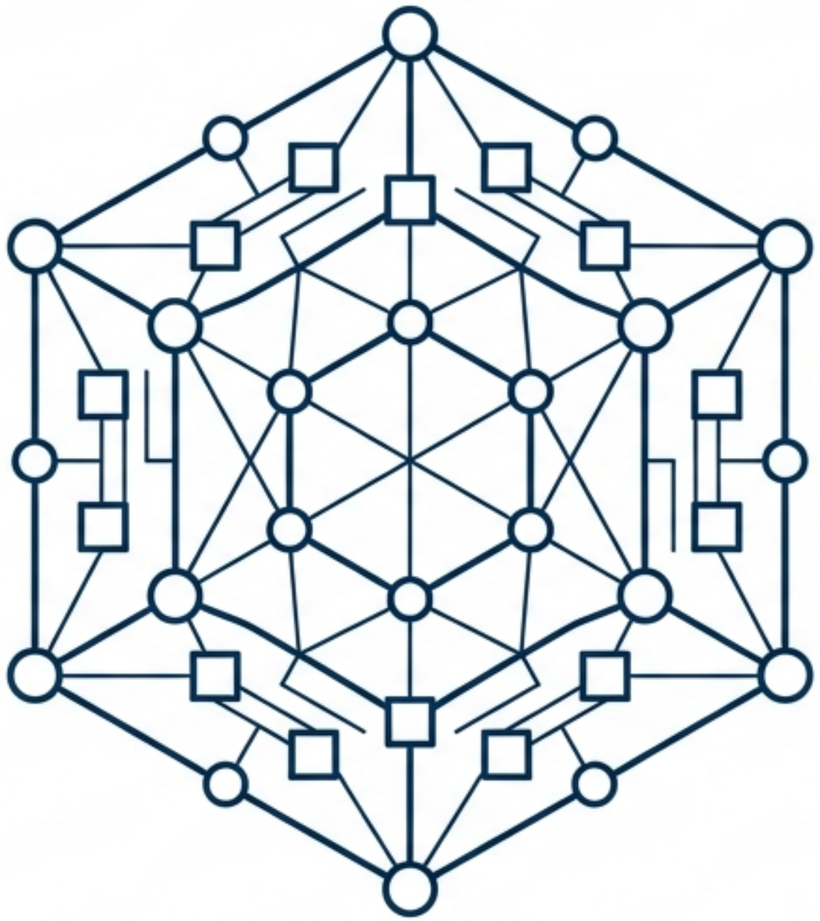
ISO/IEC 27005:2022



Gestione del Rischio per la Sicurezza delle Informazioni

Linee guida per l'identificazione, l'analisi e il trattamento dei rischi nel contesto ISO/IEC 27001

Il Contesto Normativo

- Ruolo della norma: Fornisce le linee guida per soddisfare i requisiti di gestione del rischio specificati nella ISO 27001.
- Natura: Standard di supporto, non certificabile autonomamente.
- Flessibilità: Metodologia adattabile (es. NIST, OCTAVE) purché allineata all'ISMS.

Evoluzione Normativa: 2018 vs 2022

Versione 2018 (Statico)

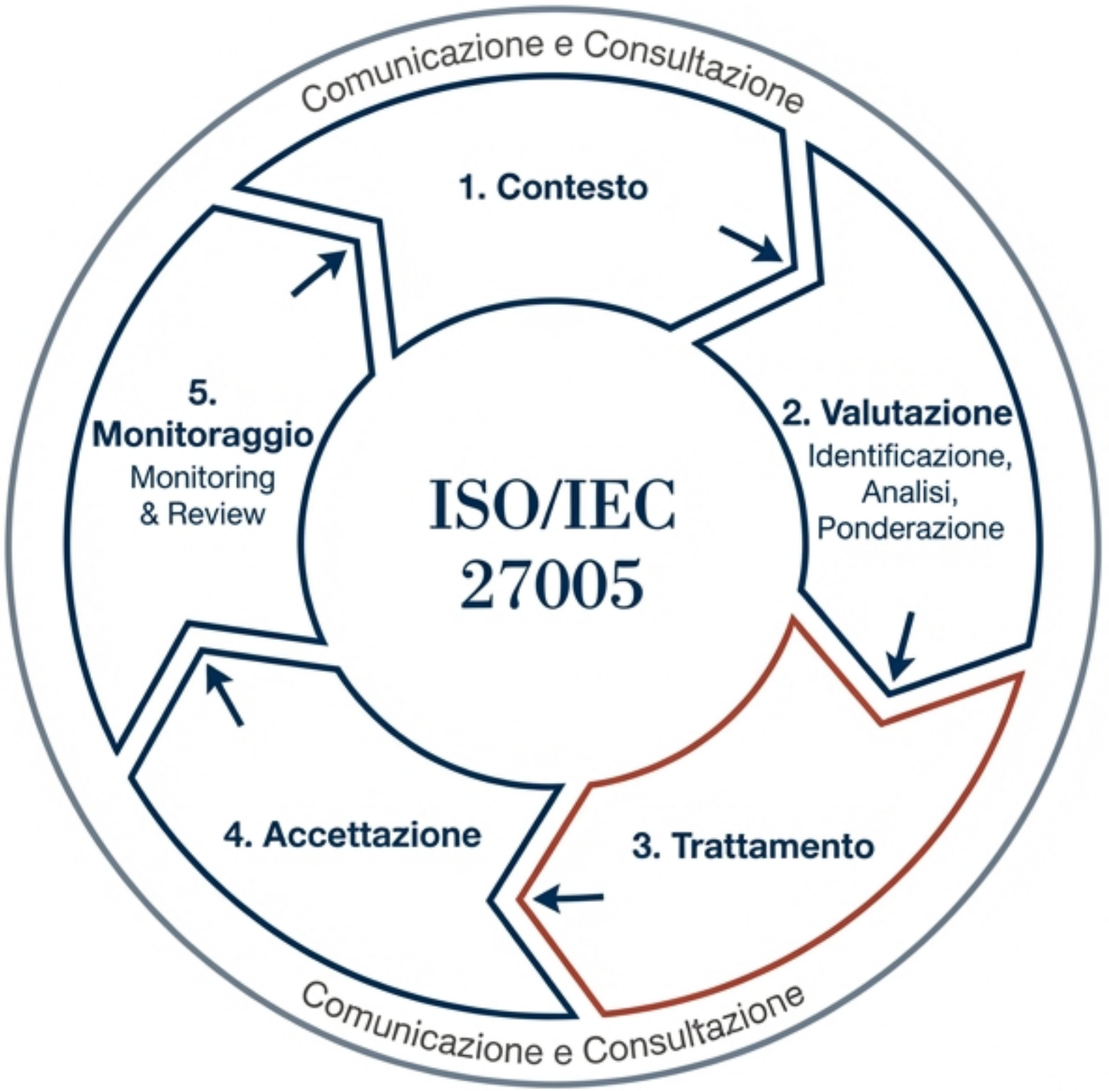
- Focus: Asset-based
- Termine: Impatto
- Struttura: 12 Clausole
- Concetto: Scenario di Incidente

Versione 2022 (Dinamico)

- Focus: Asset-based & Event-based
- Termine: Conseguenza (Consequence)
- Struttura: 10 Clausole (Allineamento ISO 27001)
- Concetto: Scenario di Rischio
- Analisi: Introduzione metodo Semi-quantitativo

Obiettivo 2022: Allineamento con ISO 31000 e passaggio a un processo ciclico.

Il Ciclo di Gestione del Rischio



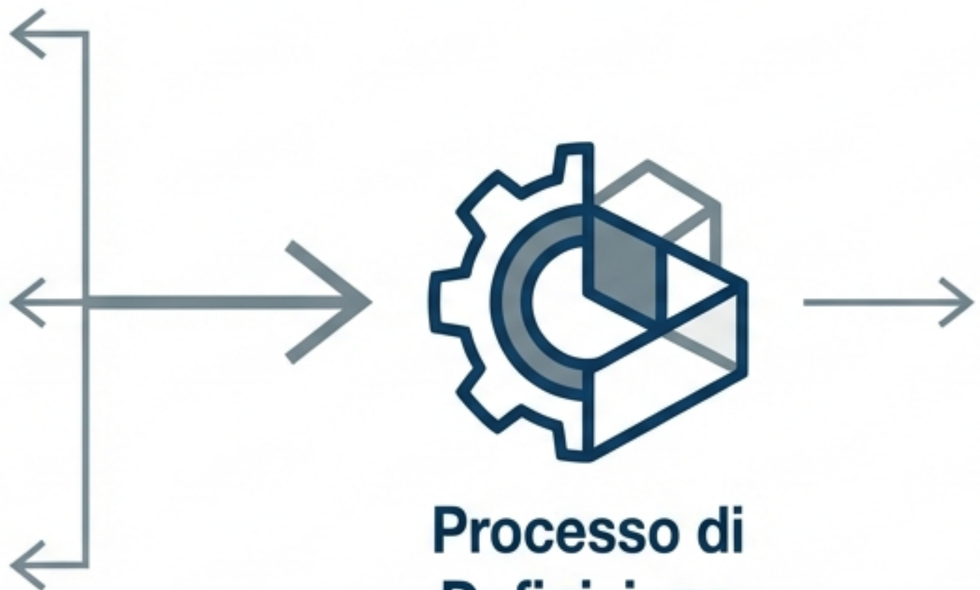
Processo iterativo integrato nel ciclo PDCA.

Stabilire il Contesto (Clausola 6)

Requisiti Legali (GDPR, KVKK)

Obiettivi di Business

Aspettative Stakeholder



Processo di Definizione

1. Criteri di Valutazione:
(Scale di Probabilità e Conseguenza).

2. Criteri di Impatto:
(Danno economico, operativo, reputazionale).

3. Criteri di Accettazione:
(Soglia di tolleranza del rischio).

I criteri devono essere approvati dal management prima della valutazione.

Due Approcci all'Identificazione

Basato sugli Eventi (Event-based)

- Livello Strategico (Top-Down)
- Focus: Scenari globali e obiettivi di business
- Esempio: Attacco Ransomware su scala aziendale

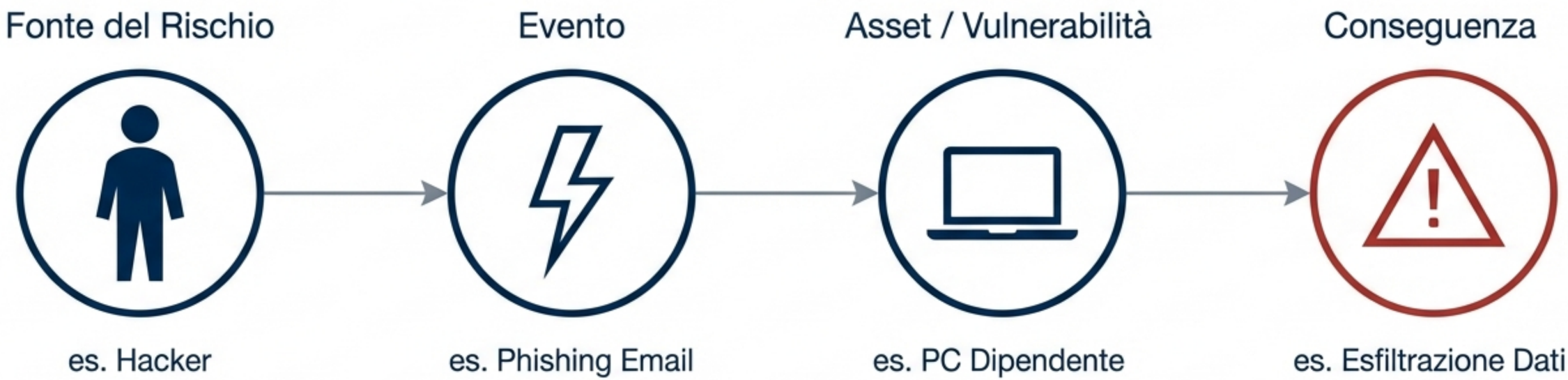
Basato sugli Asset (Asset-based)

- Livello Operativo (Bottom-Up)
- Focus: Vulnerabilità specifiche di hardware e software
- Esempio: Mancato patching del server SQL

ISO 27005:2022 suggerisce la complementarità dei due metodi.

Lo Scenario di Rischio

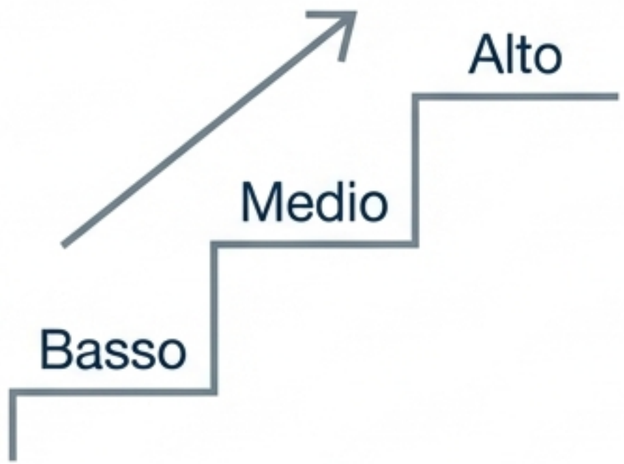
Anatomia del percorso di attacco



Una sequenza o combinazione di eventi che conduce da una causa iniziale a una conseguenza indesiderata.

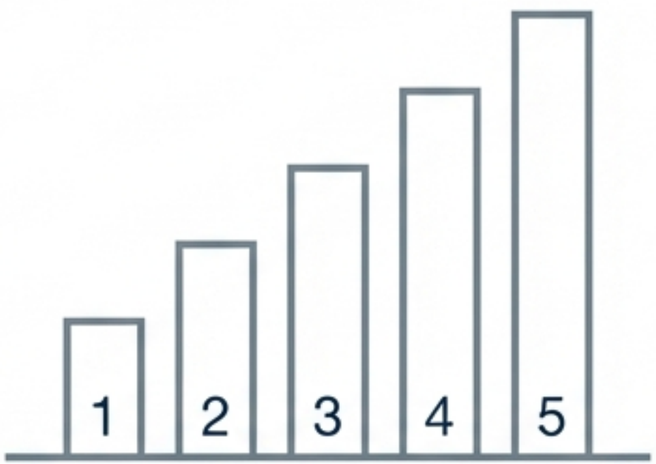
Metodologie di Analisi del Rischio

Qualitativa



- Scala descrittiva
- Veloce ma soggettiva

Semi-Quantitativa

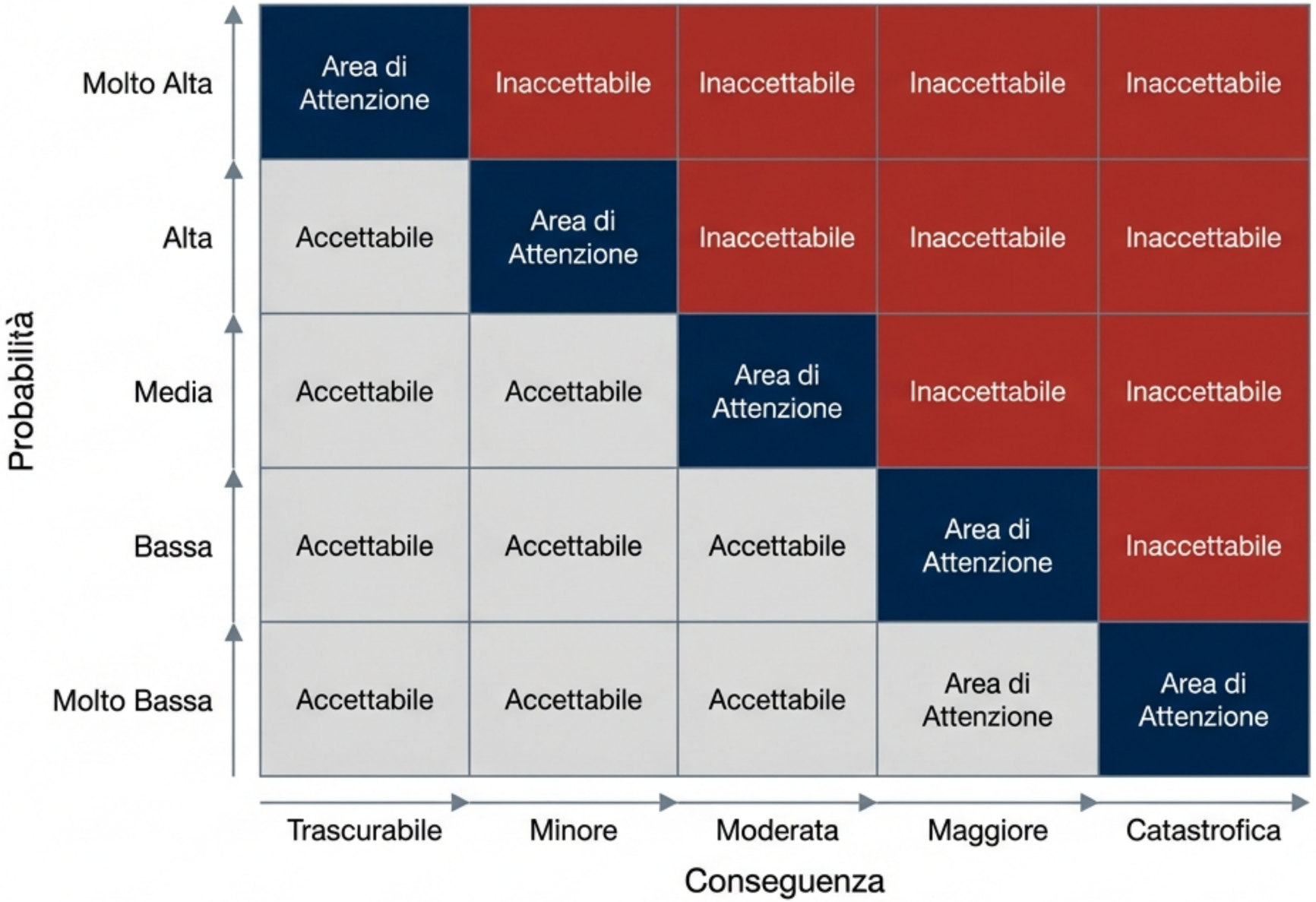


- Scala numerica (1-5) con descrittori
- Compromesso bilanciato (Focus 2022)

Quantitativa

- Valori monetari o percentuali
- Precisa ma richiede dati storici complessi

Valutazione del Rischio: La Matrice



Confronto tra il livello di rischio stimato e i Criteri di Accettazione per determinare la priorità di trattamento.

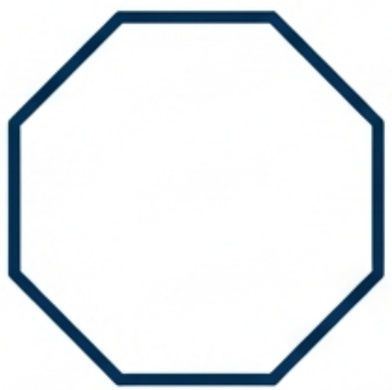
Opzioni di Trattamento (Clausola 8)

Modifica (Mitigazione)

Applicare controlli di sicurezza (ISO 27001 Annex A) per ridurre probabilità o conseguenze.

Ritenzione (Accettazione)

Accettare il rischio consapevolmente (se rientra nei criteri).



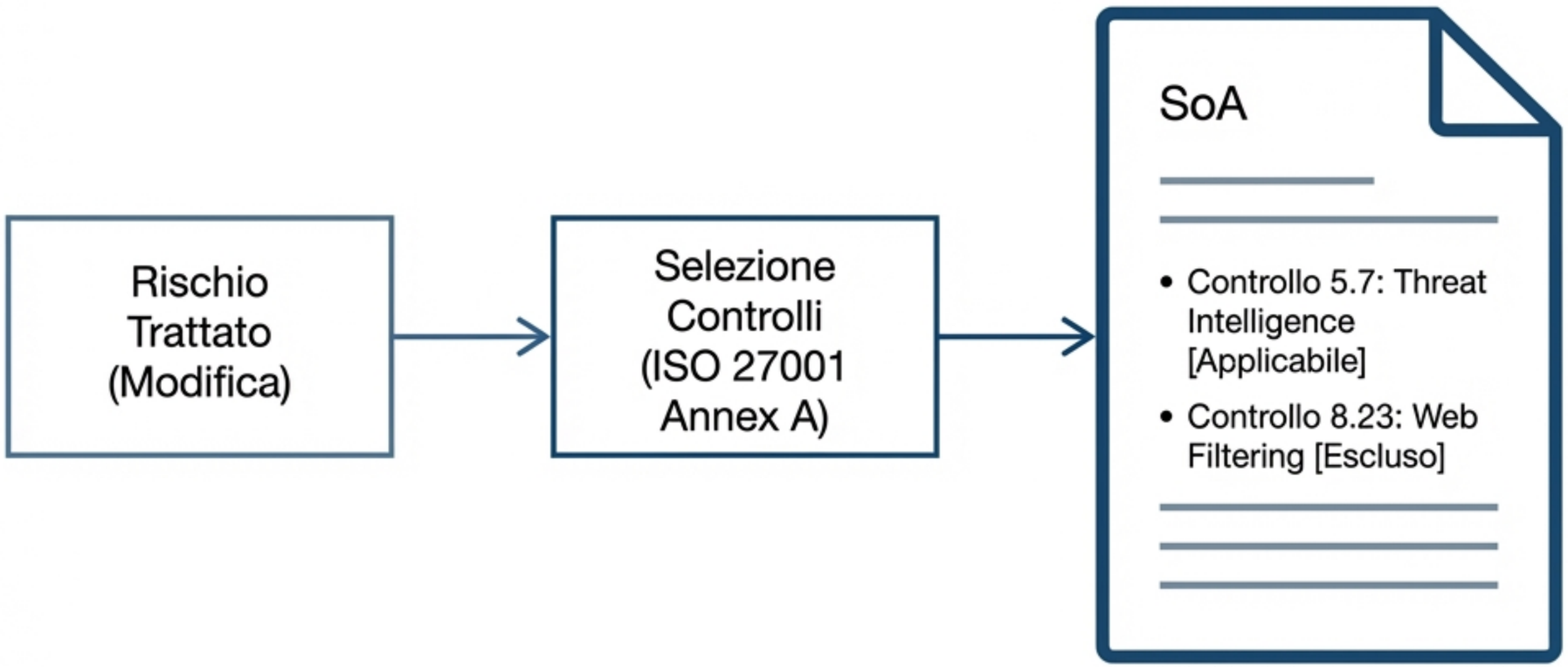
Evitamento

Terminare l'attività o il processo rischioso.

Condivisione (Trasferimento)

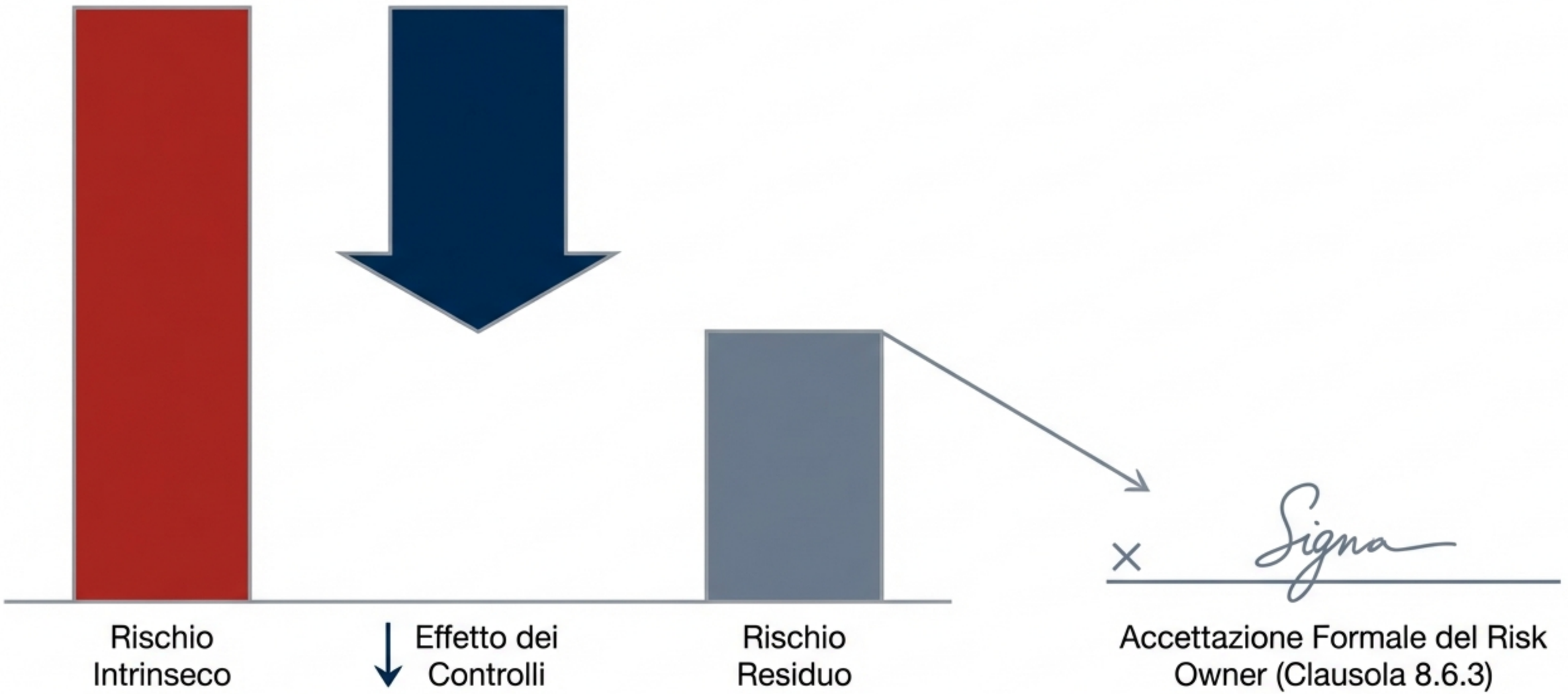
Assicurazioni o outsourcing a terze parti.

Dichiarazione di Applicabilità (SoA)

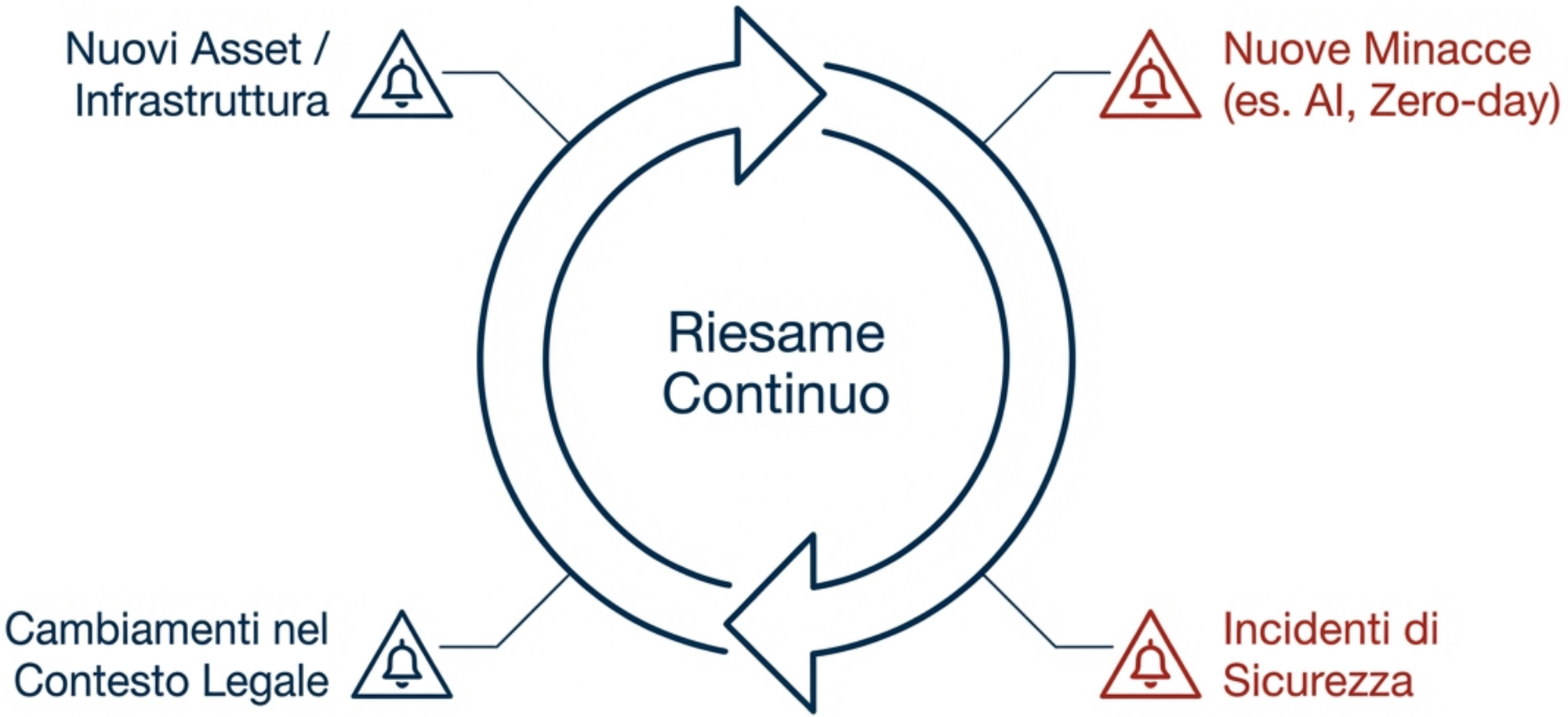


Documento mandatorio che collega i rischi ai controlli e giustifica le inclusioni/esclusioni (ISO 27001 Cl. 6.1.3).

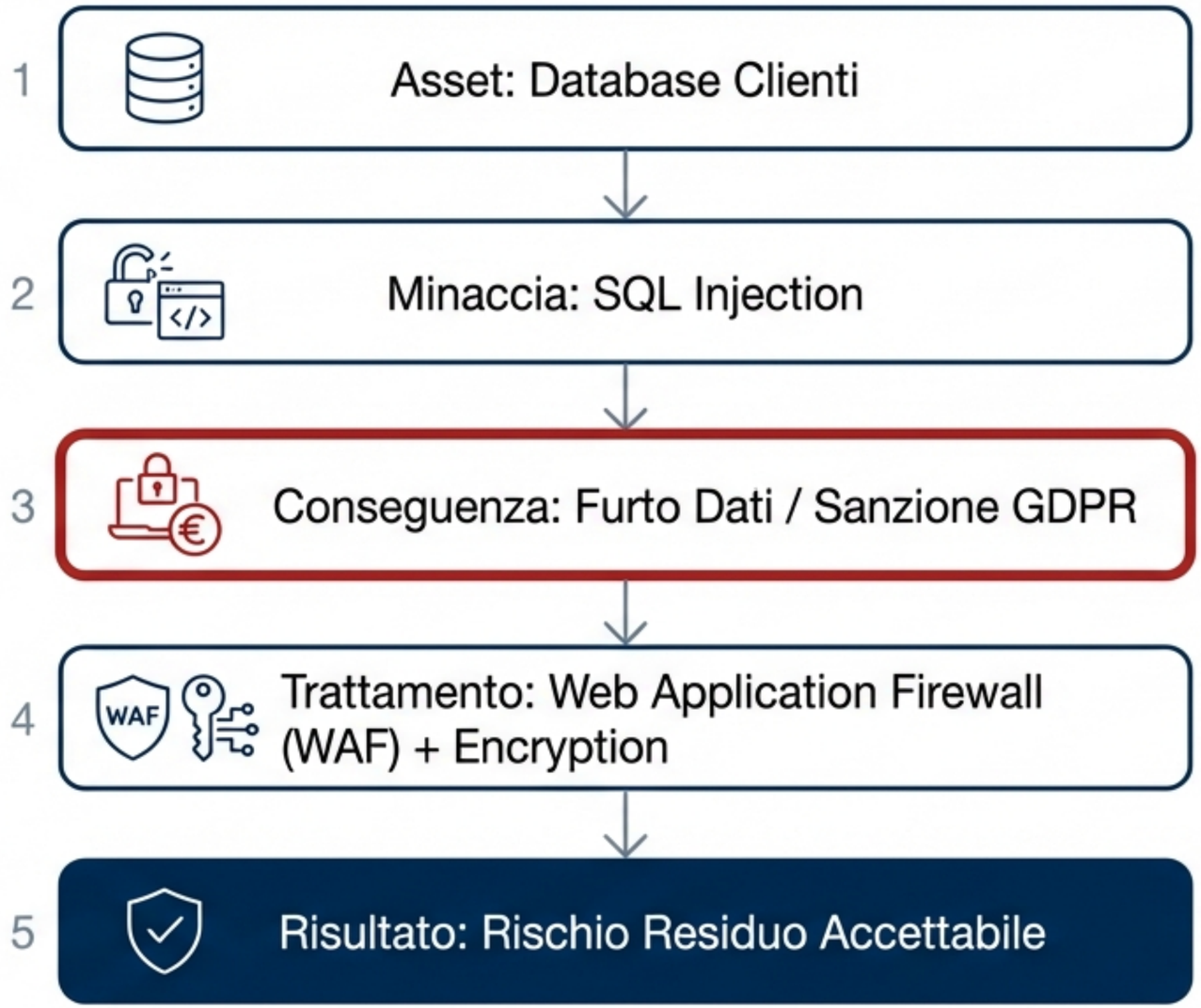
Rischio Residuo e Accettazione



Monitoraggio e Riesame



Caso Studio: Settore E-commerce



Conclusioni e Sintesi Accademica

1. Metodo non Prescrittivo: ISO 27005 definisce il “come”, offrendo flessibilità metodologica.
2. Integrazione Strategica: Ponte tra i requisiti di ISO 27001 e i controlli di ISO 27002.
3. Resilienza Proattiva: Trasformazione della sicurezza in un vantaggio competitivo basato sui dati.
4. Ciclicità: La gestione del rischio è un processo continuo, non un evento singolo.