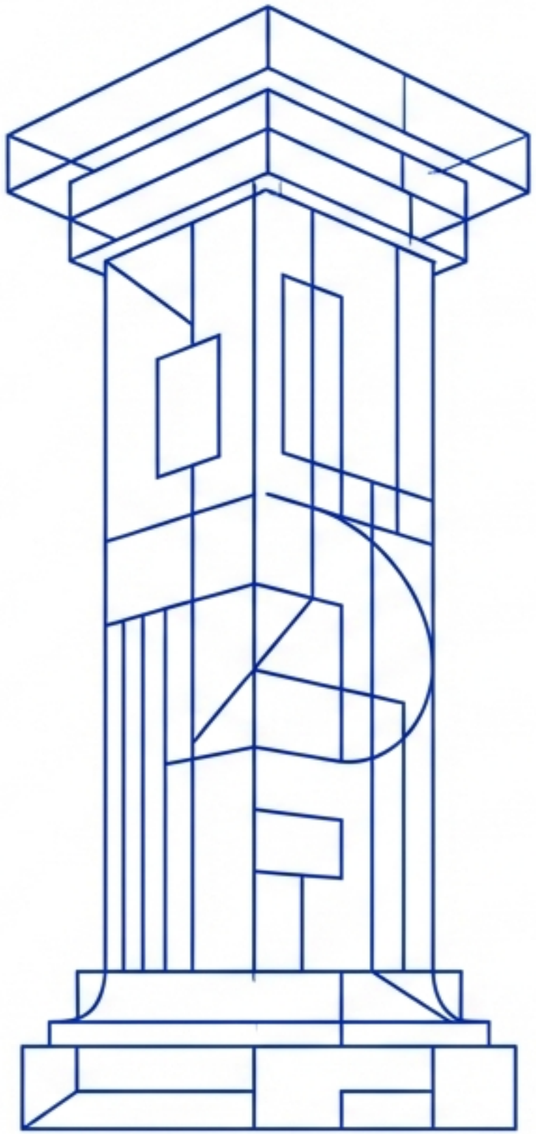
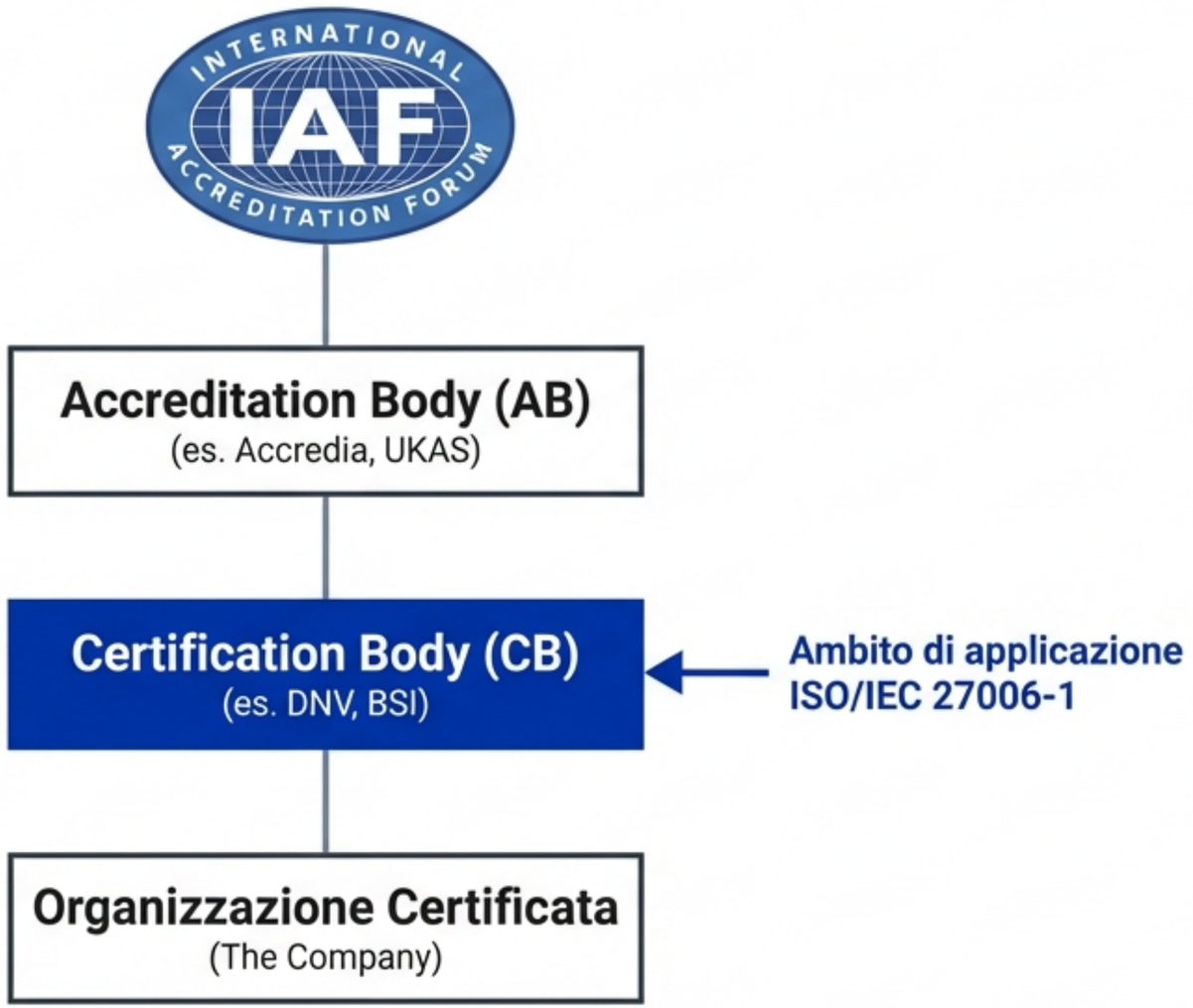
ISO/IEC 27006-1:2024 – L’Architettura della Fiducia Digitale

Requisiti per gli organismi di audit e certificazione dei sistemi di gestione della sicurezza delle informazioni (ISMS)



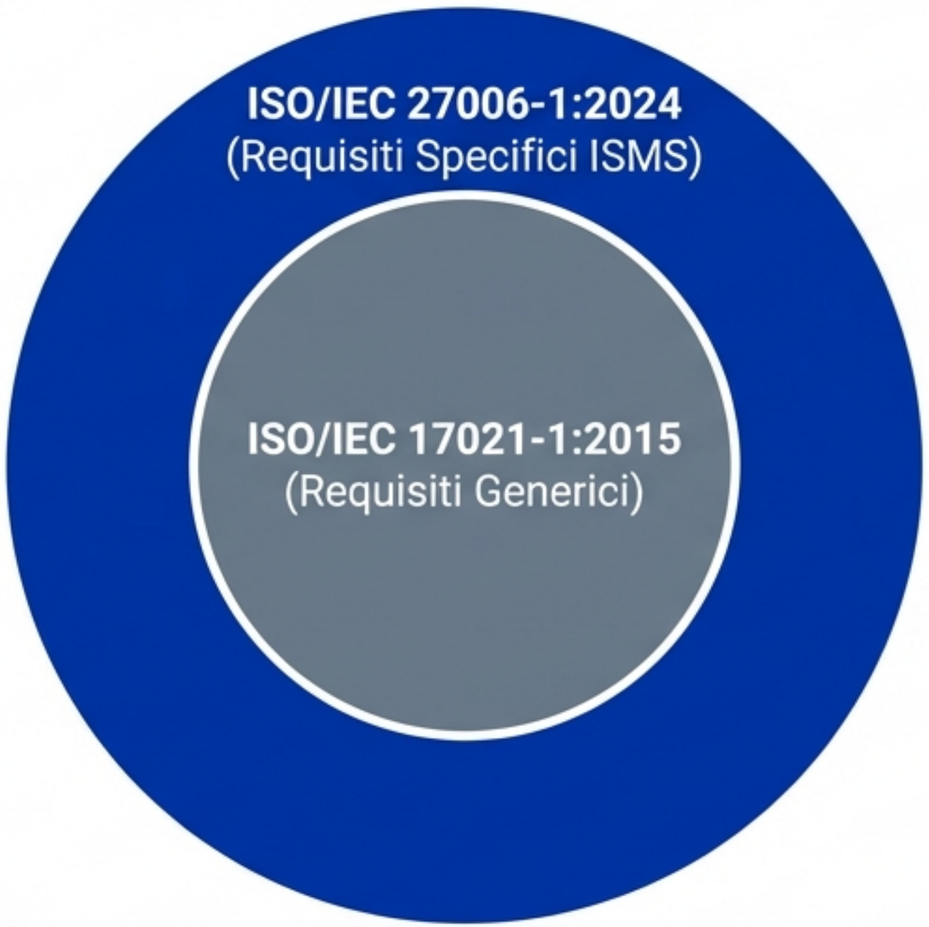
L’Ecosistema dell’Accreditamento Globale



Il Ruolo della Norma: La ISO/IEC 27006-1 non si applica all’azienda certificata, ma all’Organismo di Certificazione (CB). È lo standard che “controlla i controllori”.

Garanzia di Validità: Senza accreditamento secondo questa norma, i certificati ISO/IEC 27001 perdono il riconoscimento internazionale IAF MLA.

Definizione e Relazioni Normative



- **ISO/IEC 17021-1:2015**: Fornisce i requisiti generici per *tutti* i sistemi di gestione (Qualità, Ambiente, ecc.). Stabili sce le basi d imparzialità e processo.
- **ISO/IEC 27006-1:2024**: Aggiunge il rigore tecnico specifico per la sicurezza delle informazioni (ISMS).
- **Obiettivo:** Standardizzare la competenza degli auditor e il calcolo dei **tempi di audit** a livello globale, riducendo le ridondanze con la 17021-1 (es. clausole 5.2, 7.1.3, 9.4).

Le Innovazioni della Versione 2024

Una “Revisione Limitata” con Impatti Operativi Sostanziali

Competenza (Qualitativa)

Audit Remoto

Matematica dell'Audit

Allineamento 27001:2022

La norma sostituisce la ISO/IEC 27006:2015 e risponde alla modernizzazione del lavoro (ibrido/remoto), introducendo un approccio matematico più rigoroso al calcolo dei giorni/uomo.

Evoluzione della Competenza: Da Quantità a Qualità

Vecchio Requisito
(Tempo)

Nuovo Requisito
(Dimostrazione)

- **Rimozione del Vincolo Temporale:** Eliminato il requisito rigido di “4 anni di esperienza pratica a tempo pieno” per gli auditor.
- **Competenza Contestuale:** La valutazione si sposta sull’expertise reale e sulla capacità di applicare le skills in scenari specifici (es. Cloud, ICS).
- **Competenza Collettiva:** Il team di audit *nel suo complesso* deve possedere le conoscenze tecniche necessarie.

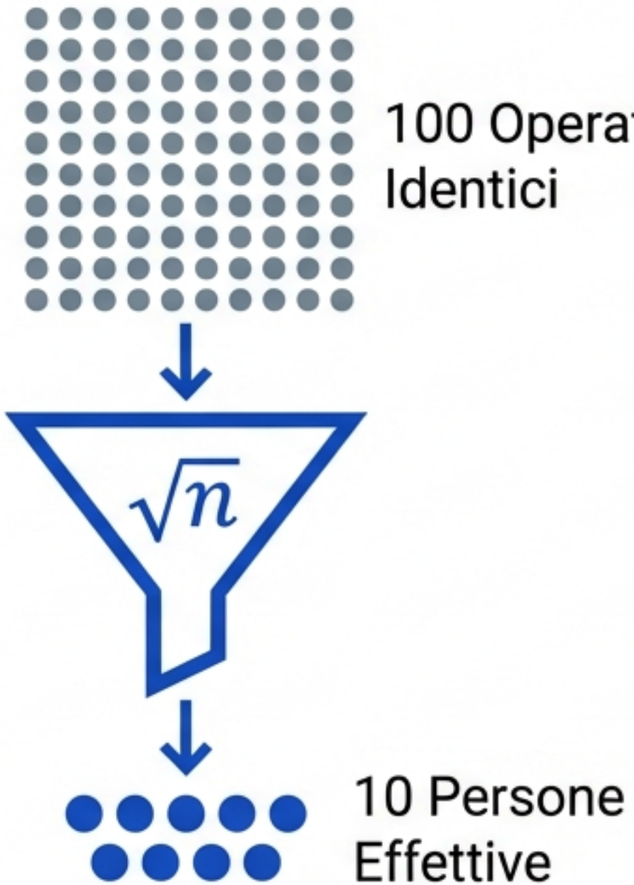
La Normalizzazione dell’Audit Remoto

Abolizione della Soglia del 30%: Rimossa la necessità di approvazione dell’Ente di Accreditamento se l’audit remoto supera il 30% del tempo totale.

Organizzazioni ‘Site-less’: Per aziende senza sedi fisiche, il certificato deve indicare esplicitamente che le attività sono condotte in remoto.

Obbligo di Trasparenza: Il rapporto di audit deve dettagliare l’estensione e l’efficacia delle tecniche remote utilizzate (Clausola 9.4.3.2).

La Matematica dell’Audit: Il Personale Effettivo (Annex C)

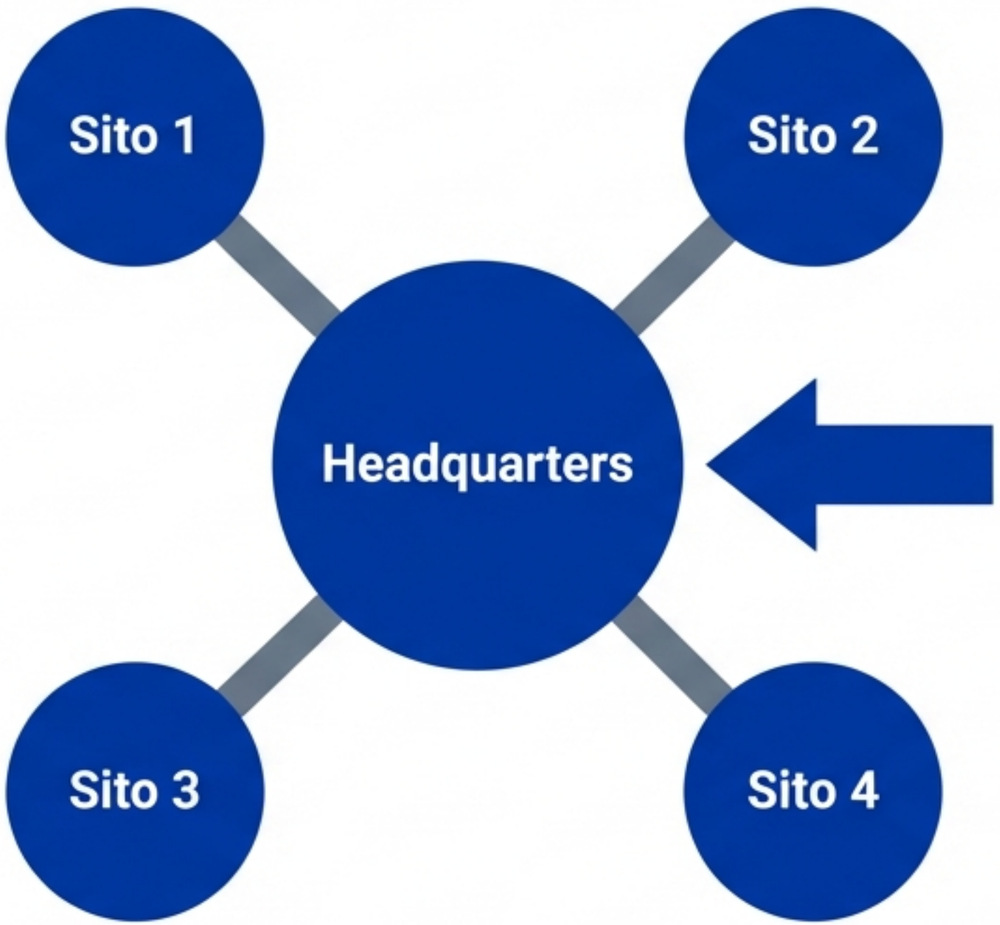


Concetto di Personale Effettivo: Il calcolo dei giorni di audit si basa sul numero di persone sotto il controllo dell’organizzazione (inclusi contractor).

Riduzione per Attività Ripetitive: Per gruppi che svolgono compiti identici e a basso rischio, si applica una riduzione basata sulla radice quadrata.

Giustificazione: Ogni riduzione deve essere documentata e giustificata categoria per categoria.

Gestione Multisito e Campionamento



Approccio 'Top-Down' (Preferito):
Il tempo totale è calcolato sul numero complessivo di dipendenti dell'intera organizzazione.

Approccio 'Bottom-Up':
La somma dei tempi dei singoli siti è permessa solo se il totale è *superiore* al calcolo top-down.

Formule di Campionamento:

- Audit Iniziale: $\sqrt{n}$
- Sorveglianza: $0.6 \times \sqrt{n}$
- Recertificazione: $\sqrt{n}$ (o $0.8 \times \sqrt{n}$)

Allineamento con ISO/IEC 27001:2022

Annex D (2015) Annex E (2024)

Nuovo Annex E:

L'ex Annex D è stato aggiornato e rinominato.

Sincronizzazione dei Controlli:

Guida per la verifica dei 93 controlli di sicurezza della ISO/IEC 27001:2022 (Organizzativi, Persone, Fisici, Tecnologici).

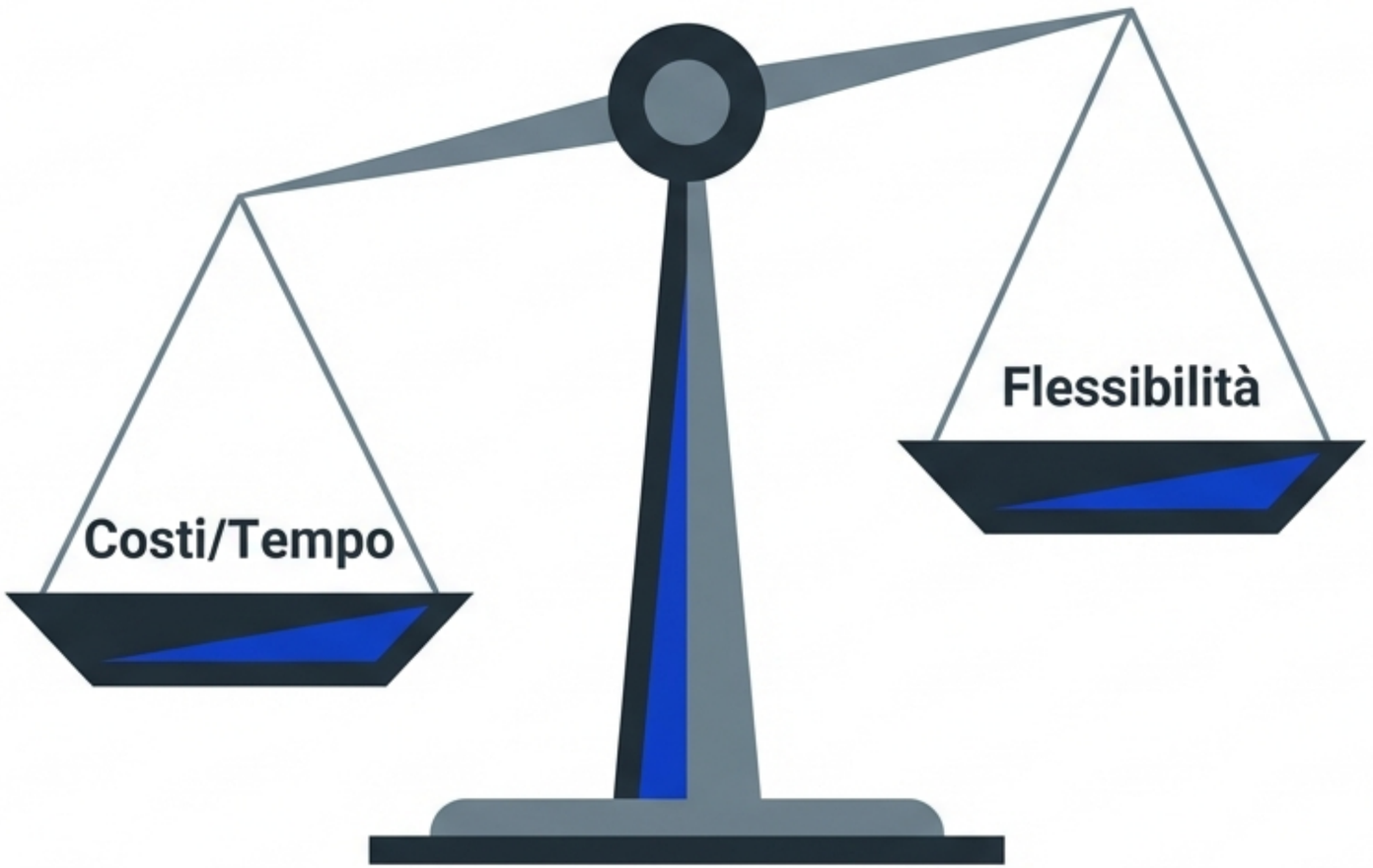
Verifica dell'Efficacia:

Gli auditor devono cercare evidenze concrete di incidenti e tracciarne la gestione nei nuovi controlli, superando la semplice revisione documentale.

Impatto Operativo sugli Organismi di Certificazione (CB)

1. **Gap Analysis**: Obbligo di analizzare le differenze procedurali (es. form UKAS F627).
2. **Aggiornamento Procedure**: Revisione dei ‘quotation tools’ per il calcolo dei tempi e policy per l’audit remoto.
3. **Formazione**: Training obbligatorio per auditor e personale decisionale sulle nuove regole.
4. **Valutazione:** Assessment da parte dell’Ente di Accreditamento (stima: 1.0 - 1.25 giorni uomo).

Impatto sulle Organizzazioni Certificate



Ricalcolo dei Tempi:

- *Possibile Aumento:* Se inclusi molti contractor/freelancer.
- *Possibile Diminuzione:* Se applicabile la riduzione 'radice quadrata'.

Revisione Contrattuale:
I contratti con i CB potrebbero richiedere emendamenti.

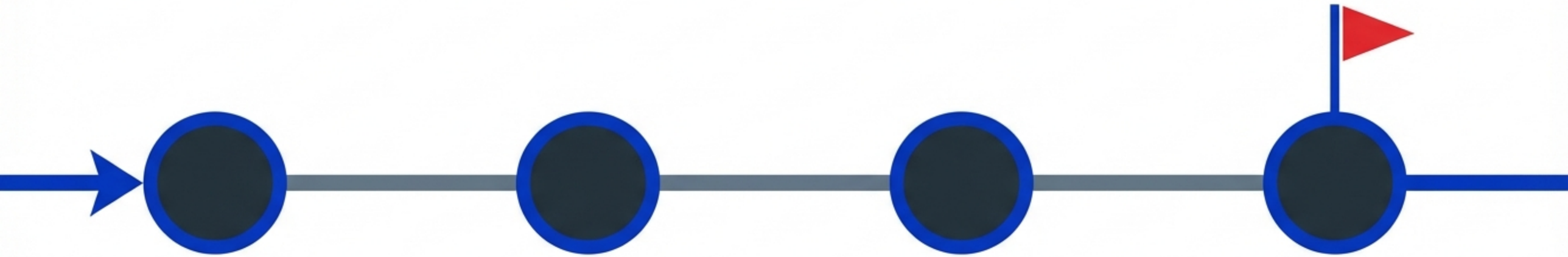
Audit di Transizione:
Previsto tempo extra (0.5 - 1.0 giorni) per verificare l'adeguamento ai nuovi standard.

Trasparenza e Documentazione

Riferimenti ad Altri Standard: (Clausola 8.2.3) Citazioni di standard extra (es. ISO/IEC 27017, 27701) devono essere inequivocabili per evitare di indurre in errore.

Estensioni di Scopo: Nuovi criteri rigorosi per l’aggiunta di perimetri o controlli. Non sono più semplici “aggiunte amministrative” ma richiedono un audit tecnico calcolato.

La Roadmap di Transizione (IAF MD 29)



Marzo 2024:
Pubblicazione Standard

Dicembre 2024:
AB pronti all'assessment

Marzo 2025:
AB usano solo la nuova norma

31 Marzo 2026:
Scadenza Finale (Deadline)

Finestra di 24 Mesi: Il periodo di transizione termina tassativamente il **31 Marzo 2026**. Dopo tale data, gli accreditamenti basati sulla versione 2015 non saranno più validi.

Fonte: IAF Mandatory Document 29.

Conseguenze della Mancata Conformità

Sospensione: Se un Organismo di Certificazione (CB) non completa la transizione, l'accreditamento viene sospeso (max 6 mesi).

Ritiro: La mancata risoluzione porta al ritiro totale dell'accreditamento per lo schema ISMS.

Effetto a Catena: I certificati emessi da un CB non accreditato perdono il riconoscimento IAF MLA, danneggiando la reputazione e la validità commerciale delle aziende clienti.

Verso una Nuova Era dell’Assurance ISMS

Da Burocrazia a Professionalismo: Passaggio da un esercizio rigido a una disciplina basata sul rischio e sulla competenza reale.

Adattabilità: L’integrazione del remoto e del ‘personale effettivo’ riflette la realtà operativa del business digitale globale.

L'Obiettivo Finale: Mantenere alto il valore del certificato ISO 27001, evitando la mercificazione della fiducia (*commoditization of trust*).