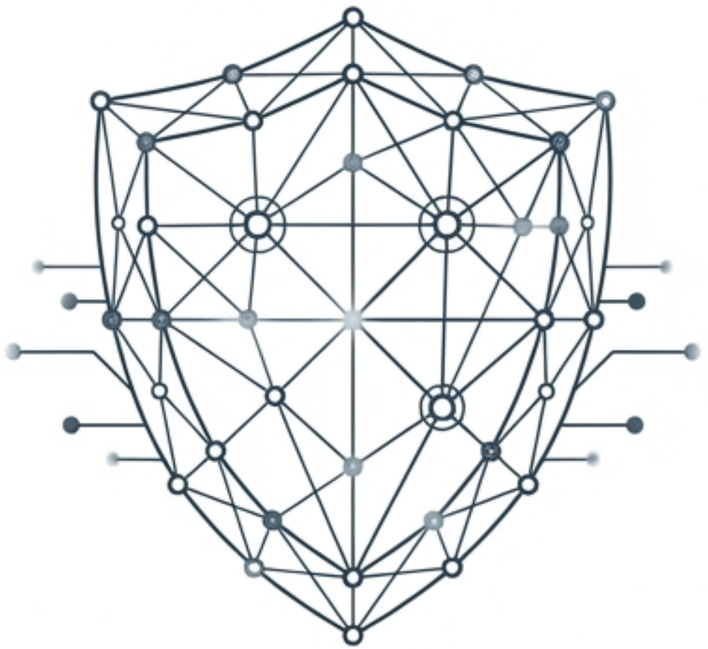
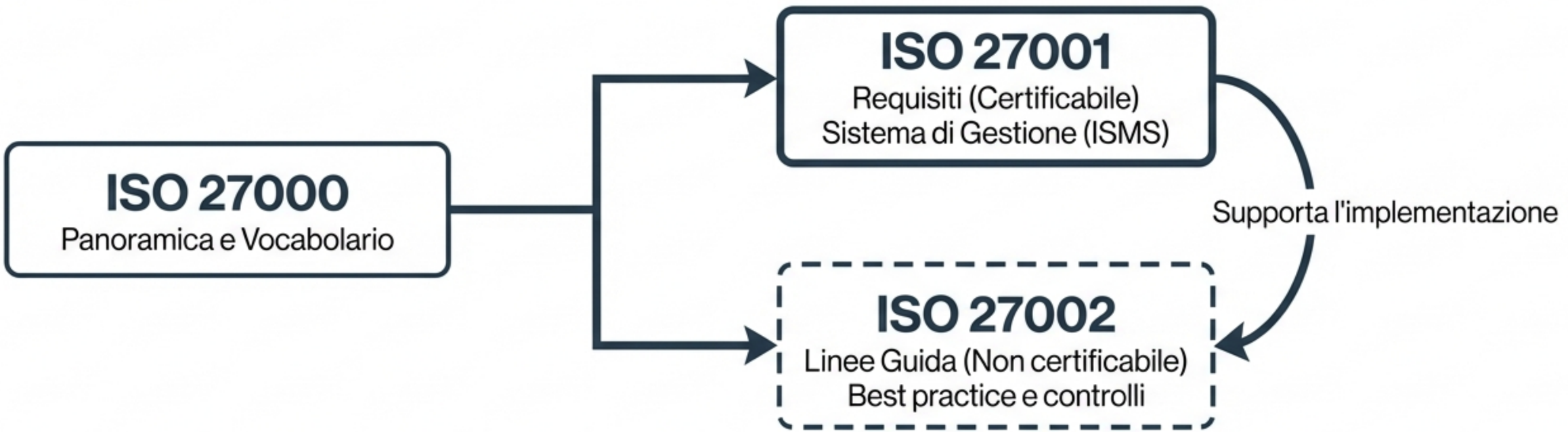
ISO/IEC 27002:2022



Information security, cybersecurity and privacy protection — Information security controls

- Standard internazionale per i controlli di sicurezza delle informazioni.
- Una guida completa per l'implementazione delle best practice in organizzazioni di ogni dimensione.
- Aggiornamento critico rispetto alla versione 2013 per affrontare le minacce moderne.

Il Contesto Normativo: La Famiglia ISO 27000



Note

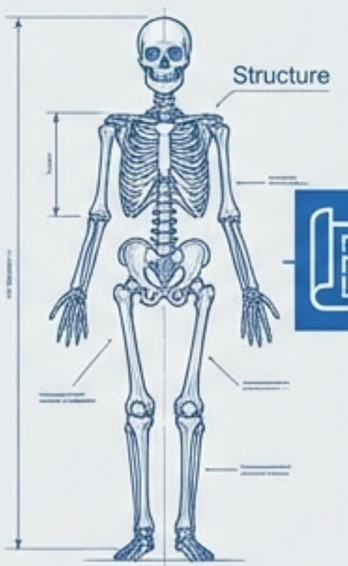
Relazione Chiave: La ISO 27001 definisce *cosa* fare (Requisiti per l'ISMS). La ISO 27002 spiega *come* farlo (Guida all'implementazione dei controlli dell'Annex A).

Nota Bene: Un'organizzazione non può essere certificata ISO 27002; la certificazione avviene solo a fronte della ISO 27001.

Requisiti vs. Guida Pratica

ISO/IEC 27001 (Il Mandato)

- Focalizzato sul Sistema di Gestione (ISMS).
- Approccio basato sul rischio (Risk Assessment).
- Contiene i requisiti normativi (“Shall”).
- Appendice A: Lista sintetica dei controlli.



ISO/IEC 27002 (Il Metodo)

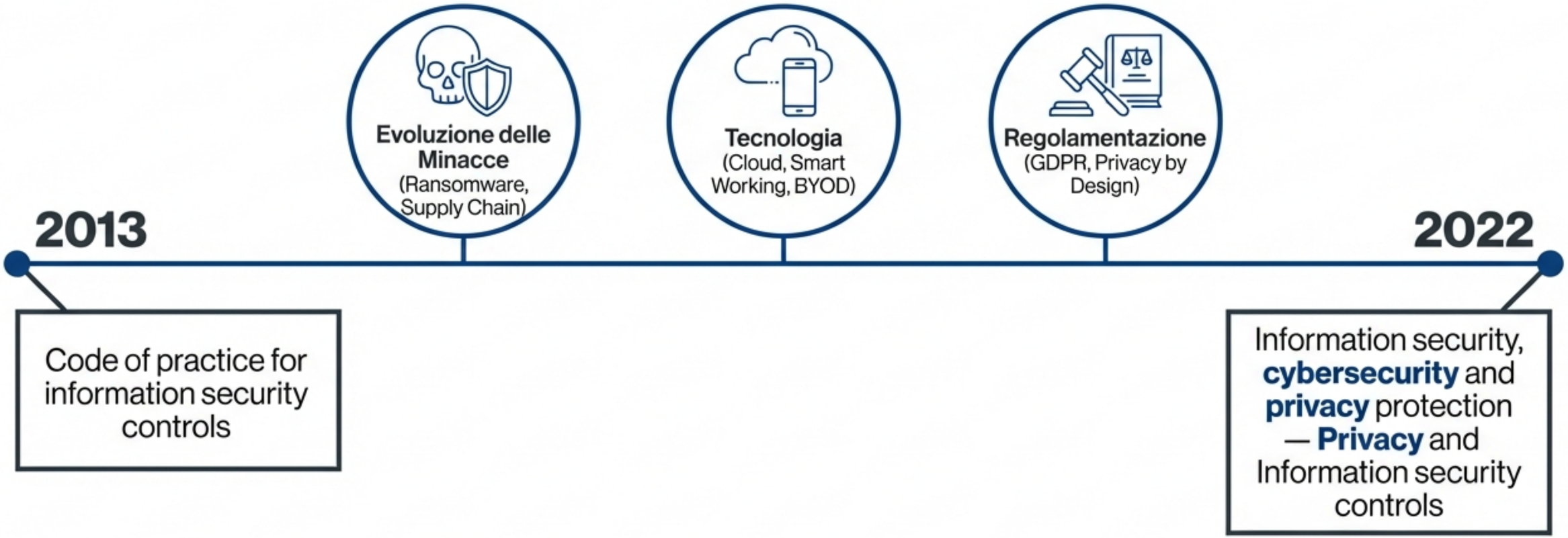
- Focalizzato sui singoli Controlli di Sicurezza.
- Fornisce best practice dettagliate (“Should”).
- Descrive l’obiettivo, la guida all’implementazione e altre informazioni per ogni controllo.
- Circa una pagina di guida per ogni controllo.

Note

Relazione Chiave: La ISO 27001 definisce cosa fare (Requisiti per l'ISMS). La ISO 27002 spiega come farlo (Guida all'implementazione dei controlli dell'Annex A).

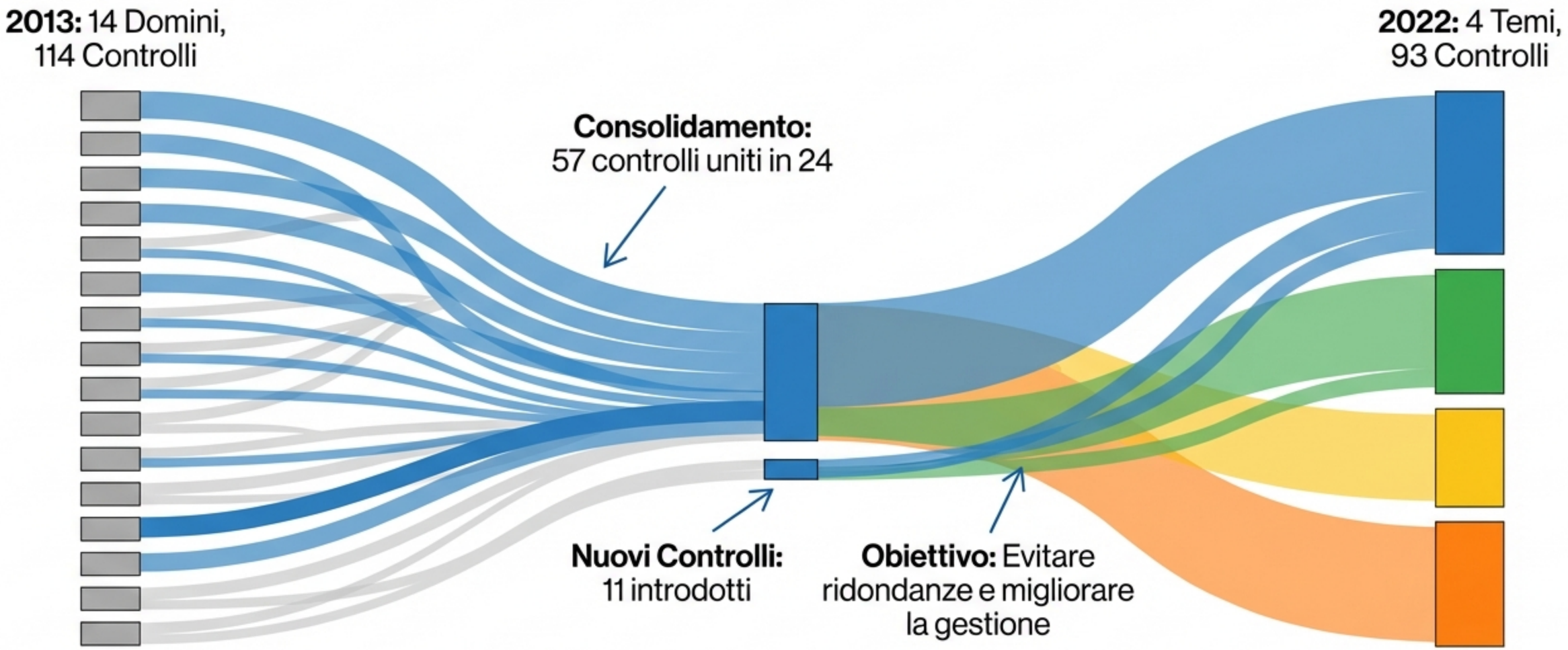
Nota Bene: Un'organizzazione non può essere certificata ISO 27002; la certificazione avviene solo a fronte della ISO 27001.

L’Evoluzione: 2013 vs 2022



Lo standard si è evoluto per integrare
Cybersicurezza e Privacy, non solo sicurezza IT.

Il Cambio Strutturale: Semplificazione e Riorganizzazione



Nota: La riorganizzazione è pensata per rendere lo standard più moderno, gestibile e applicabile.

La Nuova Tassonomia: I 4 Temi

Controlli Organizzativi (Clausola 5)

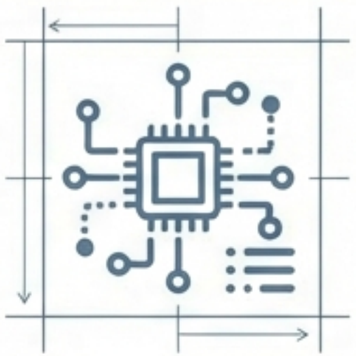
37 Controlli.
Politiche, governance, gestione risorse.

Controlli sulle Persone (Clausola 6)

8 Controlli.
Risorse umane, formazione, sensibilizzazione.

Controlli Fisici (Clausola 7)

14 Controlli.
Perimetri, sicurezza uffici, protezione hardware.

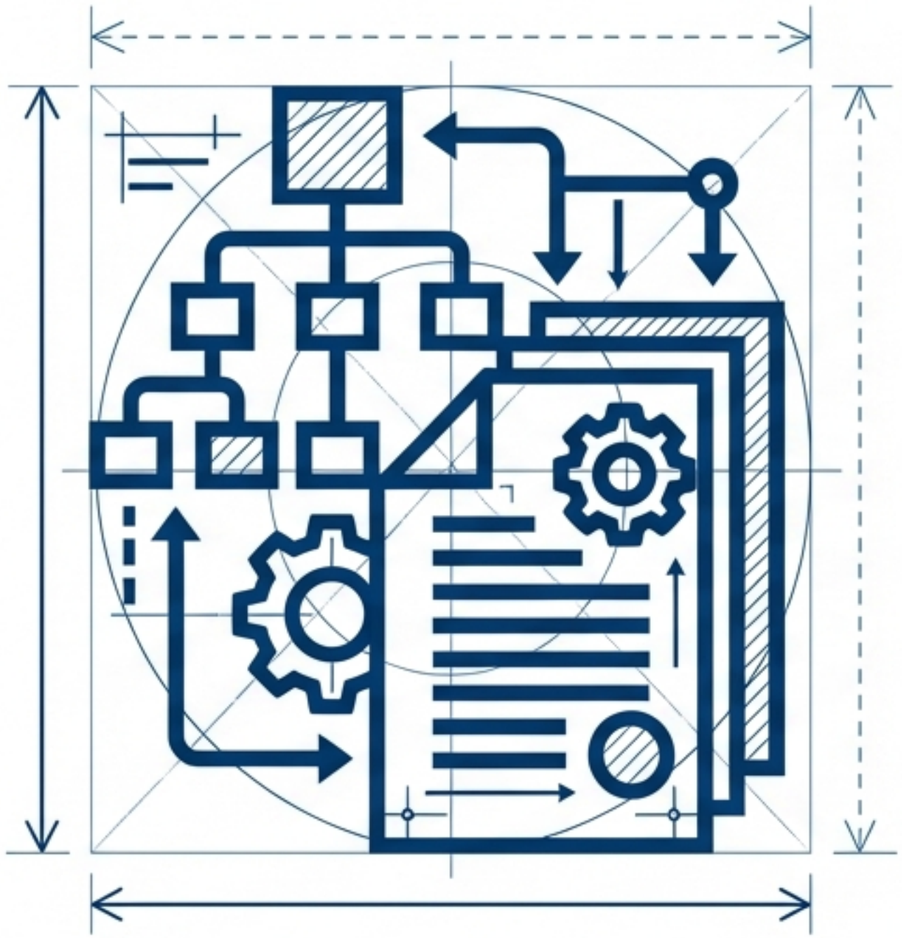


Controlli Tecnologici (Clausola 8)

34 Controlli.
Autenticazione, crittografia, sicurezza rete.

Tema 1: Controlli Organizzativi

Clausola 5: La base della governance e della gestione



- Politiche per la sicurezza delle informazioni
- Ruoli e responsabilità
- Intelligence sulle minacce (Threat Intelligence) [NUOVO]
- Sicurezza nelle relazioni con i fornitori
- Gestione dell’identità (Identity Management) e autenticazione
- Sicurezza per l’utilizzo dei servizi Cloud [NUOVO]

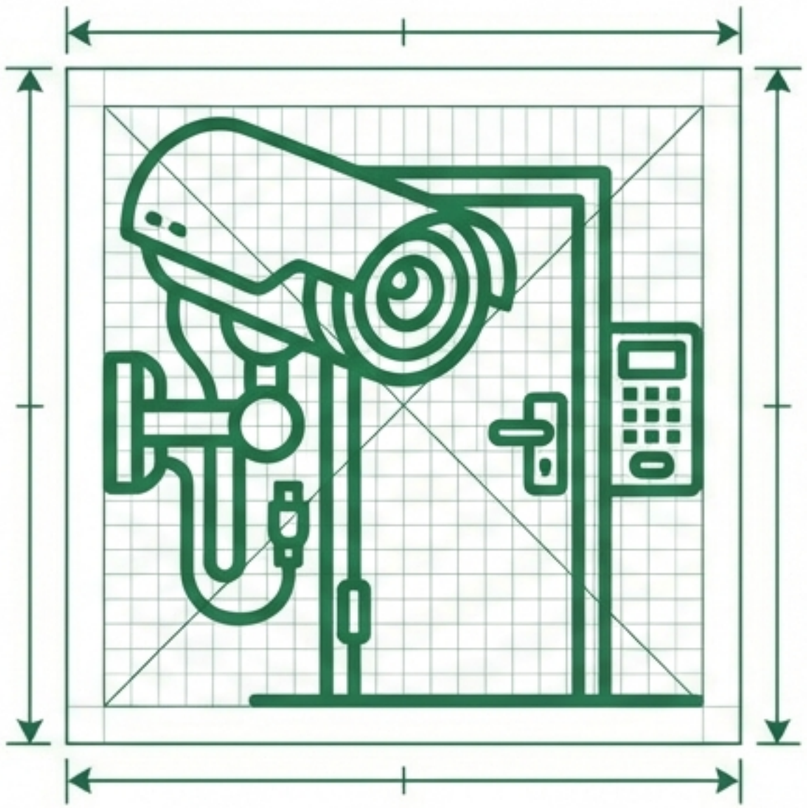
Tema 2: Controlli sulle Persone

Clausola 6: Gestire il fattore umano nel ciclo di vita lavorativo.

- ☑ Screening dei candidati (Background checks)
- ☑ Termini e condizioni di impiego
- ☑ Consapevolezza, istruzione e formazione sulla sicurezza
- ☑ Processo disciplinare
- ☑ Lavoro a distanza (Remote working)
- ☑ Accordi di riservatezza (NDA)

Tema 3: Controlli Fisici

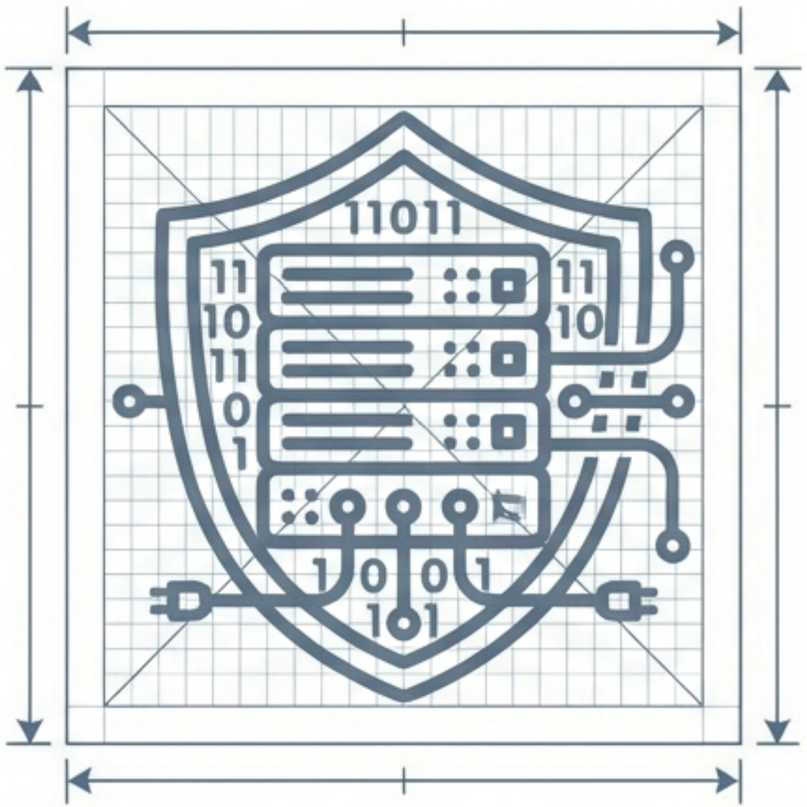
Clausola 7: Protezione degli asset tangibili e degli ambienti.



- ☑ Perimetri di sicurezza fisica
- ☑ Controlli fisici agli ingressi
- ☑ Monitoraggio della sicurezza fisica [NUOVO]
- ☑ Politica della scrivania pulita e dello schermo libero (Clear desk / Clear screen)
- ☑ Sicurezza del cablaggio
- ☑ Manutenzione dell'attrezzatura

Tema 4: Controlli Tecnologici

Clausola 8: Salvaguardia digitale, reti e applicazioni.



- ☑ Dispositivi endpoint degli utenti
- ☑ Gestione della configurazione [NUOVO]
- ☑ Cancellazione delle informazioni [NUOVO]
- ☑ Data masking (Mascheramento dei dati) [NUOVO]
- ☑ Prevenzione della perdita di dati (DLP) [NUOVO]
- ☑ Monitoraggio delle attività e Web filtering
- ☑ Secure coding (Sviluppo sicuro del codice) [NUOVO]

Il Concetto di ‘Attributi’: Una Tassonomia Multidimensionale

- Ogni controllo è associato a un set di attributi (metadati).
- Permette di creare “viste” personalizzate dei controlli (es. filtrare solo i controlli “Preventivi”).
- Facilita l’allineamento con altri framework (es. NIST CSF).

Le 5 Categorie di Attributi

Tipo di Controllo → #Preventive #Detective #Corrective

Proprietà InfoSec → #Confidentiality #Integrity #Availability (Modello CIA/RID)

Concetti Cybersecurity → #Identify #Protect #Detect #Respond #Recover (Allineamento NIST)

Capacità Operative → Vista del professionista (es. Governance, Asset Management)

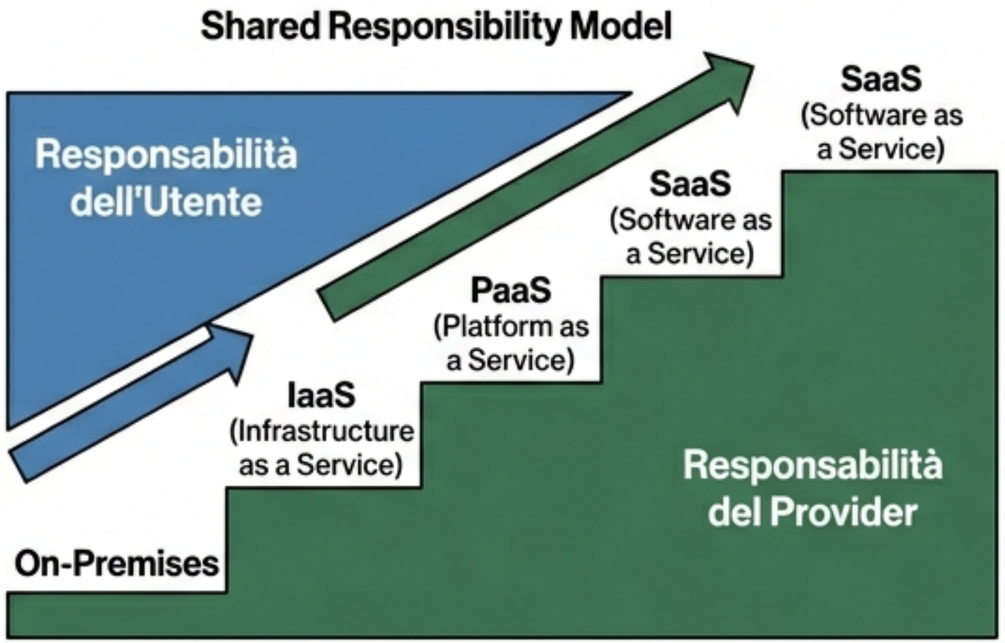
Domini di Sicurezza → Vista strategica (es. Protection, Defence, Resilience)

Focus: Gli 11 Nuovi Controlli

Threat intelligence	Information security for use of cloud services	ICT readiness for business continuity	Physical security monitoring
Configuration management	Information deletion	Data masking	Data leakage prevention
Monitoring activities	Web filtering	Secure coding	 Modernization

Approfondimento: Cloud e Threat Intelligence

Controllo 5.23: Sicurezza dei Servizi Cloud



Obiettivo: Definire processi per acquisizione, utilizzo, gestione e uscita dai servizi cloud.

Controllo 5.7: Threat Intelligence

Obiettivo: Raccogliere e analizzare informazioni sulle minacce per agire preventivamente.

Conclusioni e Implementazione

Risk Assessment → Selezione dei Controlli → Statement of Applicability (SoA) → Implementazione

Dichiarazione di Applicabilità (SoA)

Aggiornare la SoA per allinearsi ai nuovi 93 controlli.

Flessibilità

Utilizzare gli attributi per personalizzare la selezione in base ai rischi.

Transizione

Periodo di transizione per le organizzazioni già certificate ISO 27001.

La ISO 27002 non è una checklist statica, ma un framework resiliente per la protezione dei dati nell'era digitale.