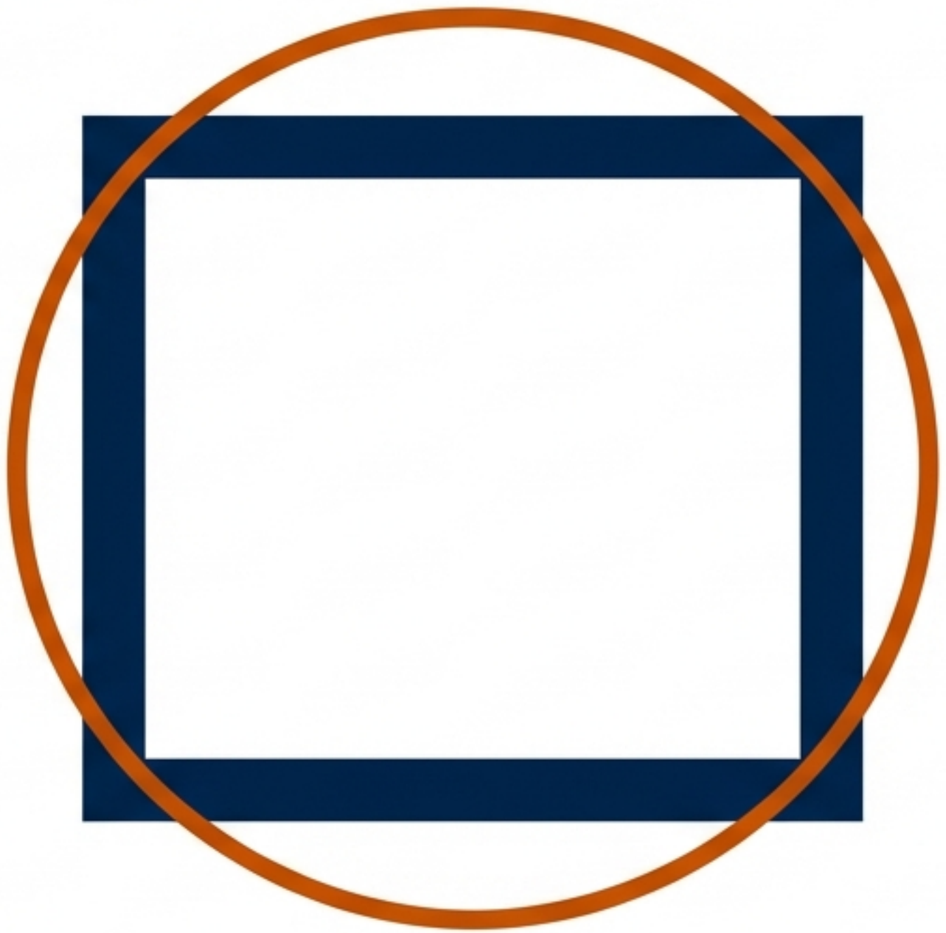
Gestione del Rischio: Fondamenti e Metodologie

Analisi, Valutazione e Standard ISO 31000:2018



Modulo 2 – Principi di Sicurezza delle Informazioni

www.vincenzocalabro.it

Distinzione Terminologica e Concettuale

Risk Management

Il processo globale (macro). Include l"identificazione, le le strategie di governo e il controllo.

Risk Assessment

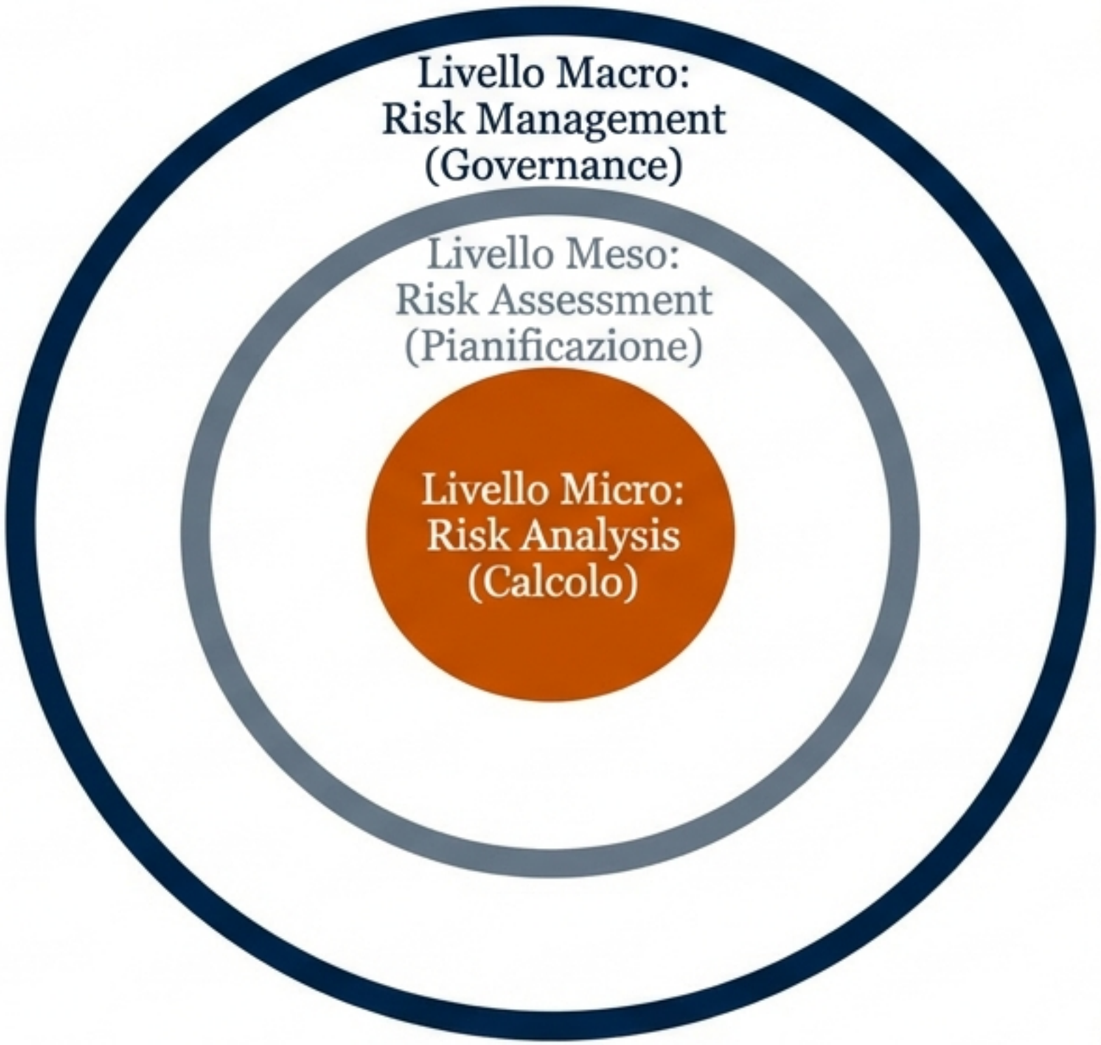
La valutazione (meso). Pianificazione delle misure per ridurre il rischio a un livello accettabile.

Risk Analysis

L'analisi operativa (micro). Il calcolo specifico di probabilità e danno sui beni (assets).

Nel linguaggio comune sono spesso usati come sinonimi, ma in ambito accademico rappresentano perimetri distinti.

La Gerarchia del Rischio: Il Modello a "Contenitore"



Il "Management" è il contenitore globale che racchiude le fasi di valutazione e calcolo operativo.

Livello Micro: L’Analisi del Rischio

Il cuore operativo parte dall’identificazione degli Assets (beni da proteggere).

Rischio = Probabilità × Danno Potenziale

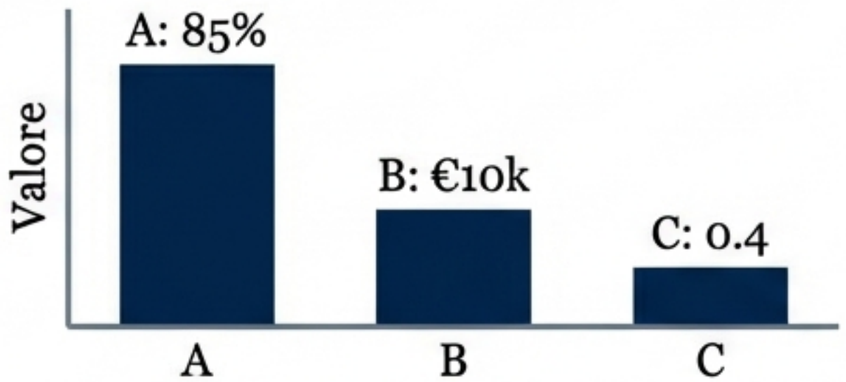
Probabilità: Verosimiglianza dell’evento

Danno Potenziale: Impatto dell’evento

Nota Bene: Il rischio non è mai pari a zero. Nessun sistema è invulnerabile poiché gli attaccanti sono variabili esterne non controllabili.

Metodologie di Trattazione: Quantitativa vs Qualitativa

Approccio Quantitativo



Parametro	Valore
Parametro A	85%
Parametro B	€10k
Parametro C	0.4

Basato su dati numerici e calcoli statistici. Offre concretezza e misurabilità precisa. (Focus del corso)

Approccio Qualitativo

	Prob. Alta	Prob. Media	Prob. Bassa
Impatto Alto	Alto	Alto	Alto
Impatto Medio	Medio	Medio	Medio
Impatto Basso	Basso	Basso	Basso

Basato su descrittori verbali. Più semplice da implementare ma meno concreto.

www.vincenzocalabro.it

Evoluzione Storica e Normativa

Medioevo

Banchieri e Rischio di Credito (Gestione non formalizzata)

Anni '90

Nascita dell’Enterprise Risk Management (ERM)

Oggi

GDPR & Normative Privacy

La parola ‘Rischio’ appare ~75 volte nel testo del regolamento.

Lo Standard ISO 31000:2018

Definizione

Linee guida per una metodologia efficiente.

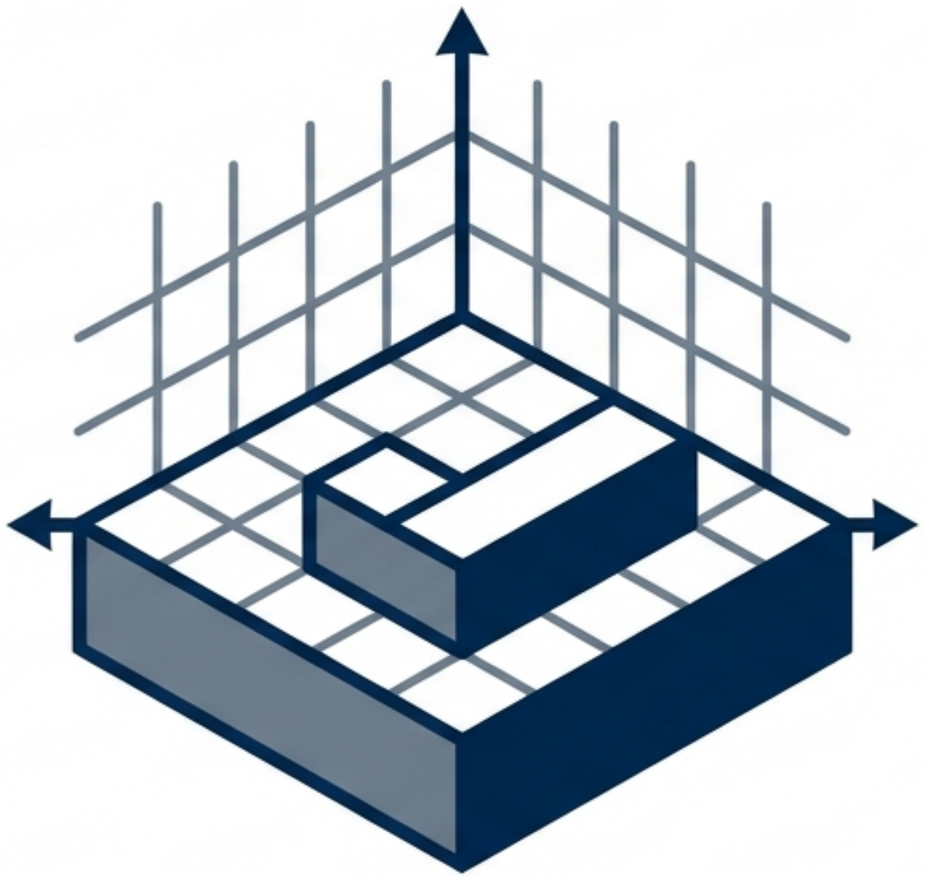
Cosa vs Come

Lo standard definisce COSA fare (le fasi del processo), ma non impone COME farlo (nessun algoritmo matematico specifico).

Esempio

La norma richiede una ‘Valutazione del Rischio’, ma lascia all’organizzazione la scelta del metodo di calcolo.

Fase 1: Stabilire il Contesto (Context Establishment)



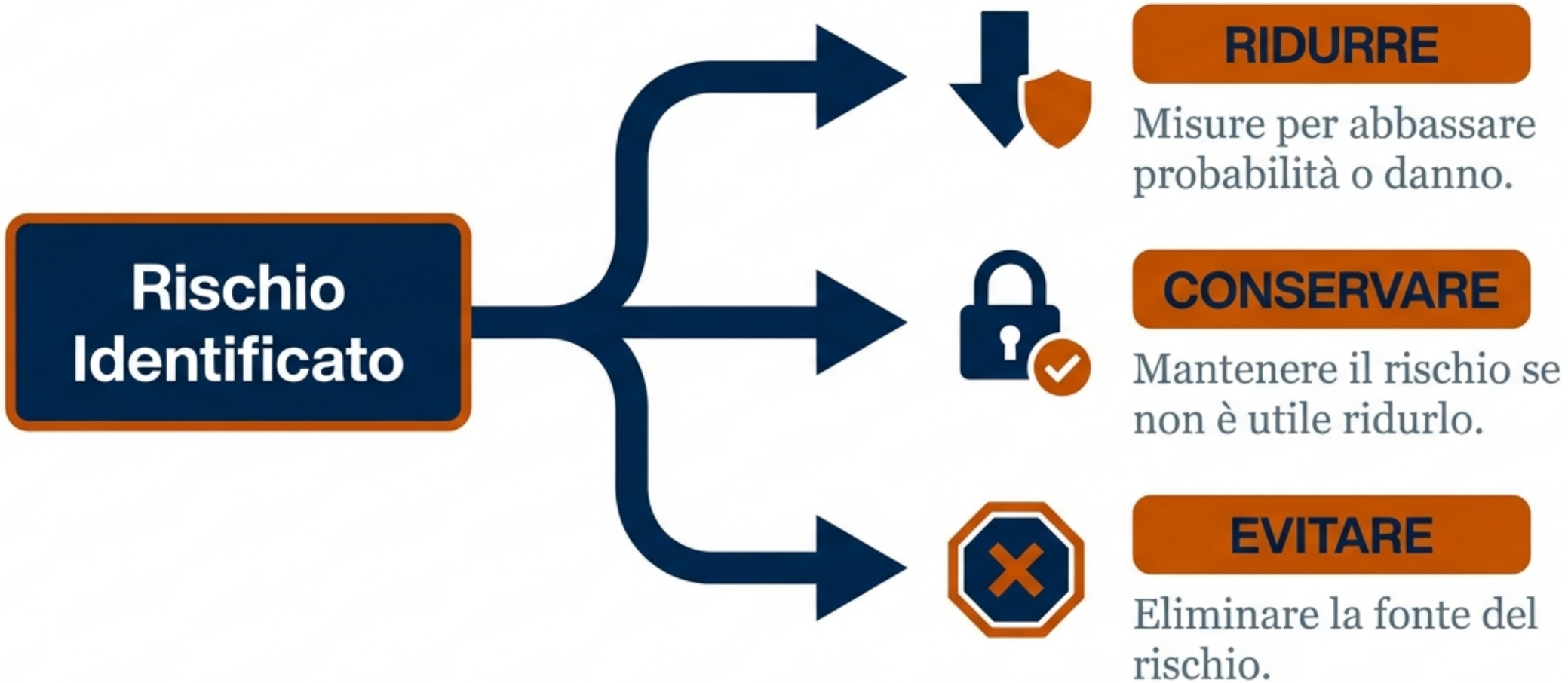
- Scopo e obiettivi dell’analisi
- Strumenti e tecniche da utilizzare
- Definizione dei Criteri di Accettazione

È fondamentale definire in anticipo quale livello di rischio è tollerabile.

Fase 2: Valutazione del Rischio (Risk Assessment)

Lo scopo è quantificare i rischi per decidere quali azioni hanno la priorità, basandosi sui criteri della Fase 1.

Fase 3: Trattamento del Rischio (Risk Treatment)



Il piano include controlli per verificare l’efficacia delle misure.

www.vincenzocalabro.it

Fase 4: Accettazione del Rischio (Risk Acceptance)

Firma Autorizzata

Decisione formale di accettare i rischi residui.

- Definizione delle responsabilità (Accountability).
- Elenco dei rischi consapevolmente accettati.
- Giustificazione formale (basata sui criteri della Fase 1).

Attività Trasversale: Comunicazione del Rischio

Non è solo un report finale. È uno scambio parallelo a tutte le fasi.

Principio: Scripta Manent (Documentazione essenziale per turnover e audit).

Attività Trasversale: Monitoraggio e Revisione

Obiettivo: Testare e migliorare l’efficacia del processo.

Attività Continue:

- Pianificare e raccogliere dati.
- Registrare risultati.
- Fornire feedback per il ciclo successivo.

www.vincenzocalabro.it

La Natura Iterativa del Processo

La norma ISO 31000 non è una checklist lineare. L'uscita del processo alimenta nuovamente la definizione del contesto per adattarsi ai cambiamenti.

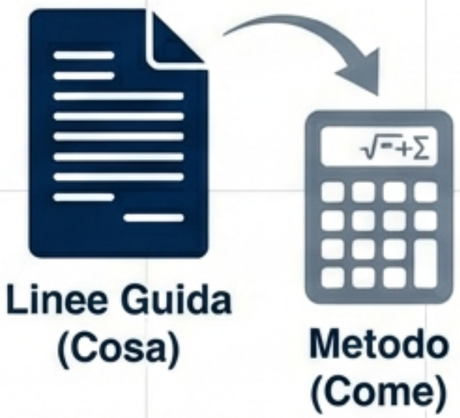
Punti Chiave del Modulo

1. Terminologia

Management, Assessment e Analysis sono concetti distinti e gerarchici.

2. Rischio ≠ 0

Il rischio non può mai essere eliminato totalmente; esiste sempre un rischio residuo.



3. Ruolo ISO 31000

Fornisce il ‘cosa’ (linee guida) ma lascia libero il ‘come’ (calcolo).

4. Ciclicità

La gestione del rischio è un processo continuo, non un evento singolo.