ISO/IEC 27007:2020

Linee guida per l'audit dei sistemi di gestione della sicurezza delle informazioni (ISMS)

Il Contesto Normativo della Serie ISO 27000

Funzione

ISO 27007 funge da ponte tra i principi generici di audit e i requisiti specifici di sicurezza.

Distinzione

Vitale per audit interni (Prima Parte) e verifica fornitori (Seconda Parte), distinto dall'accreditamento (ISO 27006).

Scopo e Campo di Applicazione

Audit di Prima Parte

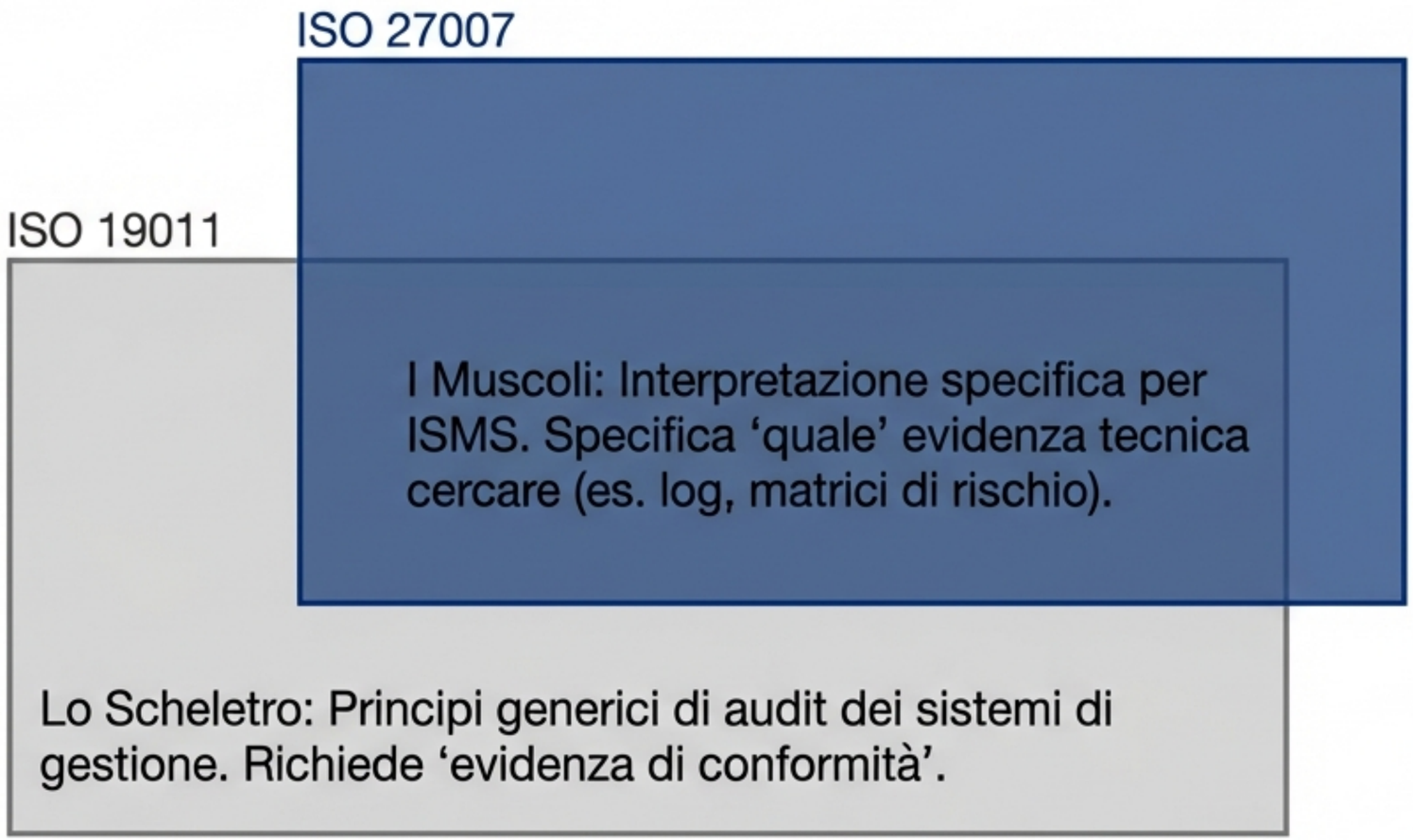
Audit Interno
Verifica della conformità e dell’efficacia del proprio ISMS.

Audit di Seconda Parte

Audit della Supply Chain
Verifica dei fornitori e dei partner esterni.

Obiettivo: Fornire orientamenti sulla gestione dei programmi di audit ISMS e sulla competenza degli auditor per organizzazioni di ogni dimensione.

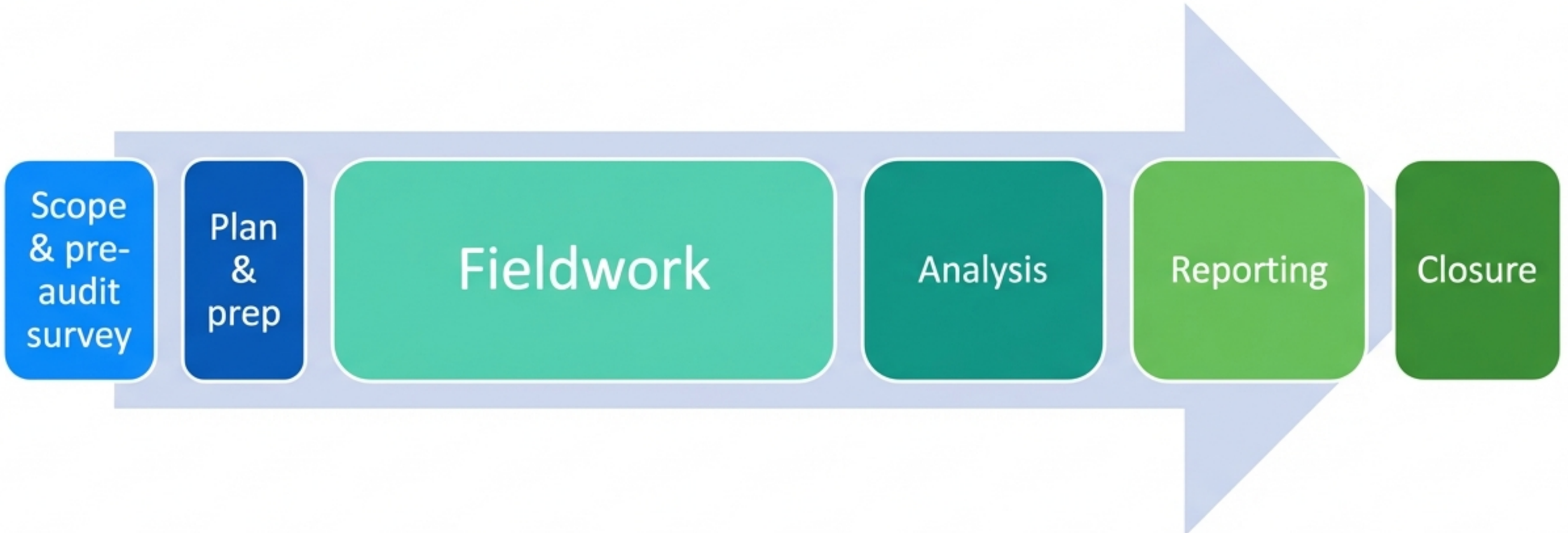
ISO 19011 e ISO 27007: Lo Scheletro e i Muscoli



Relazione Complementare:

ISO 27007 non sostituisce ISO 19011, ma ne espande l’applicazione al dominio della sicurezza delle informazioni.

Gestione del Programma di Audit (Clause 5)



- **Allineamento Strategico**: Il programma deve riflettere la propensione al rischio dell'organizzazione.
- **Approccio Basato sul Rischio**: Frequenza e profondità dipendono dalla criticità degli asset.
- **Governance**: Definizione di obiettivi, risorse e competenza degli auditor.

Esecuzione dell'Audit: Dal 'Poliziotto' al 'Medico'

Approccio Reattivo (Poliziotto)

Cercare colpevoli, focus sulla carta.

Approccio Proattivo (Medico)

Diagnosticare la salute del sistema, focus sui 'living artifacts'.

Oltre la Checklist:

L'auditor moderno verifica l'efficacia delle difese reali analizzando log in tempo reale, registri degli incidenti e rapporti di change management.

Focus Critico: La Dichiarazione di Applicabilità (SoA)

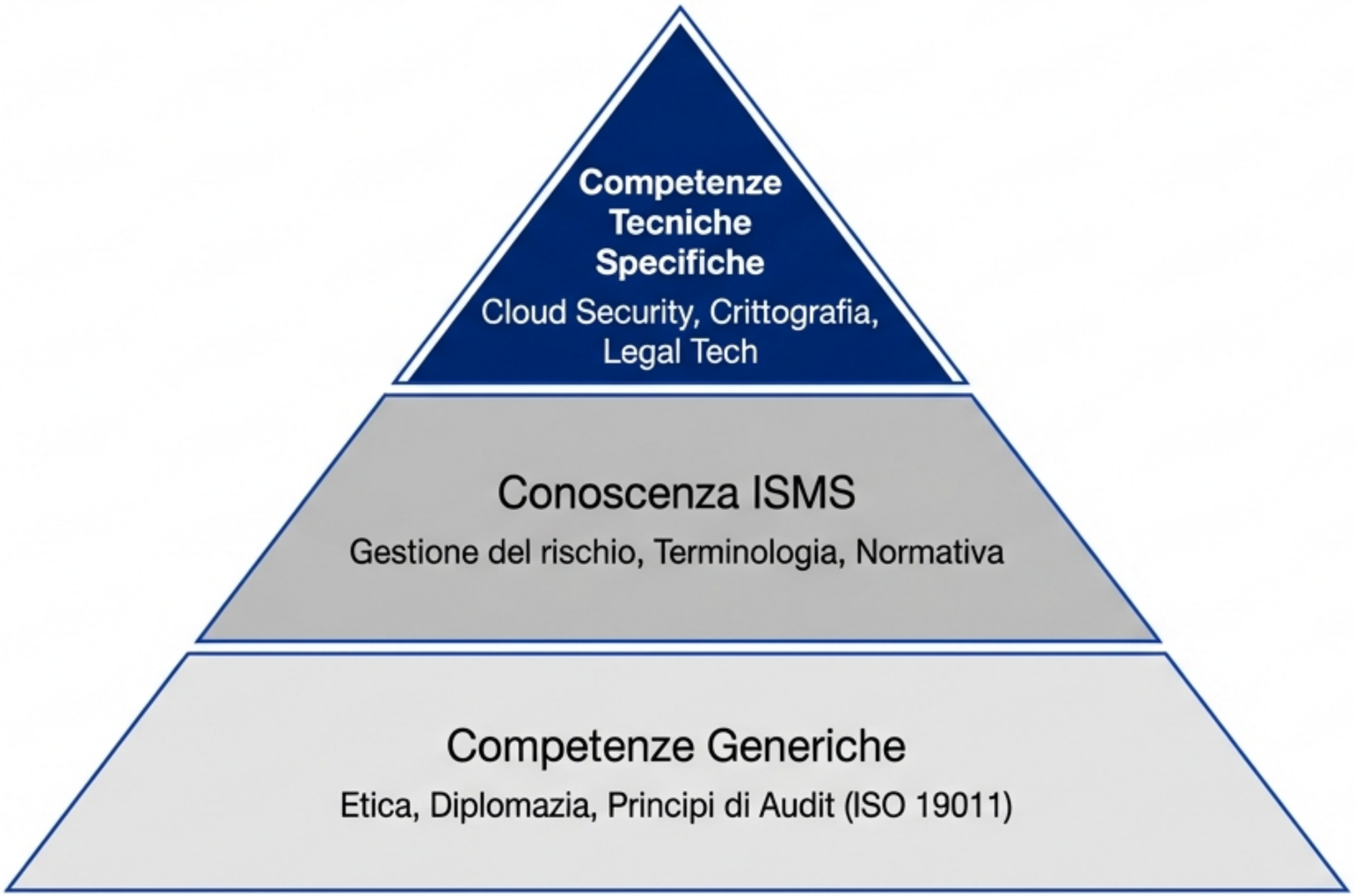
- **Completezza:** La SoA deve includere TUTTI i controlli necessari.
- **Trappola per l'Auditor:** Verificare rigorosamente le GIUSTIFICAZIONI per le esclusioni.
- **Approccio:** Auditare contro il Piano di Trattamento del Rischio (Clause 8.3). Il rischio determina il controllo, non viceversa.

L’Appendice A di ISO 27007: La Guida Pratica

Requisito ISO 27001	Guida Pratica (ISO 27007)	Evidenza Tipica
4.1 Contesto dell'organizzazione	Verificare l'analisi dei fattori interni/esterni	Analisi PESTLE / SWOT, Verbali direzionali
6.1.3 Trattamento del rischio	Verificare l'attuazione del piano	Piani di progetto, Log di configurazione
7.2 Competenza	Mappare le skill sui ruoli	Matrici di competenza, non solo attestati

Valore Operativo: Traduce i requisiti astratti in azioni di audit concrete.

Competenza degli Auditor (Clause 7)



Credibilità: L'auditor non può verificare ciò che non comprende. È richiesta una conoscenza 'discipline-specific'.

Adattamento a ISO/IEC 27001:2022

14 Domini → 4 Temi

- Organizzativo, Persone, Fisico, Tecnologico

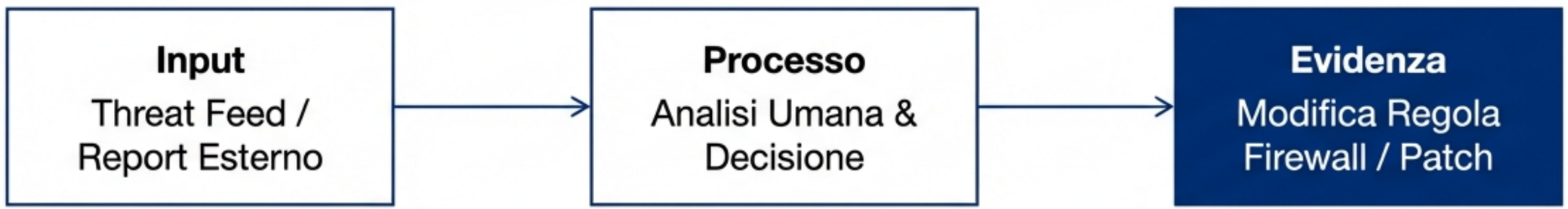
Nuovi Controlli Critici

- Threat Intelligence (A.5.7)
- Sicurezza Cloud (A.5.23)
- Monitoraggio Attività (A.8.16)

Impatto su ISO 27007: Verifica della “Chain of Action” dall’intelligence esterna alla configurazione interna.

Caso Studio: Audit della Threat Intelligence (A.5.7)

The Audit Trail



> “Domanda dell’Auditor: “Mostrami come questo report sulle minacce ha generato un cambiamento concreto nella tua sicurezza.”
>
> — Auditor

Caso Studio: Verifica della Competenza (7.2)

Consapevolezza (7.3)	Competenza (7.2)
‘Ho guardato un video.’ Evidenza: Registro presenze.	‘So configurare il firewall.’ Evidenza: Matrice delle skill, test pratici, certificazioni.

Errore Comune: Confondere l’anzianità di servizio o la semplice partecipazione ai corsi con la competenza operativa verificata.

Sfide Comuni e Errori nell'Audit

Staticità

Affidarsi a documenti obsoleti invece che a dati in tempo reale.

Scope Creep

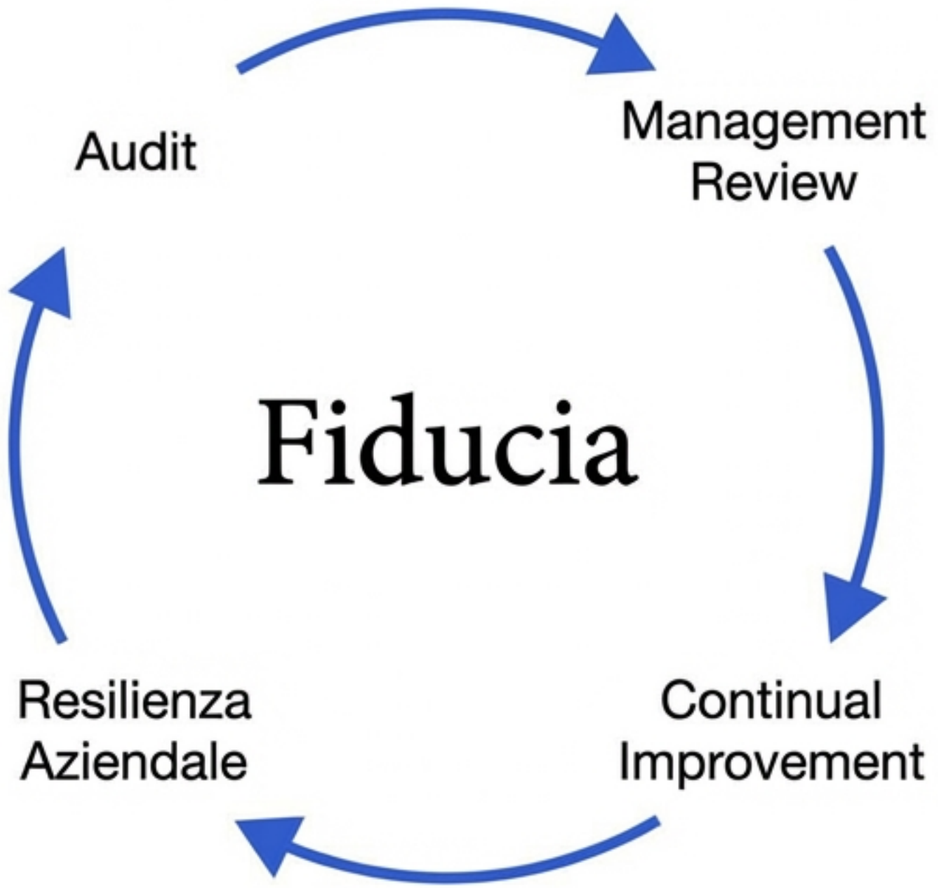
Auditare fuori perimetro o ignorare lo Shadow IT.

Paper Shield

Policy perfette sulla carta ma ignorate nella pratica operativa.

Gap di Competenza: Auditor senza skill tecniche (es. DevOps) che non riescono a valutare l'efficacia reale.

Il Valore Strategico dell'Audit ISMS



ISO 27007 trasforma la compliance in uno strumento di business enablement, assicurando che le difese siano robuste quanto previsto.

Riferimenti Bibliografici

- ISO/IEC 27007:2020 Guidelines for information security management systems auditing
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Requirements
- ISO 19011:2018 Guidelines for auditing management systems
- Brewer, D. ‘Insights into ISO/IEC 27001:2022 Annex A’
- ISO27k Forum ‘ISMS Auditing Guideline’
- Corso di Sicurezza delle Informazioni | Facoltà di Ingegneria Informatica