

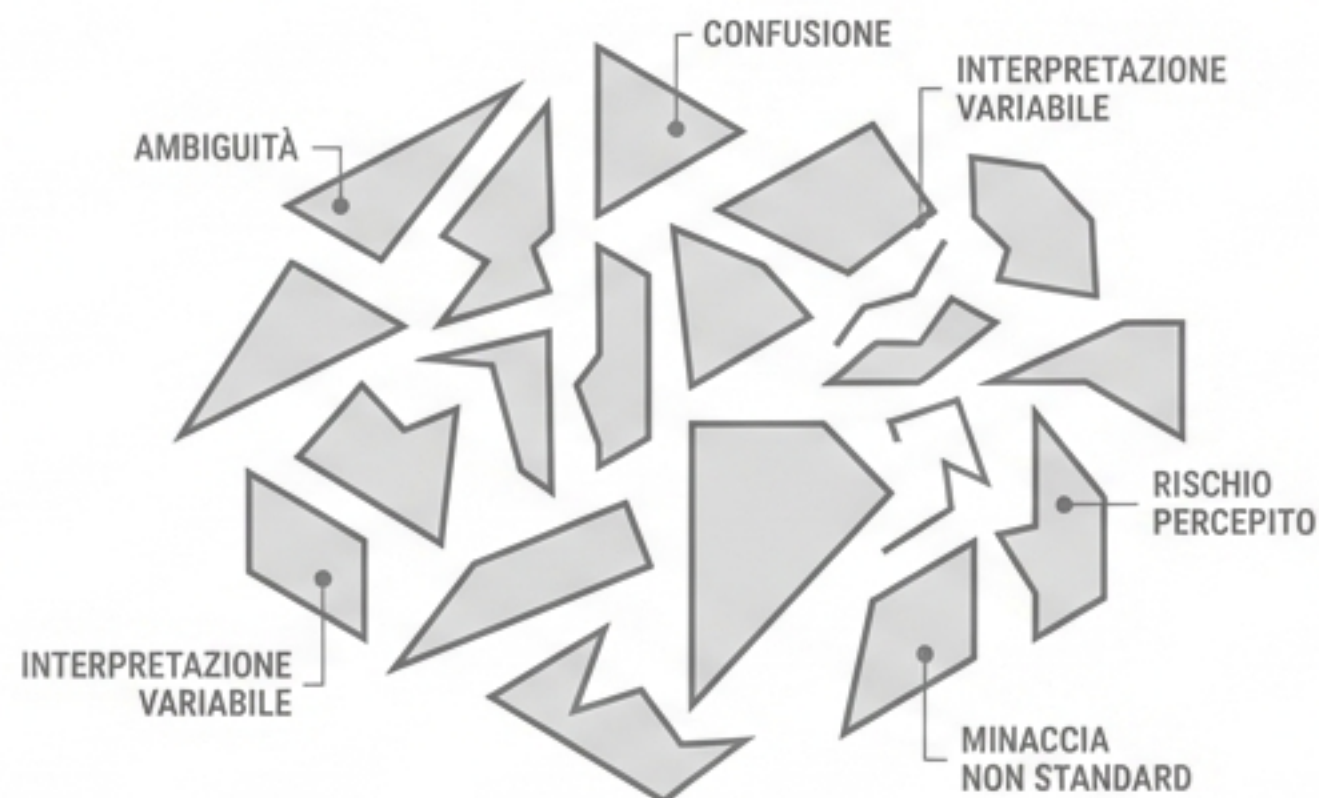
ISO/IEC 27000:2018

Tecniche di sicurezza — Sistemi di gestione
della sicurezza delle informazioni —
Panoramica e vocabolario



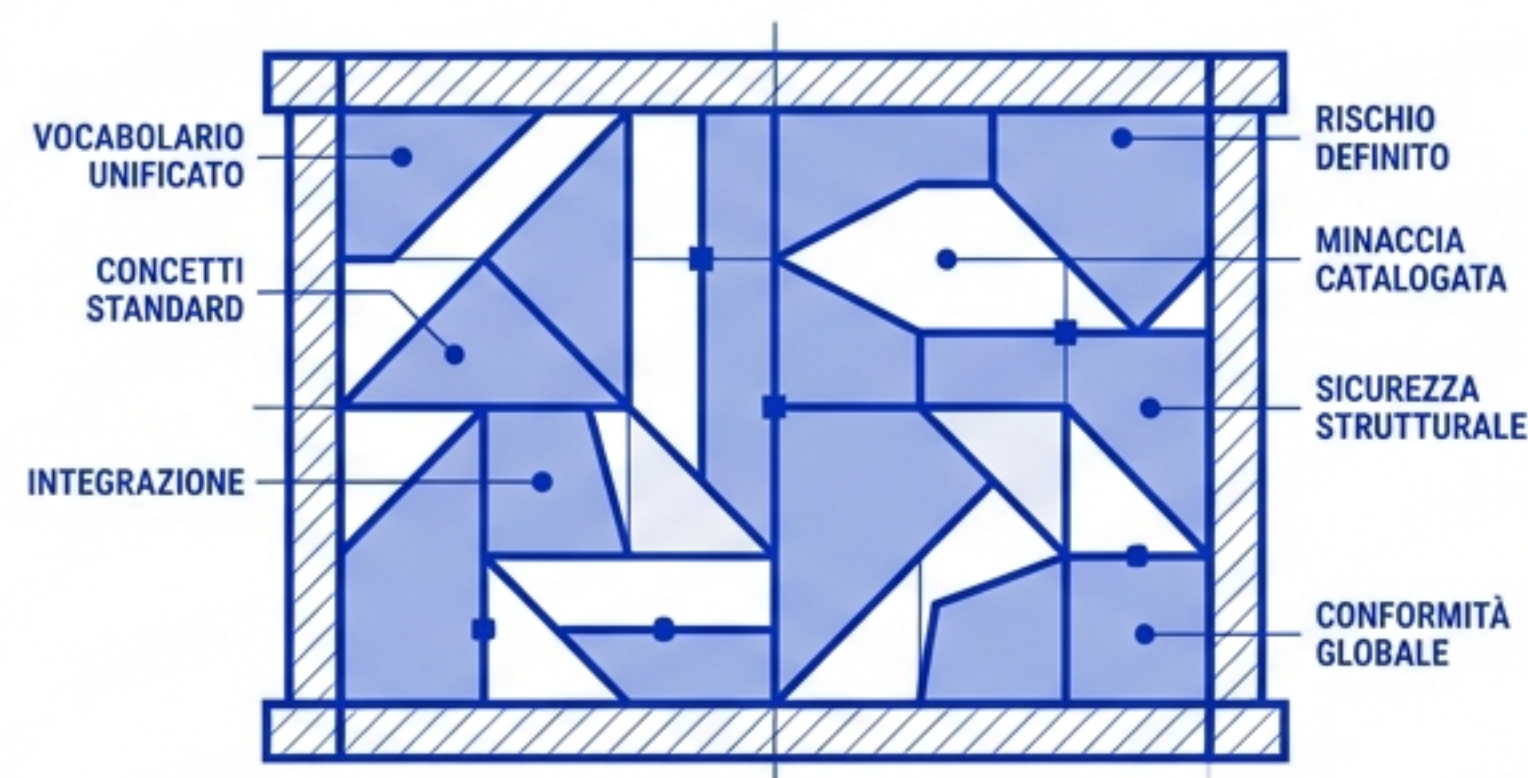
La Necessità di un Linguaggio Comune

Il Problema



DEFINIZIONI CAOTICHE E SCONNESSE

La Soluzione (ISO 27000)



LINGUA FRANCA GLOBALE PER LA SICUREZZA DELLE INFORMAZIONI

Il Problema

Senza definizioni standard, termini come "rischio" o "minaccia" creano ambiguità tra organizzazioni e confini.

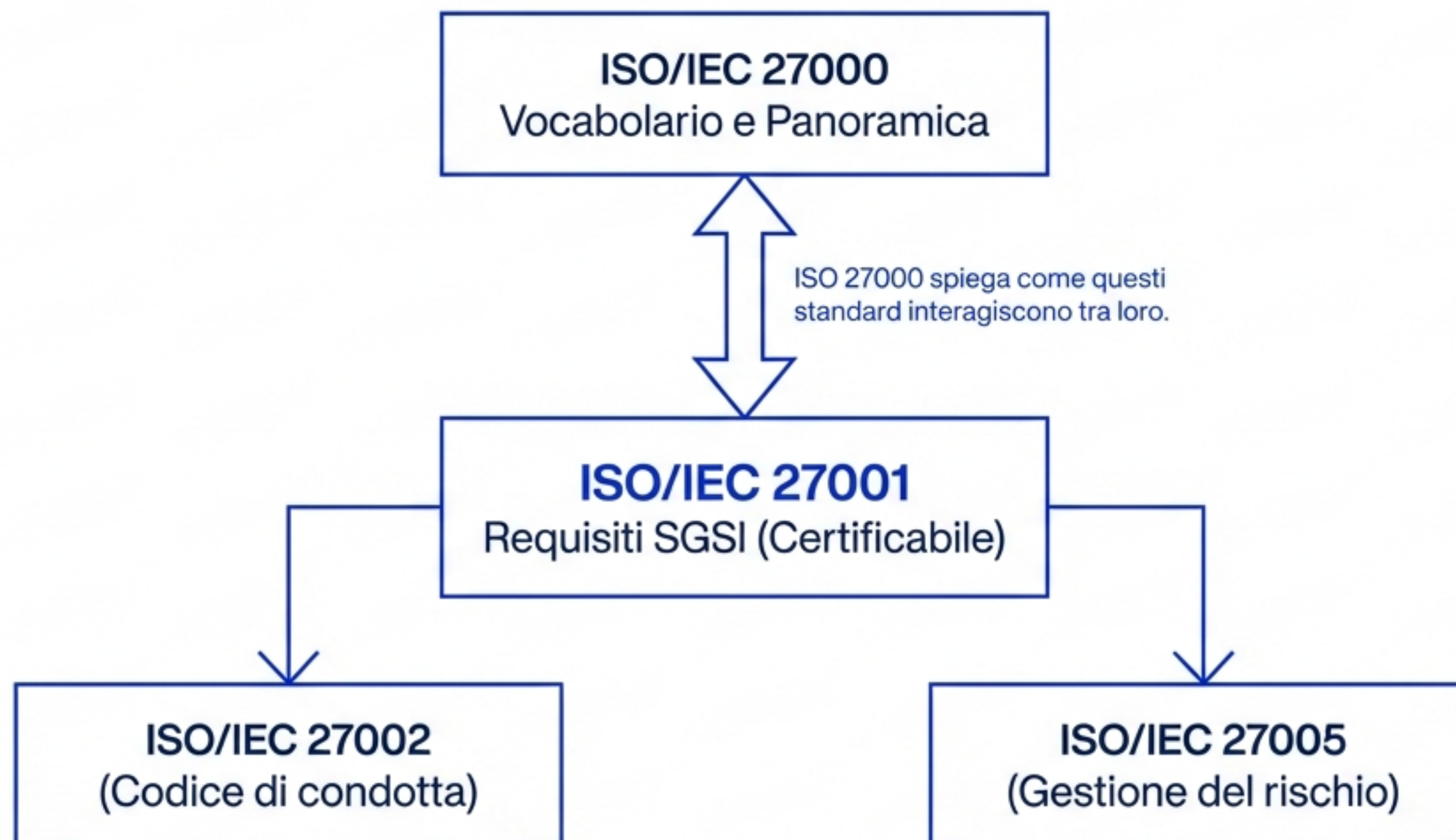
La Soluzione

ISO/IEC 27000 fornisce la Lingua Franca globale per la sicurezza delle informazioni.

Applicabilità

Universale: Imprese commerciali, agenzie governative, no-profit.

L'Ecosistema ISO 27000

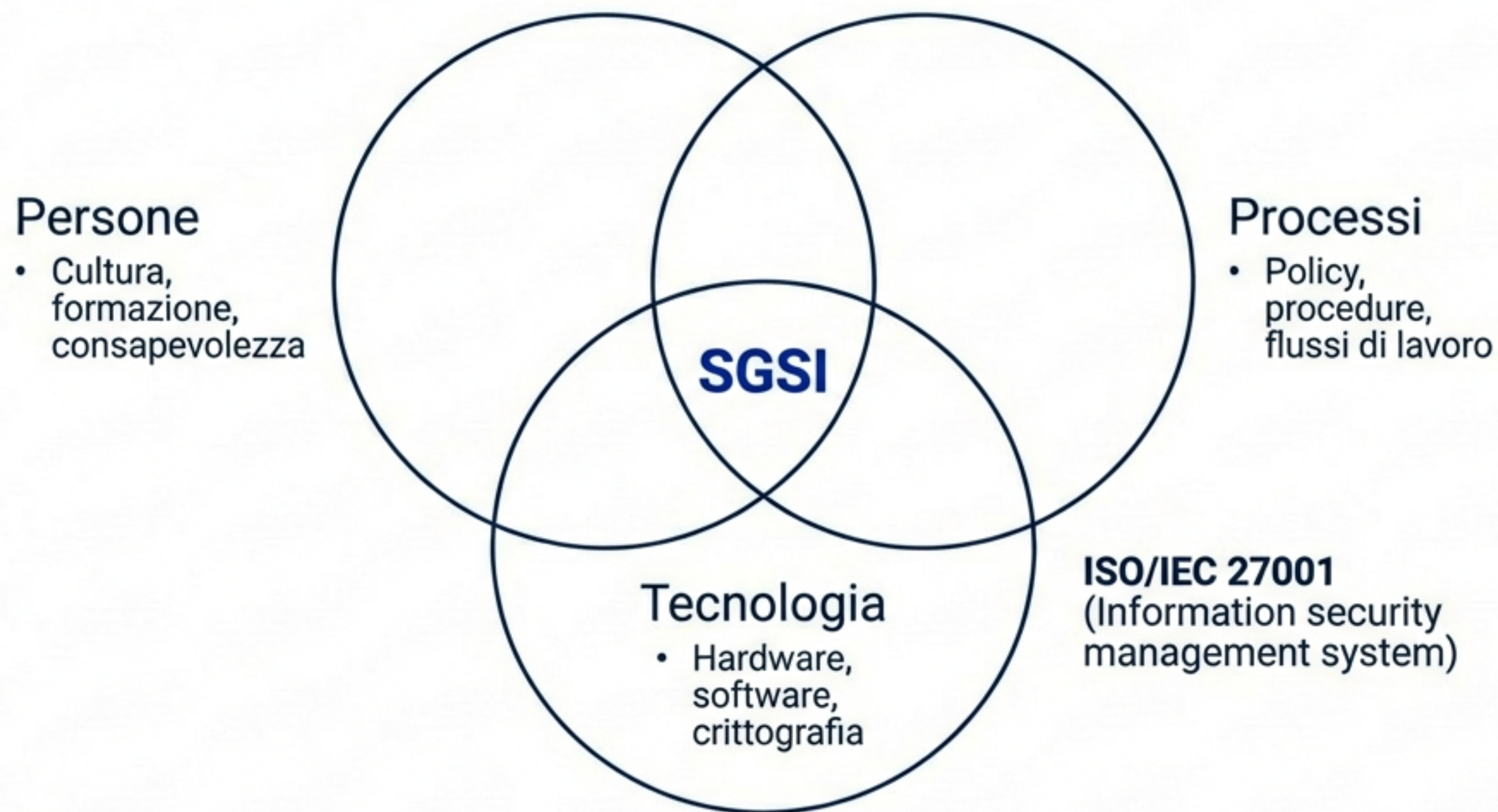


Distinguere gli Standard



Nota: Non ci si certifica in ISO 27000; essa è la chiave di lettura per la 27001.
Nota: Non ci si certifica in ISO 27000; essa è la chiave di lettura per la 27001.

Il Cuore del Sistema: SGSI



SGSI = Sistema di Gestione della Sicurezza delle Informazioni.

I Principi Fondamentali: La Triade RID



Definire l'Asset: Il “Bene”

Bene (Asset): Qualsiasi cosa che abbia valore per l'organizzazione.

Informazioni
(Dati, proprietà intellettuale)



Software e Hardware

Persone
(Competenze ed esperienza)



Intangibili
(Reputazione, immagine del brand)

Non si può proteggere ciò che non si è identificato.

L'Equazione del Rischio

Causa potenziale di
un incidente (es.
hacker, incendio).

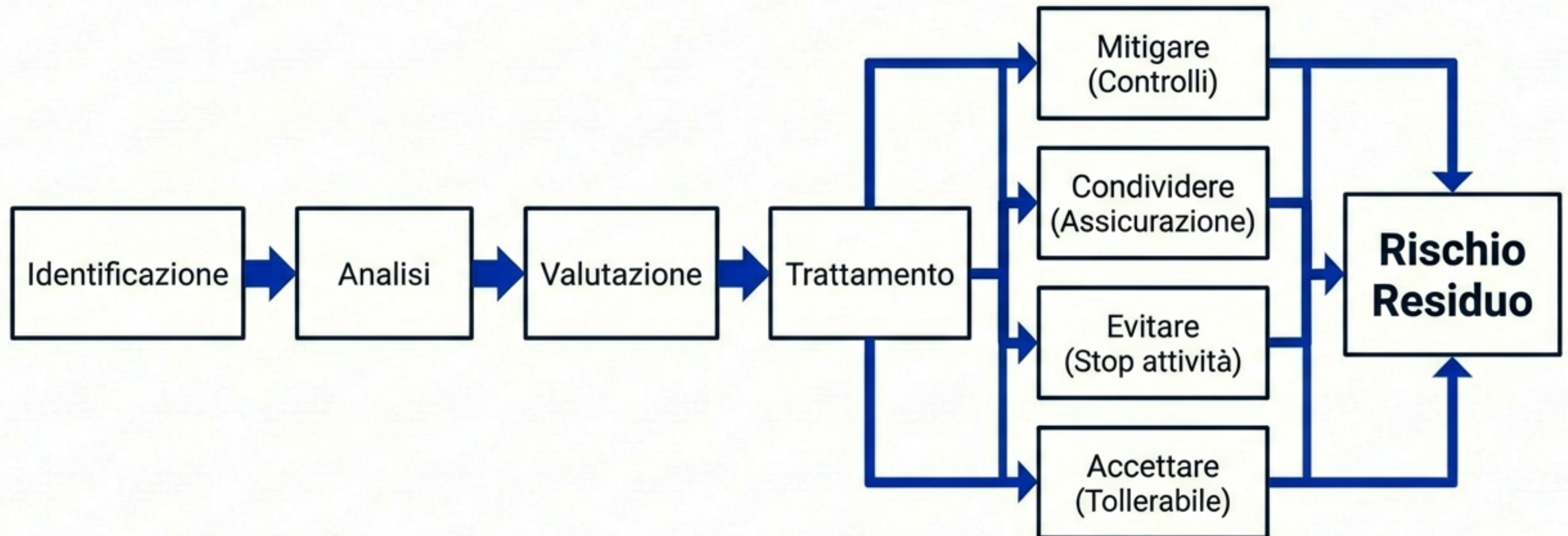
$$(\text{Minaccia} + \text{Vulnerabilità}) \times \text{Asset} = \text{Rischio}$$

Debolezza che può
essere sfruttata.

L'effetto
dell'incertezza
sugli obiettivi.

Insight: Il rischio
include sia le
minacce negative
sia la mancata
opportunità.

Gestione e Trattamento del Rischio



Guidelines
(27002-
27005)

I Controlli di Sicurezza



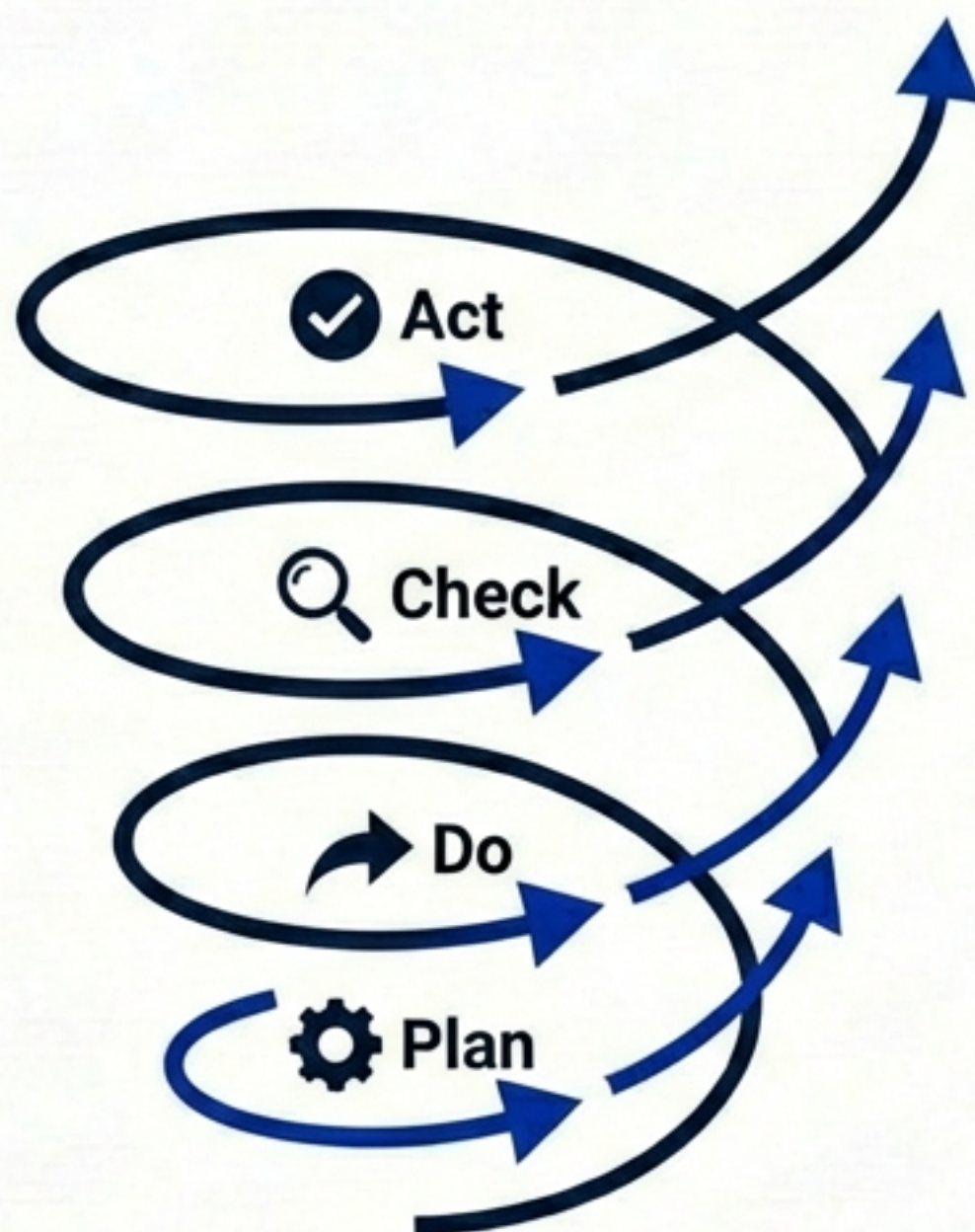
Definizione:

Misure che modificano o riducono il rischio.

Selezione:

Selezione tramite la Dichiarazione di Applicabilità (SoA).

Governance e Miglioramento Continuo



•	Alta Direzione: Responsabile della direzione del SGSI.
•	Miglioramento Continuo: Attività ricorrente per accrescere le prestazioni.
•	Non conformità: Mancato soddisfacimento di un requisito.
•	Azione Correttiva: Eliminare la causa della non conformità.

Estensioni del Vocabolario: Cloud e Privacy

Guidelines
(ISO 27017/18)



Cloud Security (ISO 27017/18)

Definisce ruoli come
Cloud Customer e
Cloud Provider.

Guidelines
(ISO 27701)



Privacy (ISO 27701)

PII: Informazioni di
Identificazione
Personale.

Estende il SGSI al **PIMS**
(Privacy Information
Management System).

Il vocabolario ISO 27000 è la base per la conformità GDPR.

Il Valore Strategico



Chiarezza negli Audit

Riduce l'ambiguità
durante le
certificazioni.



Allineamento Supply Chain

Tutti i partner
parlano la stessa
lingua.

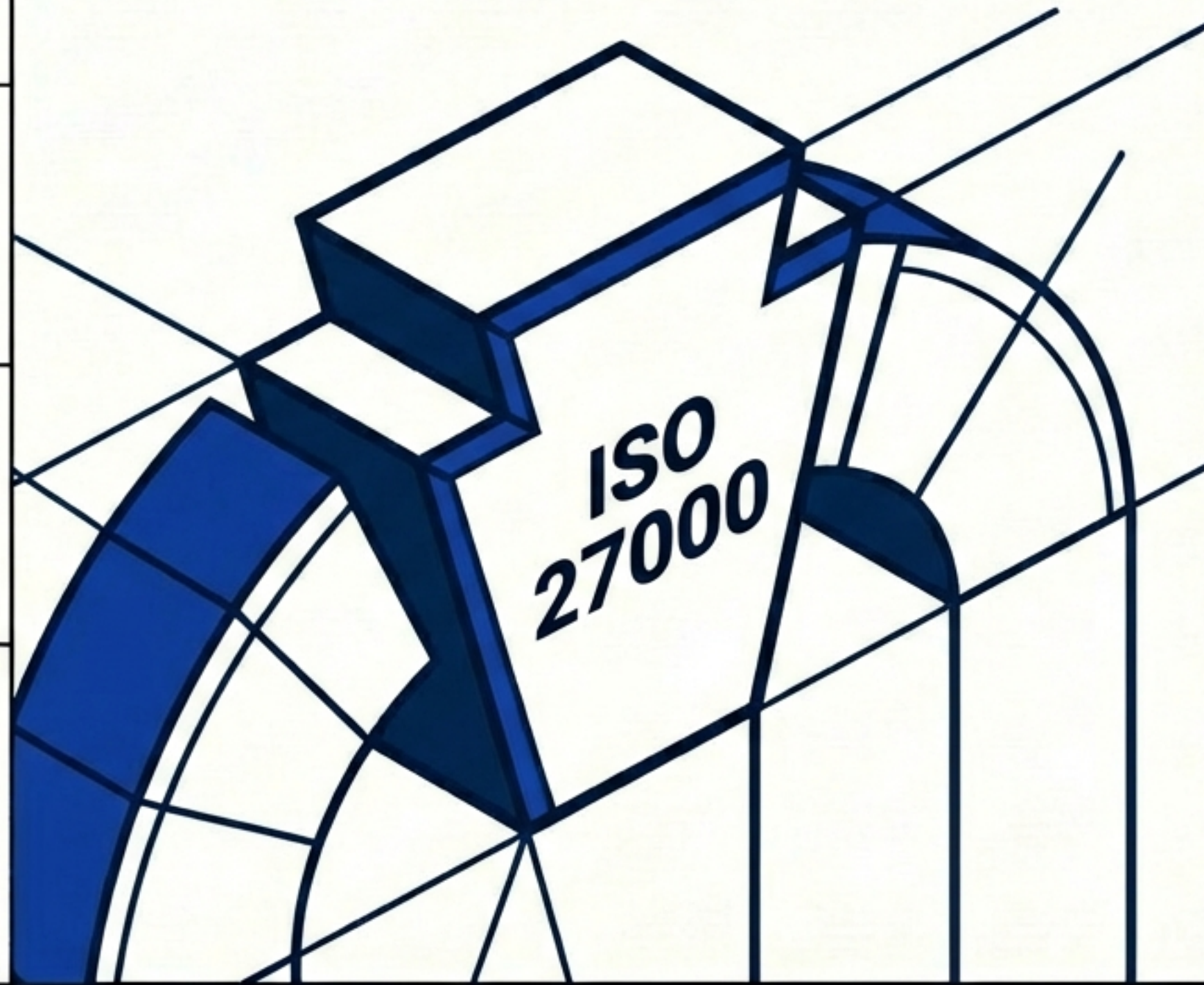


Conformità Legale

Base terminologica
per GDPR, HIPAA e
normative UE.

"Il vocabolario standardizzato trasforma controlli sparsi in un sistema unificato."

Conclusione: La Stele di Rosetta della Sicurezza



- ISO 27000 non è solo un dizionario, è un **progetto architettuale**.
- Sposta la sicurezza da 'problema IT' a **Gestione del Rischio Aziendale**.
- Padroneggiare questo vocabolario è il primo passo la **certificazione ISO 27001**.

Riferimenti Normativi

- **ISO/IEC 27000:2018**: Overview and vocabulary.
- **ISO/IEC 27001**: Requirements.
- **ISO/IEC 27002**: Code of practice for information security controls.
- **ISO/IEC 27005**: Information security risk management.
- **ISO/IEC 27017 / 27018**: Cloud security & privacy.
- **ISO/IEC 27701**: Privacy extension (PIMS).