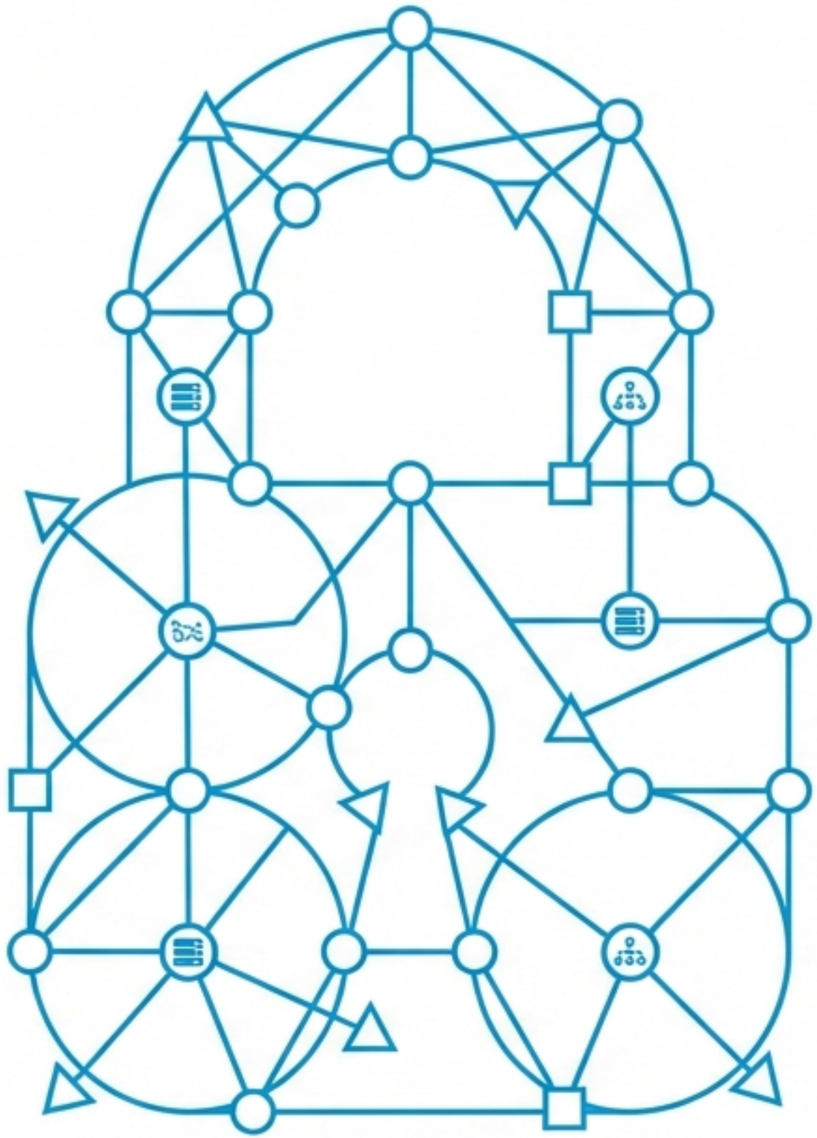
ISO/IEC 27001:2022

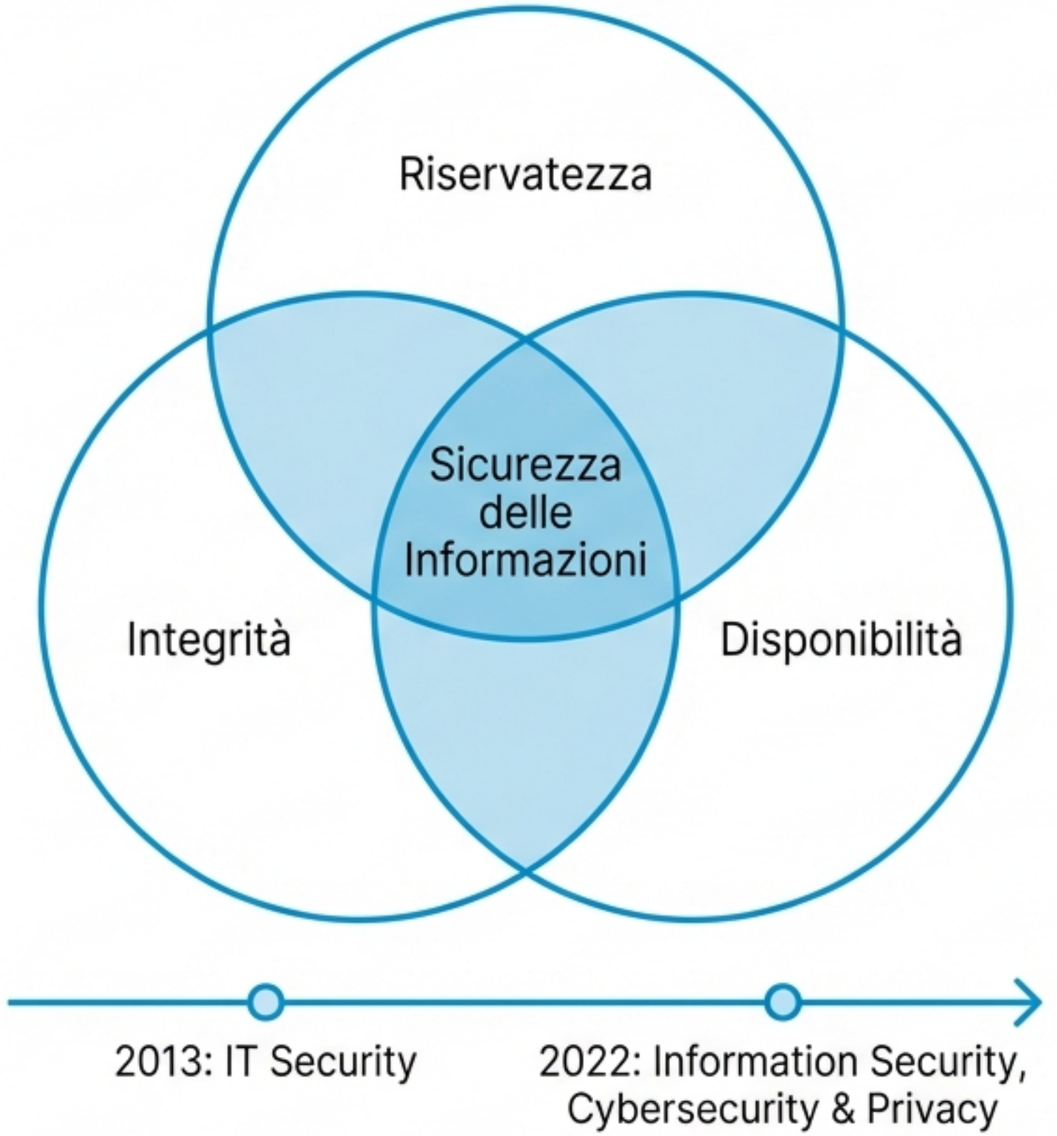
Sicurezza delle Informazioni, Cybersecurity e Protezione della Privacy

Analisi dei Requisiti del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)

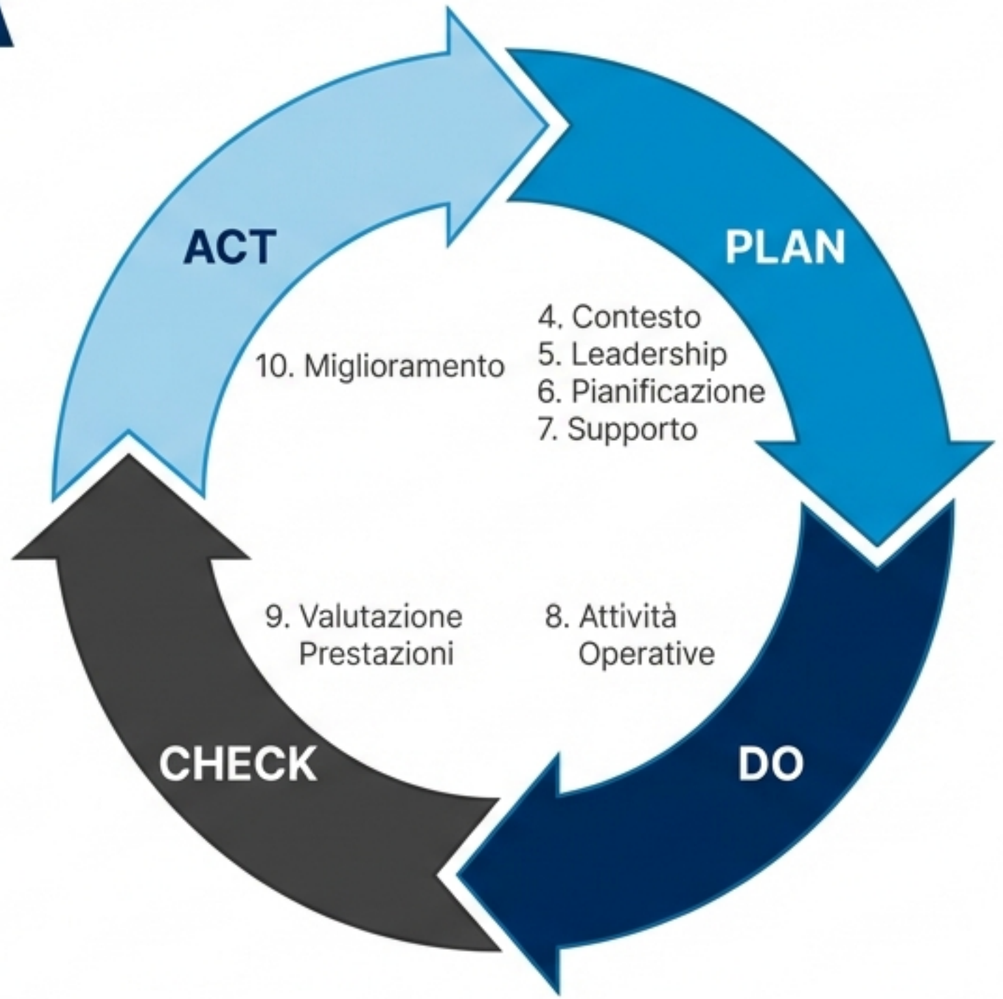


Definizione e Scopo del SGSI

- **Definizione:** L'ISO 27001 definisce i requisiti per un Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
- **Obiettivo:** Proteggere le risorse informative attraverso un approccio basato sul rischio.
- **Evoluzione:** La revisione 2022 espande il focus oltre l'IT puro per includere la protezione della privacy e la resilienza informatica.



Le Clausole Mandatorie (4-10): Il Ciclo PDCA



Il sistema di gestione funziona come un ciclo continuo, non come un progetto lineare.

Emendamento 1:2024 – Azione per il Clima

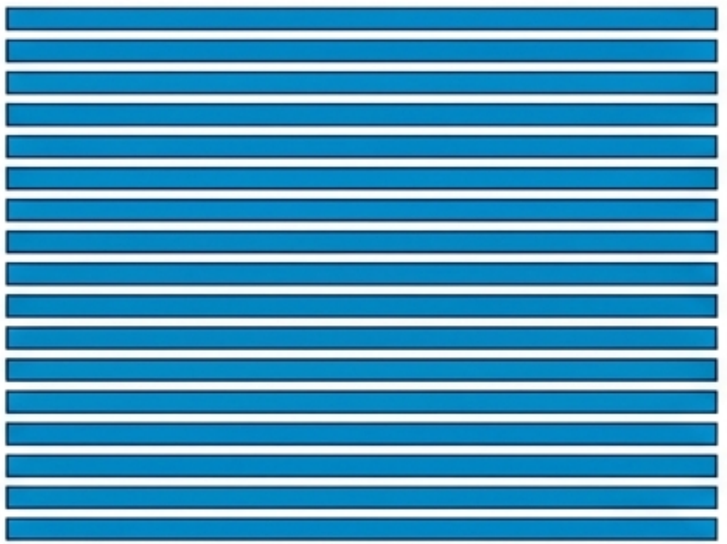
Integrazione Obbligatoria (Febbraio 2024)

- **Clausola 4.1**: L'organizzazione deve determinare se il cambiamento climatico è una questione rilevante per il SGSI.
- **Clausola 4.2**: Le parti interessate possono avere requisiti specifici relativi al cambiamento climatico.

Impatto: Integrazione dei rischi ambientali (es. alluvioni, calore estremo) nella valutazione del rischio e nel Disaster Recovery.

La Ristrutturazione dell'Allegato A

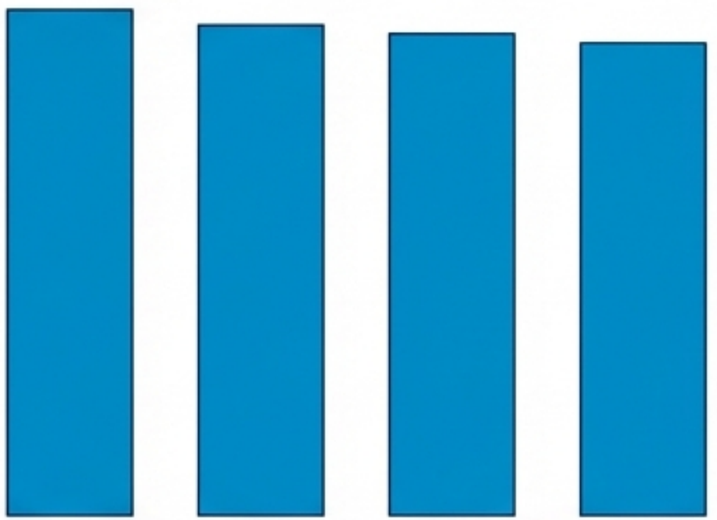
ISO 27001:2013



114 Controlli / 14 Clausole

Razionalizzazione

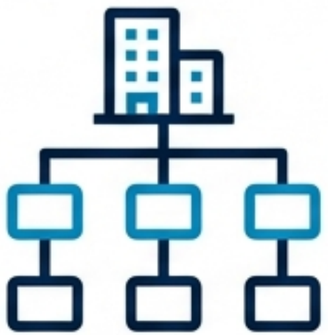
ISO 27001:2022



93 Controlli / 4 Temi

- Riduzione da 114 a 93 controlli per eliminare ridondanze.
- Nuova tassonomia basata su 4 temi trasversali invece di domini IT tradizionali.
- 57 controlli unificati, 11 nuovi controlli introdotti.

I Quattro Temi dei Controlli (Annex A)



1. Organizzativi
(37 Controlli)

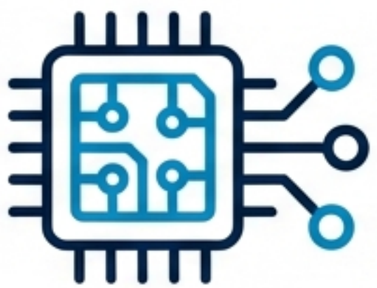
Governance, policy, cloud, fornitori.

2. Persone
(8 Controlli)

Screening, formazione, lavoro remoto.

3. Fisici
(14 Controlli)

Perimetri, monitoraggio, sicurezza uffici.



4. Tecnologici
(34 Controlli)

Crittografia, autenticazione, secure coding.

Gli 11 Nuovi Controlli di Sicurezza

A.5.7 Intelligence sulle minacce

A.5.23 Sicurezza delle informazioni per i servizi cloud

A.5.30 Prontezza ICT per la continuità operativa

A.7.4 Monitoraggio della sicurezza fisica

A.8.9 Gestione della configurazione

A.8.10 Cancellazione delle informazioni

A.8.11 Mascheramento dei dati

A.8.12 Prevenzione della perdita di dati (DLP)

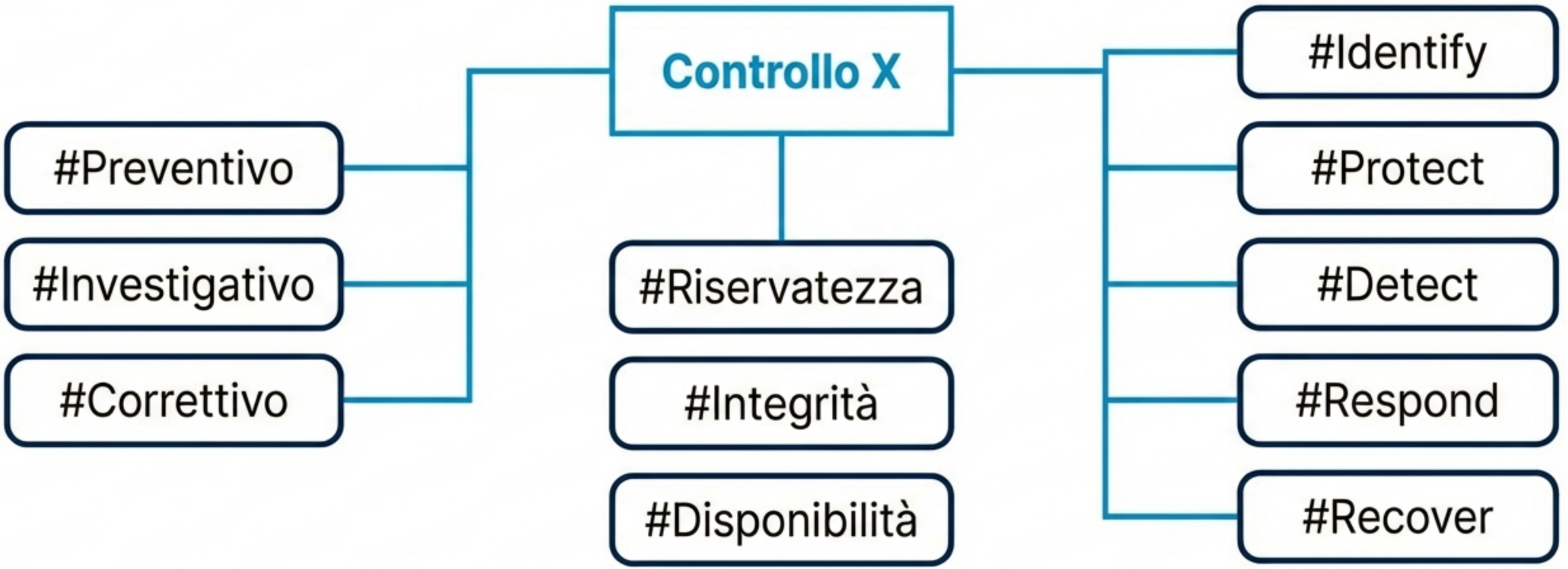
A.8.16 Monitoraggio delle attività

A.8.23 Filtraggio web

A.8.28 Codifica sicura

Attributi e Tassonomia (ISO 27002)

Nuova dimensione di metadati per facilitare il filtraggio e l'allineamento con framework globali.



Gestione del Rischio e Dichiarazione di Applicabilità

Il SoA è il documento fondamentale che giustifica l'inclusione o l'esclusione di ciascuno dei 93 controlli.

Asset

Minaccia / Vulnerabilità

Valutazione Rischio

Trattamento
Mitigare, Accettare, Trasferire, Evitare

SoA (Statement of Applicability)

Il Ciclo di Certificazione e Audit

Il certificato ha validità triennale, soggetta a verifiche annuali.

Tempistiche di Transizione (2013 -> 2022)

Tutti i certificati basati sulla versione 2013 perderanno validità il 31 Ottobre 2025.

Ott 2022
Pubblicazione ISO 27001:2022

Apr 2024
Stop nuove certificazioni 2013

31 Ott 2025
Scadenza Transizione

ISO 27001 e GDPR: Conformità Normativa

L’ISO 27001 fornisce le misure tecniche e organizzative adeguate richieste dall’Articolo 32 del GDPR.

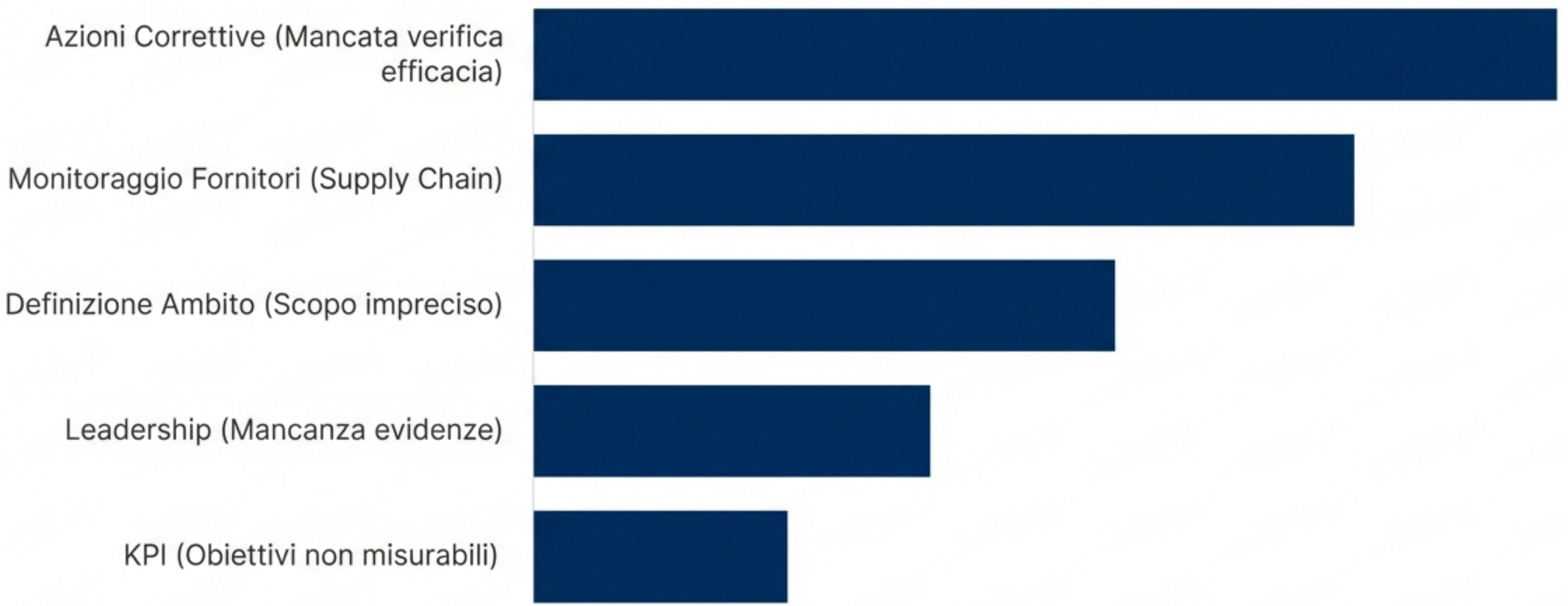
GDPR (Regolamento UE 2016/679)	ISO/IEC 27001:2022
Art. 32 (Sicurezza)	Allegato A (Misure Tecniche)
Art. 33 (Notifica Violazione)	A.5.24 (Incident Mgmt)
	A.5.34 (Privacy PII)

Confronto Framework Internazionali

Framework	Natura	Focus	Geografia
ISO 27001	Certificabile	Sistema di Gestione (SGSI)	Internazionale
NIST CSF	Volontario	Risk Management (IPDRR)	USA / Infrastrutture Critiche
SOC 2 Type II	Attestazione	Trust Services Criteria	USA / Service Organizations

Non Conformità Comuni negli Audit

Aree critiche di fallimento durante la certificazione



Conclusioni: Verso un Futuro Digitale Resiliente

Oltre la Conformità: Un'architettura per la resilienza operativa, non solo un badge.

Cambiamento Culturale: Da 'Sicurezza IT' a 'Sicurezza delle Informazioni' olistica.

Miglioramento Continuo: Adattamento ciclico alle nuove minacce.