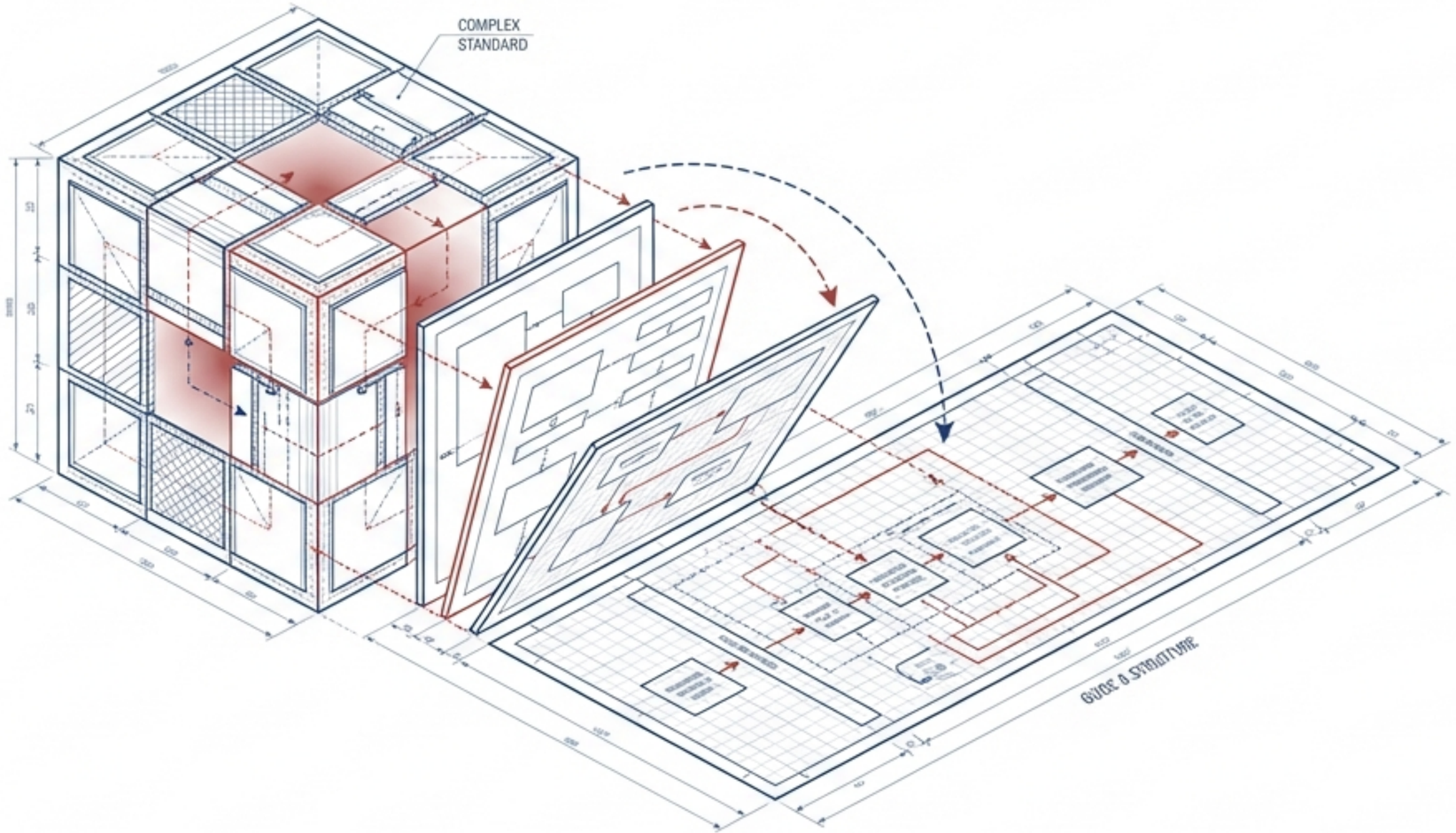
ISO/IEC 27003:2017

Guida all'Implementazione del SGSI

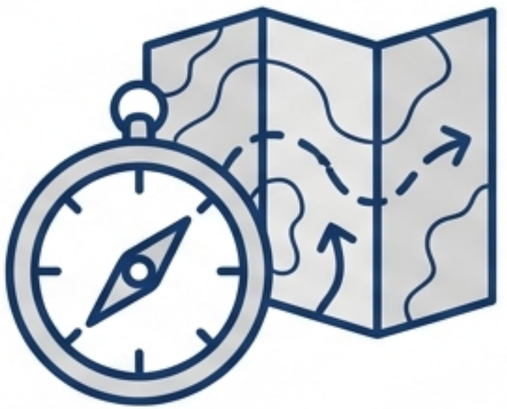
Linee guida per i Sistemi di Gestione della Sicurezza delle Informazioni



Scopo e Ruolo della Norma ISO 27003

ISO 27001 (Requisiti)

- Cosa fare
- Normativa Certificabile
- Mandatorio

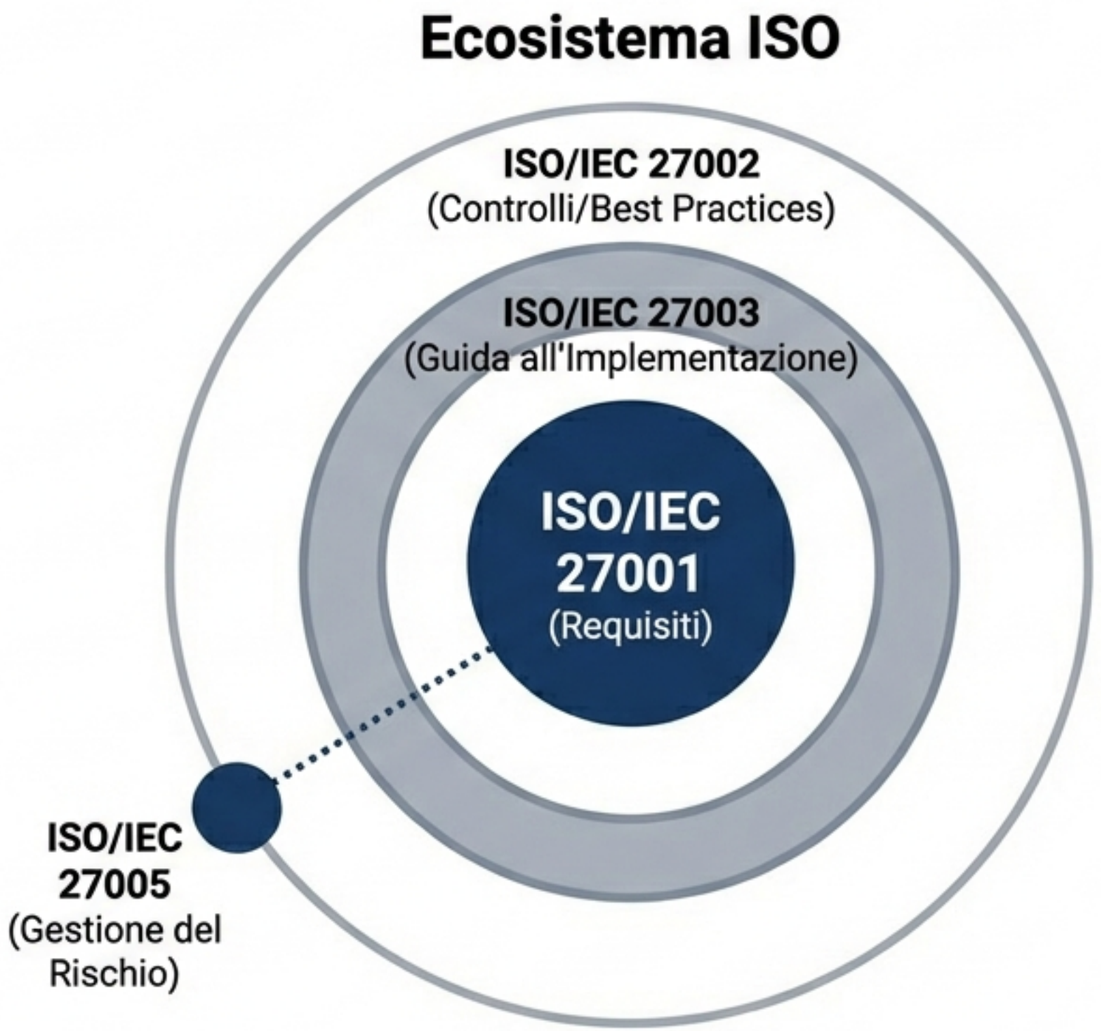


ISO 27003 (Guida Pratica)

- Come farlo
- Norma di Orientamento
- Raccomandazioni (‘dovrebbe’, ‘può’)

Obiettivo: Tradurre i requisiti rigidi in processi operativi adattabili a organizzazioni di ogni dimensione.

L’Ecosistema della Famiglia ISO 27000



ISO 27001	Il Gold Standard. Certificabile.
ISO 27003	Metodologia di progetto. Il “Ponte” verso l’operatività.
ISO 27002	Catalogo dei controlli (Annex A).

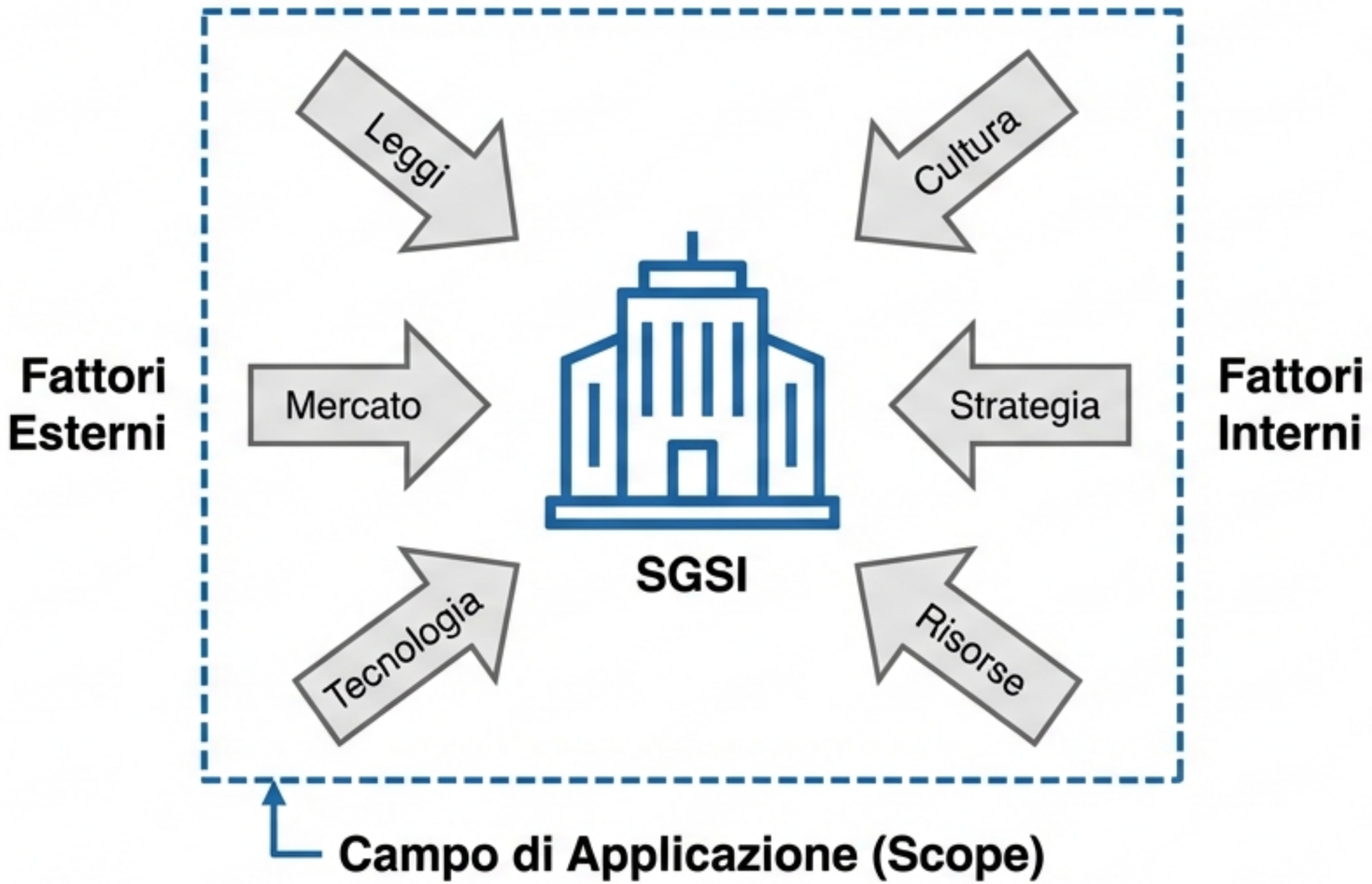
Struttura e Allineamento Normativo

Allineamento delle Clausole (ISO 27001 & ISO 27003)

ISO 27003 rispecchia esattamente la struttura della 27001.

- Clausola 4: Contesto
- Clausola 5: Leadership
- Clausola 6: Pianificazione
- Clausola 7: Supporto
- Clausola 8: Attività Operative
- Clausola 9: Valutazione
- Clausola 10: Miglioramento

Clausola 4: Contesto dell'Organizzazione



Passo Critico: Definizione dello Scope.

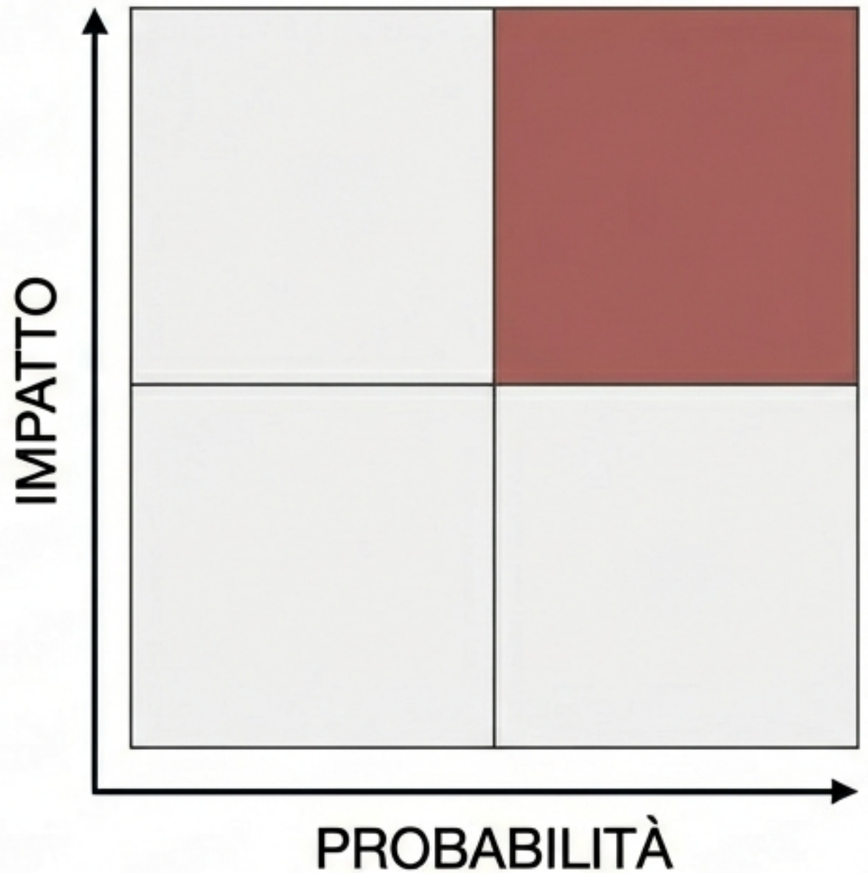
Analisi delle Parti Interessate: Clienti, Regolatori, Dipendenti.

Attenzione: Evitare uno scope troppo ampio (spreco) o troppo stretto (rischi non gestiti).

Clausola 5: Leadership e Impegno

Errore Comune: Senza un impegno attivo della direzione, il SGSI diventa un mero esercizio burocratico.

Clausola 6: Pianificazione e Gestione del Rischio



Mitigare
(Controlli)

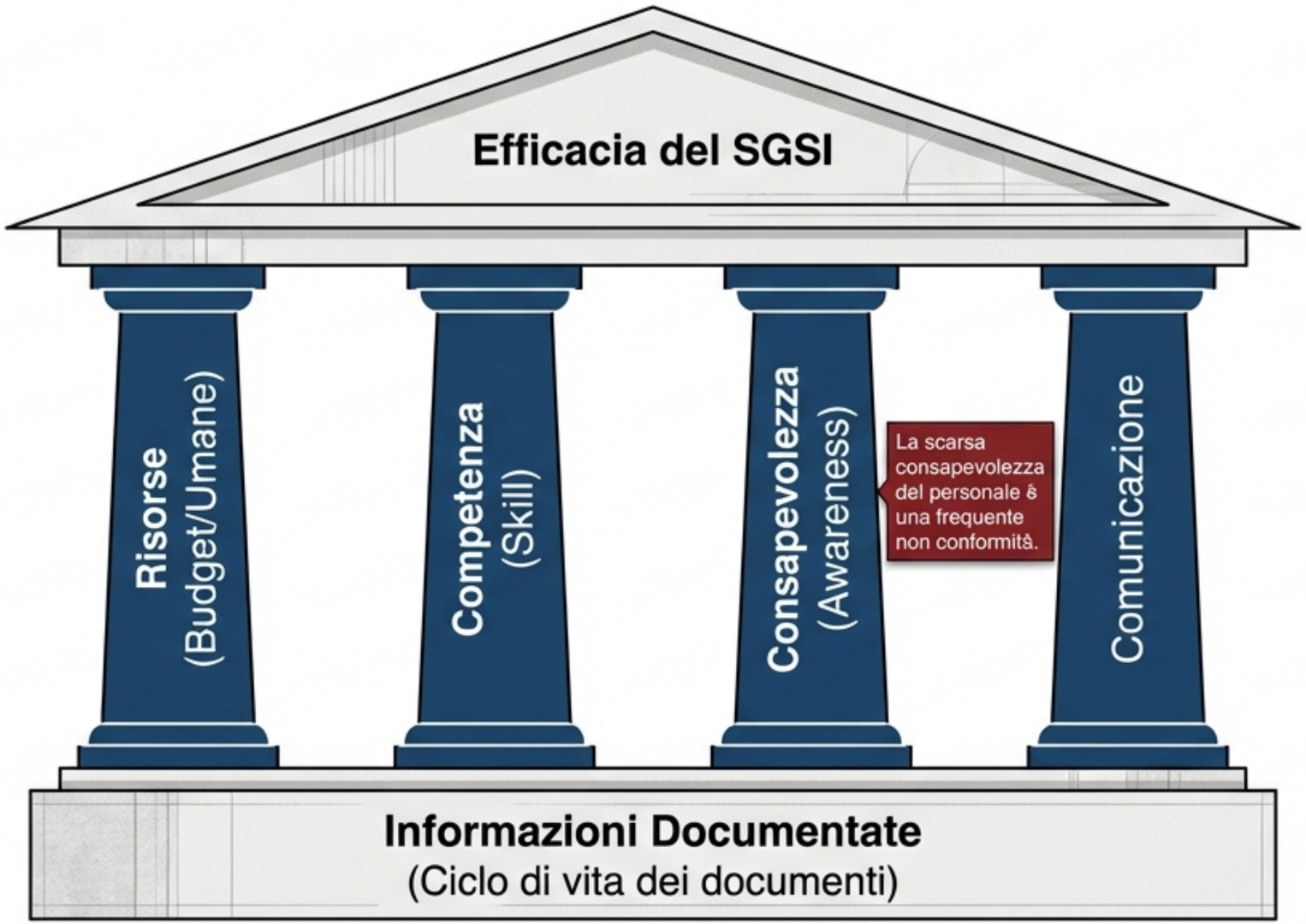
Trasferire
(Assicurazione)

Accettare
(Risk Appetite)

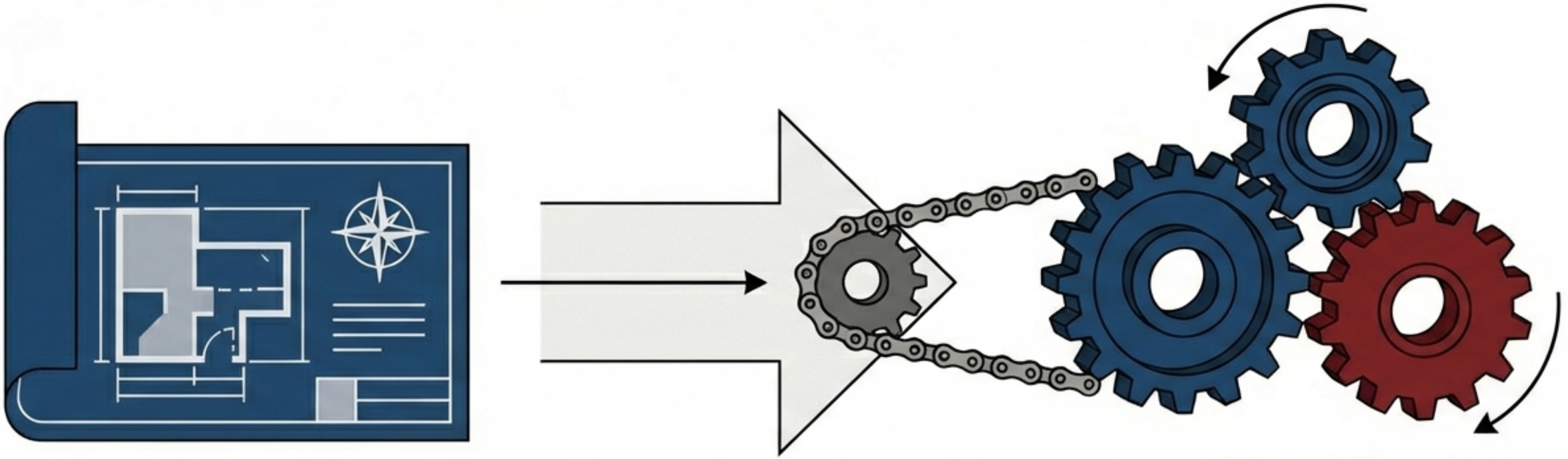
Evitare
(Cessare attività)

Output Chiave: Dichiarazione di Applicabilità (Statement of Applicability - SoA)

Clausola 7: Supporto e Risorse



Clausola 8: Attività Operative

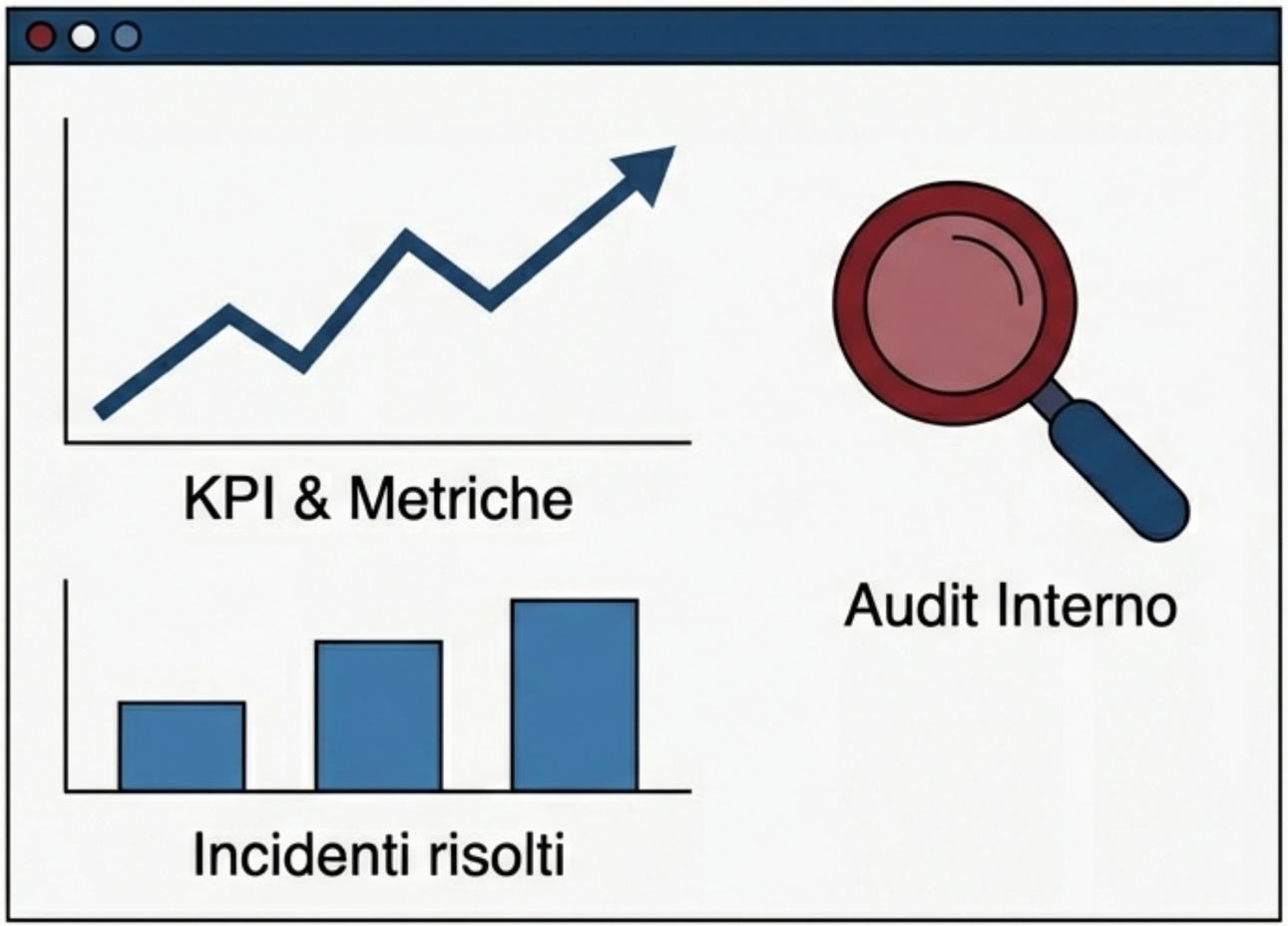


Pianificazione
(Clausola 6)

Esecuzione
(Clausola 8)

- **Pianificazione e Controllo Operativo**
- Valutazione dei Rischi periodica
- Gestione dei Fornitori (Supply Chain Security)

Clausola 9: Valutazione delle Prestazioni



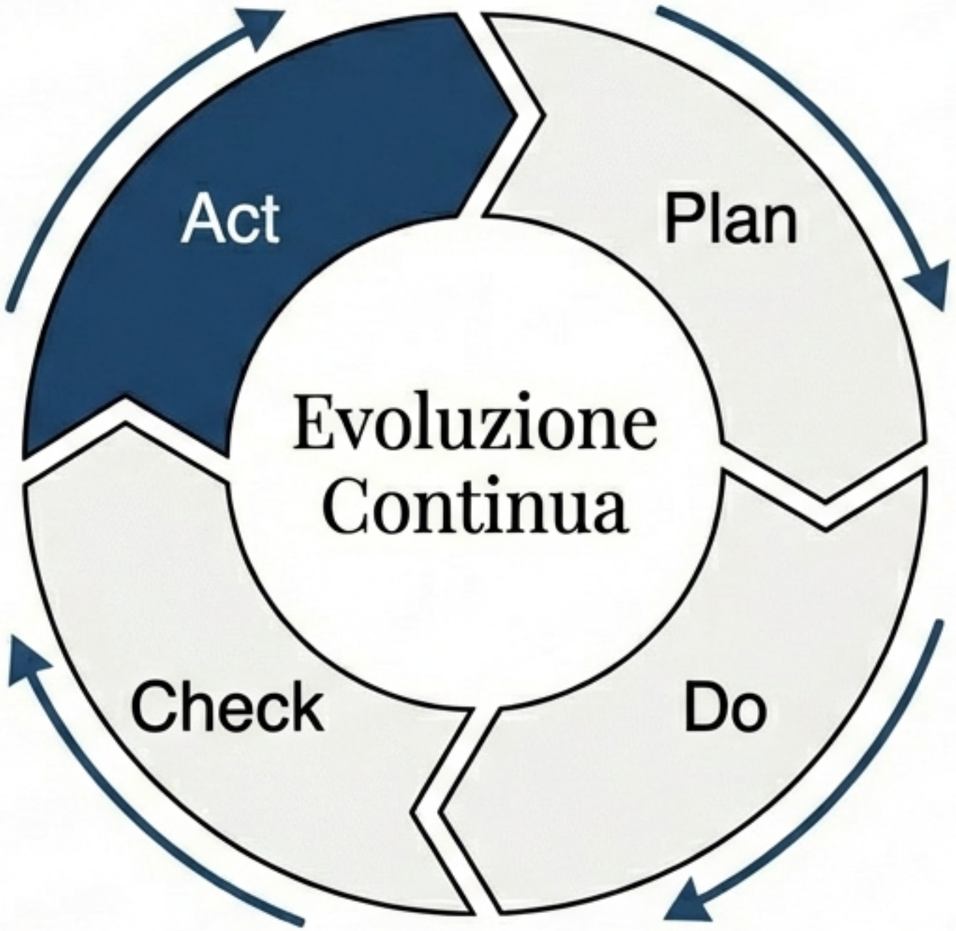
Monitoraggio: Definire metriche misurabili.

Audit Interno: Verifiche indipendenti di conformità.

Riesame della Direzione: Valutazione strategica dell’efficacia.

Fallimento comune:
Mancanza di metriche definite.

Clausola 10: Miglioramento



- Gestione delle Non Conformità
- Azioni Correttive (Root Cause Analysis)
- Adattamento a nuove minacce

Metodologia di Implementazione a Fasi

Helvetica Now: Un approccio strutturato di Project Management per la conformità.

Errori Comuni e Non Conformità


Scope Errato: Troppo ampio o troppo stretto.


SoA Debole: Giustificazioni vaghe per l’esclusione dei controlli.


Inventario Asset Obsoleto: Mancanza di proprietari definiti.


Metriche Assenti: Gestione basata su intuizioni, non dati.


Shadow IT: Mancanza di controllo su servizi cloud e fornitori.

Valore Strategico della Guida ISO 27003

Accelerazione

Riduce i tempi di implementazione e ambiguità.

Resilienza

Focus su sicurezza reale, non solo compliance.

Fiducia

Facilita la certificazione e e rassicura i clienti.

Allineamento strategico tra sicurezza e obiettivi di business.

Playfair Display

Conclusioni: Dalla Teoria alla Pratica

Requisiti (27001)

Helvetica Now

Sicurezza Operativa

- ISO 27003 è la mappa per navigare la complessità.
- Obiettivo: Costruire un SGSI efficace e sostenibile.
- Reference: ISO/IEC 27003:2017 Information technology — Security techniques.

Helvetica Now

Domande & Approfondimenti