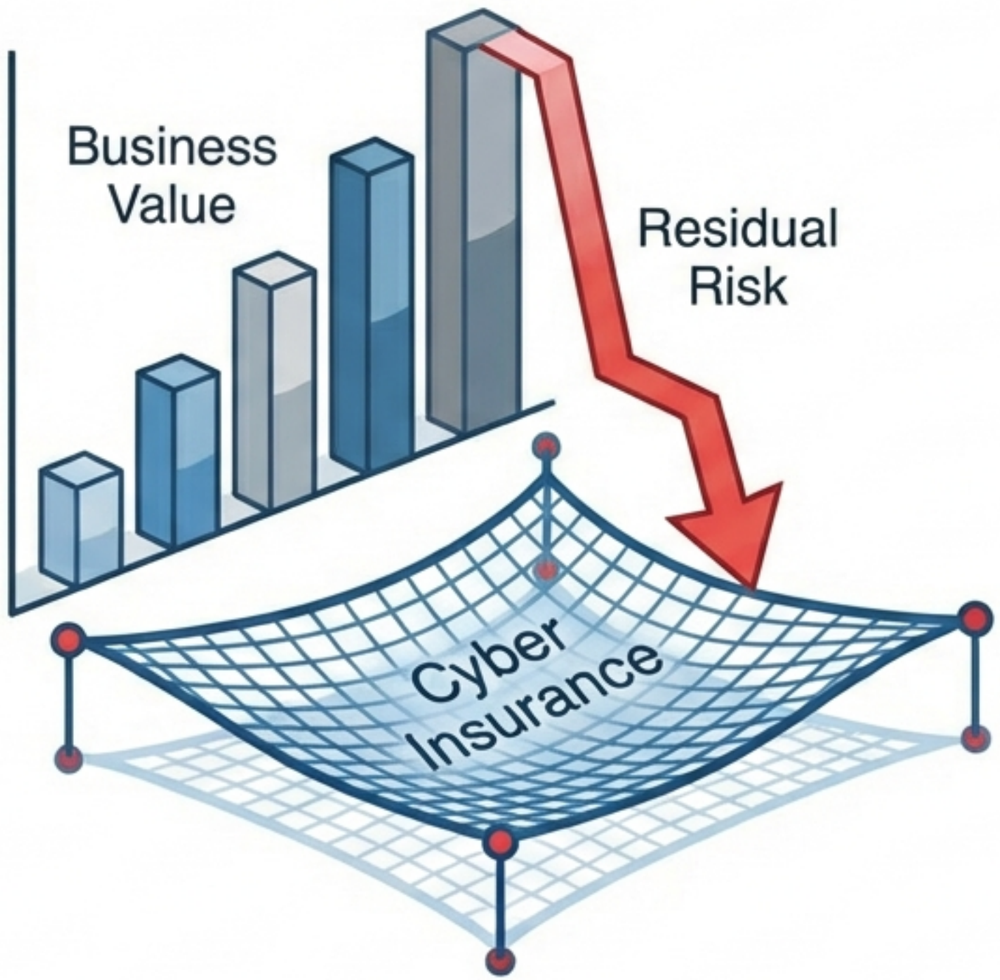
Approccio Risk-Based



Allocare risorse dove fanno la differenza (Efficacia vs Efficienza).

Ruolo della Security: Abilitatore del business e del Time-to-market.

Il Trasferimento del Rischio: Cyber Insurance



Funzione:

Un ‘Paracadute’ per il rischio residuo (non sostituisce la prevenzione).

Ambito di Copertura:

Danni finanziari, legali, reputazionali, costi di fermo attività.

Criticità nell’Assessment:

- Basato su questionari (NIST/ISO 27001) e scansioni esterne.
- Spesso la security è percepita come problema solo IT e non di business.

Sintesi e Conclusioni

1 **Processo**
L'IT Risk Management è un processo strategico continuo, non un progetto una tantum.

2 **Struttura**
La Tassonomia Forrester (4 Domini) è essenziale per l'identificazione completa dei rischi.

3 **Applicazione**
I framework teorici devono essere adattati al contesto (es. isolando il Cyber Risk).

4 **Integrazione**
Una gestione efficace combina Governance (strategia), Technology (sicurezza operativa) e Finance (assicurazione).