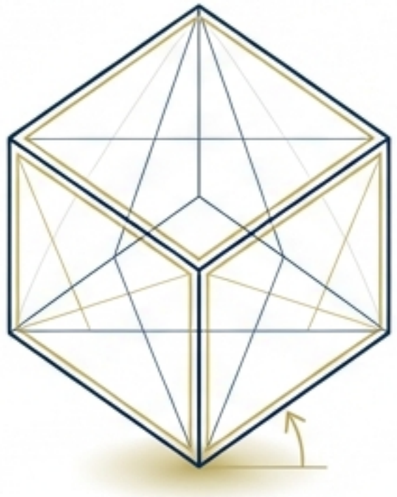


ISO 31000:2018 – Linee Guida per la Gestione del Rischio

Analisi dei Principi, della Struttura e del Processo

Modulo 3: Gestione del Rischio e Normative Internazionali

Definizione e Natura dello Standard

Origine

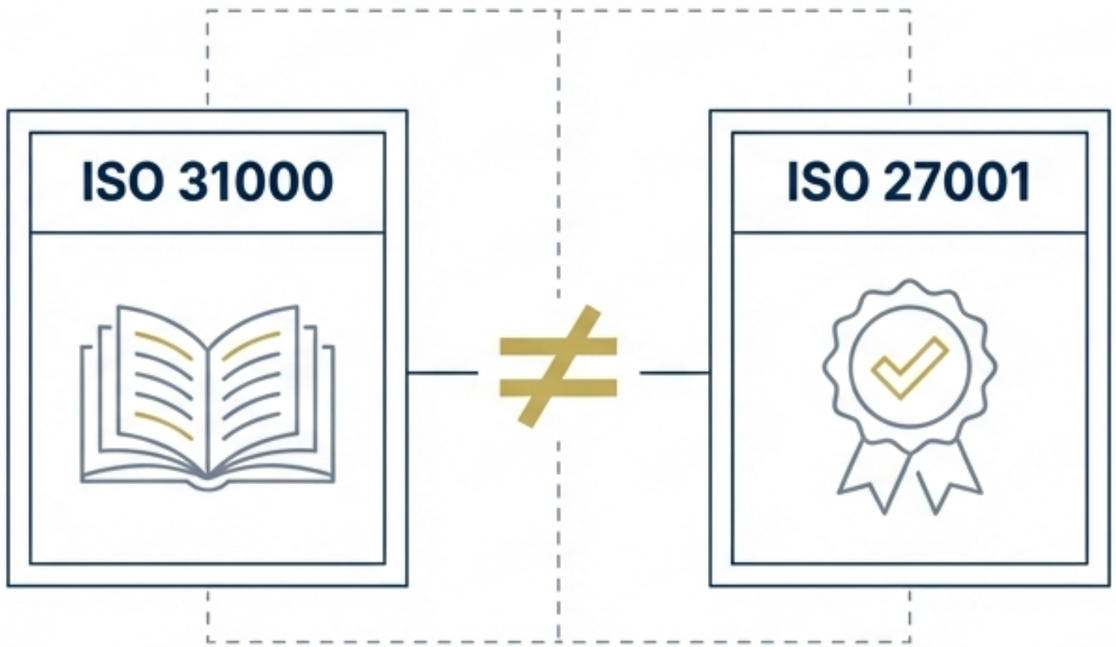
Erogata dall'International Organization for Standardization (ISO). La versione attuale (2018) aggiorna e modernizza la release del 2009.

Obiettivo

Fornire un approccio strutturato e sistematico per individuare, prevenire e gestire i rischi, permettendo alle organizzazioni di prendere decisioni informate.

Linee Guida vs. Certificazione

A differenza della ISO 27001, la ISO 31000:2018 non è uno standard certificabile. Essa fornisce raccomandazioni per l'implementazione di un sistema efficiente, utile anche in processi di audit, ma non finalizzato al rilascio di un certificato formale.



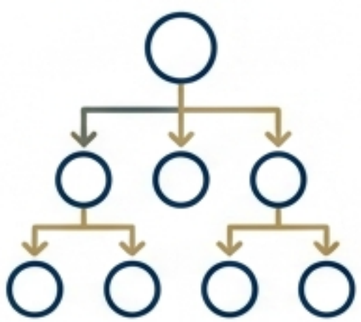
Applicabilità Universale e Destinatari

Per chi è

Applicabile a qualsiasi organizzazione, indipendentemente dal settore (pubblico/privato), dalla dimensione o dalla complessità.

Tipologia di Rischio

Non si limita al rischio informatico (cyber risk), ma copre qualsiasi tipologia di rischio che possa influenzare il raggiungimento degli obiettivi.



Stakeholder

Si rivolge a chiunque "crei e protegga valore": dal top management ai responsabili operativi, includendo l'interazione con soggetti terzi (investitori, stakeholder).

Ciclo di Vita

Non è una "fotografia" statica, ma una guida da utilizzare durante tutto il ciclo di vita dell'ente.

Il Fondamento Teorico: Ciclo di Deming (PDCA)

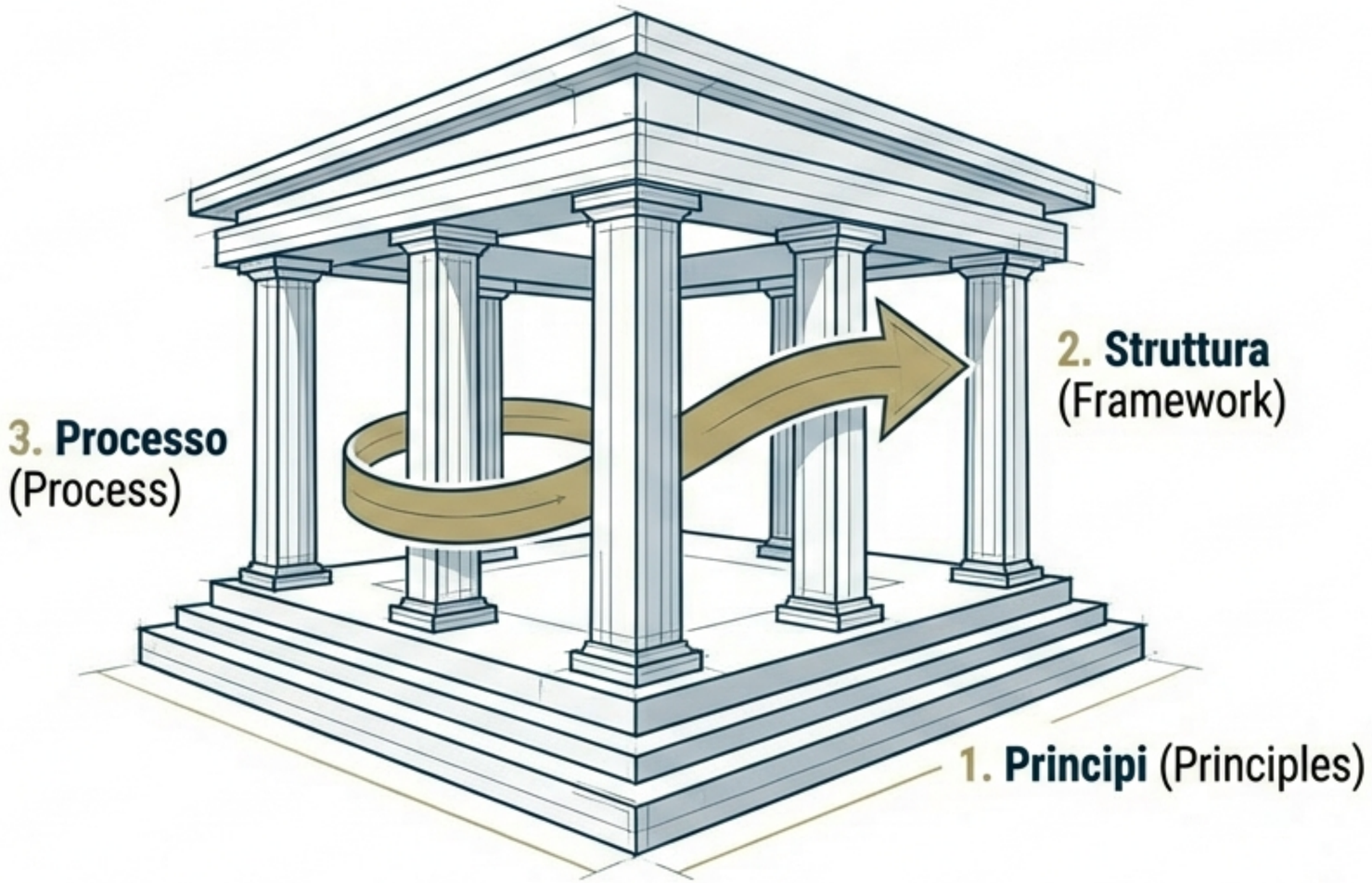
Metodologia

La ISO 31000 basa la sua ciclicità sul modello di gestione iterativo proposto da Deming.

Obiettivo

Garantire un miglioramento continuo dei processi e della qualità, promuovendo un'interazione costante tra strategia e operatività per l'utilizzo ottimale delle risorse.

L’Architettura della ISO 31000: I Tre Pilastri



Overview

La norma si regge su tre componenti fondamentali che ordinano il passaggio da concetti generali a regole pratiche.

- **Principi:** Le fondamenta. Definiscono le caratteristiche essenziali (creazione e protezione del valore).
- **Struttura:** Lo scheletro organizzativo. Assiste l’integrazione della gestione del rischio nella governance.
- **Processo:** La fase operativa. L’applicazione pratica delle politiche di gestione.

Obiettivo sistemico: **Gestire gli effetti dell'incertezza sugli obiettivi aziendali.**

I Principi: Evoluzione e Sintesi (2009 vs 2018)

ISO 31000:2009

(Elenco di 11 Principi)

- Elementi ispiratori
- Concetti dettagliati

ISO 31000:2018

Sintesi

Si passa da 11 principi a 8. La sostanza non cambia, ma i concetti sono stati sintetizzati e raggruppati.

Core Concept

Al centro del sistema vi è la “Creazione e Protezione del Valore”. La tabella del 2009 funge da elenco di elementi ispiratori per gli attuali 8 principi; una convergenza concettuale verso la sintesi.

Analisi dei Principi: Requisiti Strutturali

Integrata (Integrated)

La gestione del rischio non è un'attività isolata, ma parte integrante di tutte le attività organizzative.

Strutturata ed Esaustiva (Structured)

Richiede un approccio rigoroso per garantire risultati coerenti e comparabili.

Personalizzata (Customized)

Le regole devono essere adattate ("customizzate") al contesto specifico dell'organizzazione (obiettivi, dimensione, cultura).

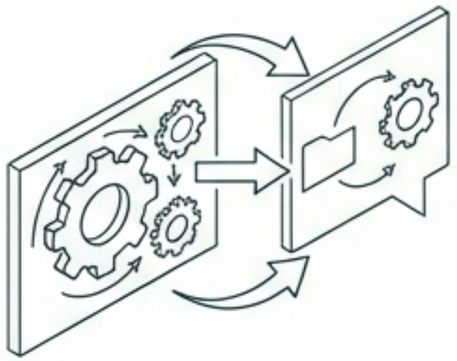
Inclusiva (Inclusive)

Deve coinvolgere tutti gli stakeholder, dal management all'ultimo dipendente. Il "punto debole" può risiedere ovunque, quindi nessuno può essere trascurato.

Analisi dei Principi: Fattori Dinamici e Umani

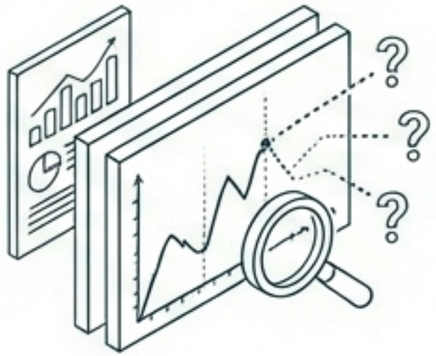
Dinamica (Dynamic)

Il sistema deve adattarsi ai cambiamenti interni ed esterni. Le policy non possono rimanere statiche per anni dato che i rischi evolvono velocemente.



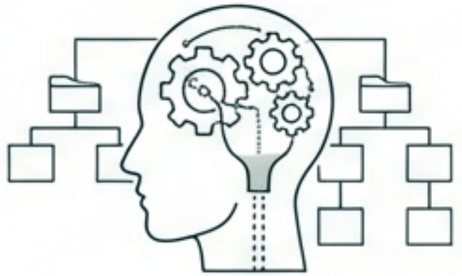
Migliori Informazioni Disponibili (Best Available Information)

Le decisioni devono basarsi su dati storici, attuali e previsioni previsioni future, pur considerando i limiti dell'incertezza.



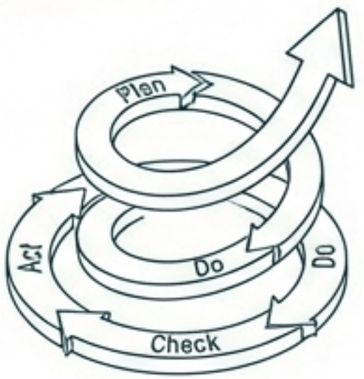
Fattori Umani e Culturali (Human and Cultural Factors)

Riconoscimento che l'uomo è spesso il "collo di bottiglia". Il comportamento e la cultura aziendale influenzano signifi-cativamente l'efficacia della gestione del rischio.

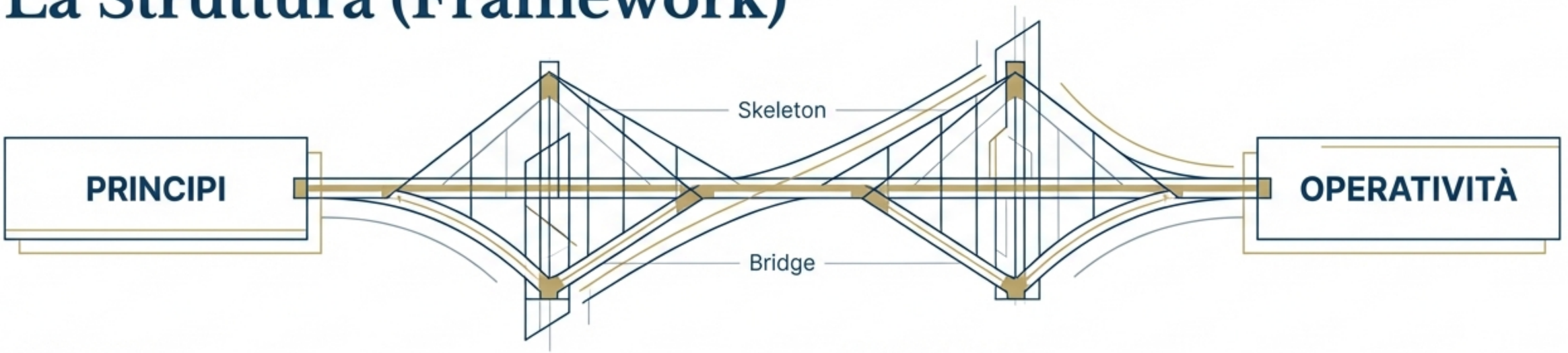


Miglioramento Continuo (Continuous Improvement)

Il sistema deve essere verificato e perfezionato regolarmente tramite l'apprendimento e l'esperienza.



Il Secondo Pilastro:
La Struttura (Framework)



Funzione

La struttura assiste l'organizzazione nell'integrare la gestione del rischio nelle sue funzioni significative. È il "ponte" tra i principi e l'operatività.

Governance

L'efficacia dipende direttamente dall'integrazione nei processi decisionali e di governance.

Mandato (Top Management)

Richiede il supporto attivo del Top Management. La sicurezza non può essere un semplice "addendum", ma deve permeare la strategia aziendale.

Gap Analysis

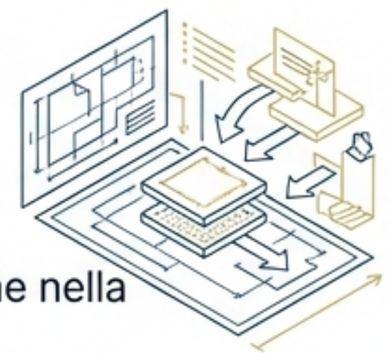
L'organizzazione deve valutare le pratiche esistenti, identificare le debolezze e indirizzarle tramite la struttura.

Fasi della Struttura: Integrazione e Progettazione

Fase 1: Integrazione (Integration)

- Comprensione della struttura esatta dell'azienda e del suo contesto.
- Il management definisce la strategia generale e assegna le responsabilità primarie.

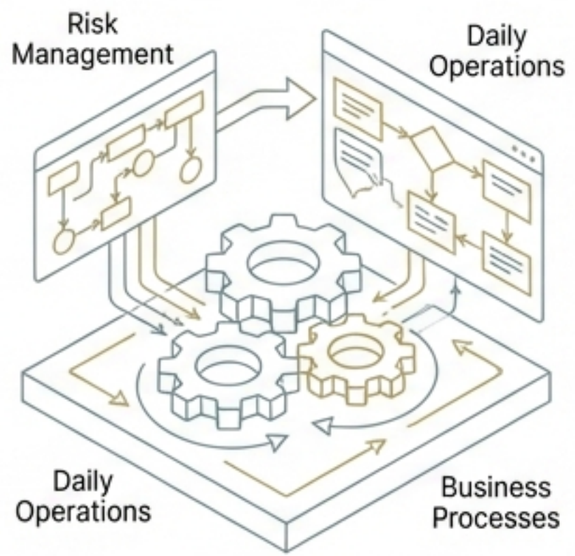
Fase 2: Progettazione (Design)



- Impegno formale della direzione nella gestione del rischio.
- Allocazione delle risorse necessarie.
- Chiarimento della strategia e assegnazione dei ruoli a tutti i dipendenti.
- Considerazione dei fattori interni ed esterni che influenzano l'incertezza.

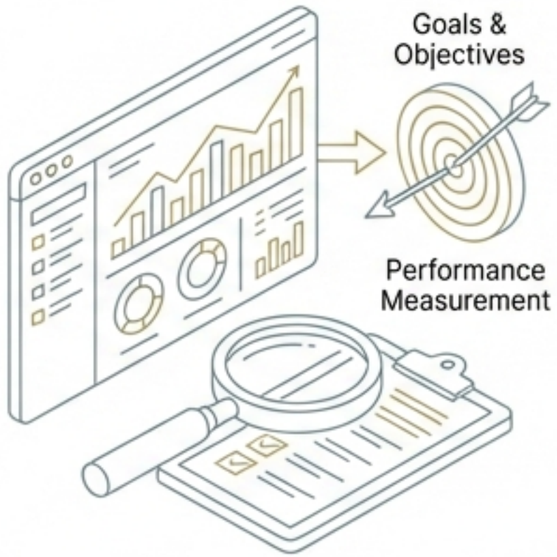
Fasi della Struttura: Implementazione, Valutazione e Miglioramento

Fase 3: Implementazione (Implementation)



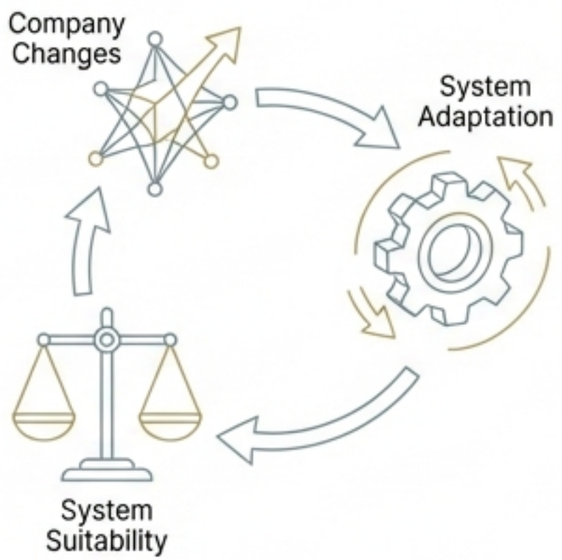
- Modifica dei processi aziendali per includere la gestione del rischio nel lavoro quotidiano.
- Obiettivo: accettazione fluida ("smooth") da parte dei dipendenti.

Fase 4: Valutazione (Evaluation)



- Esecuzione regolare di verifiche (audit) per misurare l'efficacia rispetto agli obiettivi prefissati.
- Garanzia di efficienza a lungo termine.

Fase 5: Miglioramento (Improvement)



- Adattamento dinamico ai cambiamenti dell'azienda.
- Revisioni periodiche per garantire che il sistema rimanga idoneo nel tempo.

Il Terzo Pilastro: Il Processo Operativo

Definizione
Rappresenta la fase operativa in cui le politiche definite nella Struttura vengono applicate concretamente.

Continuità
Se i Principi sono le fondamenta e la Struttura è lo scheletro, il Processo è l'azione.

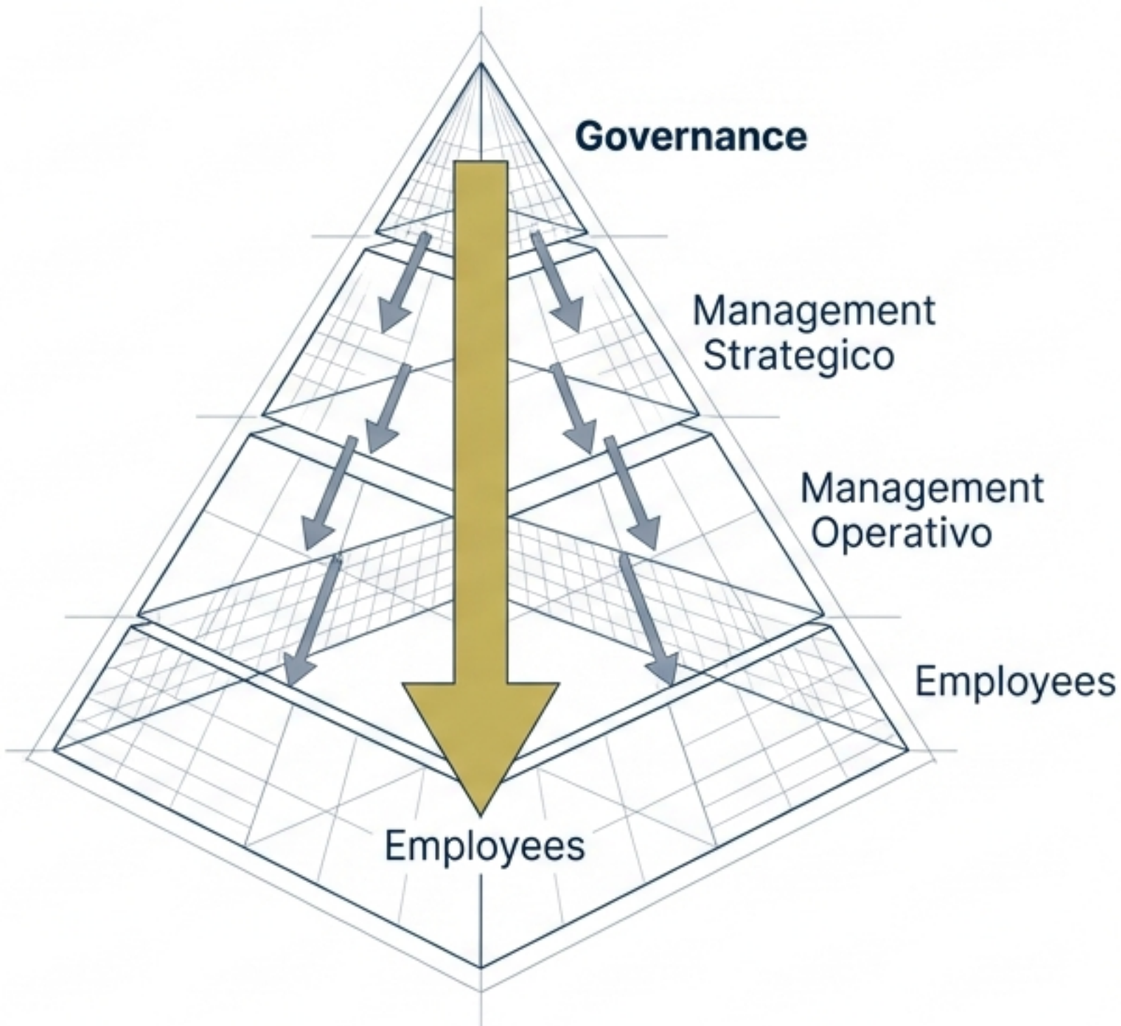
Riferimento
(Come discusso nel Modulo 2) Il processo include l'identificazione, l'analisi, la ponderazione e il trattamento del rischio. Anche il processo segue la logica iterativa e ciclica definita dal framework.

La Centralità della Governance (Approccio Top-Down)

Responsabilità
La gestione del rischio parte dall'alto. È il management che prende l'iniziativa e organizza il sistema avvalendosi di esperti.

Uniformità
Un approccio Top-Down garantisce che la cultura del rischio sia uniforme in tutta l'organizzazione e non frammentata.

Decision Making
Il processo decisionale deve essere informato dai rischi a tutti i livelli, ma la direzione strategica è unica.



Sintesi del Modello Gestionale ISO 31000

- **Natura Iterativa:** Non una "fotografia" statica, ma un ciclo continuo basato sul PDCA.
- **Approccio Olistico**: Integrazione completa tra principi (valore), struttura (governance) e processo (azione).
- **Adattabilità:** Necessità di dinamismo per affrontare la velocità di evoluzione dei rischi (specialmente nel contesto cyber).
- **Fattore Umano:** L'importanza critica di includere la cultura aziendale e il comportamento umano nell'equazione del rischio.

Riferimenti Bibliografici e Normativi

- **ISO 31000:2018** - Risk management — Guidelines. International Organization for Standardization.
- **ISO 31000:2009** - Risk management — Principles and guidelines.
- **Il Ciclo di Deming (PDCA):** Plan, Do, Check, Act – Fondamenti di gestione della qualità.