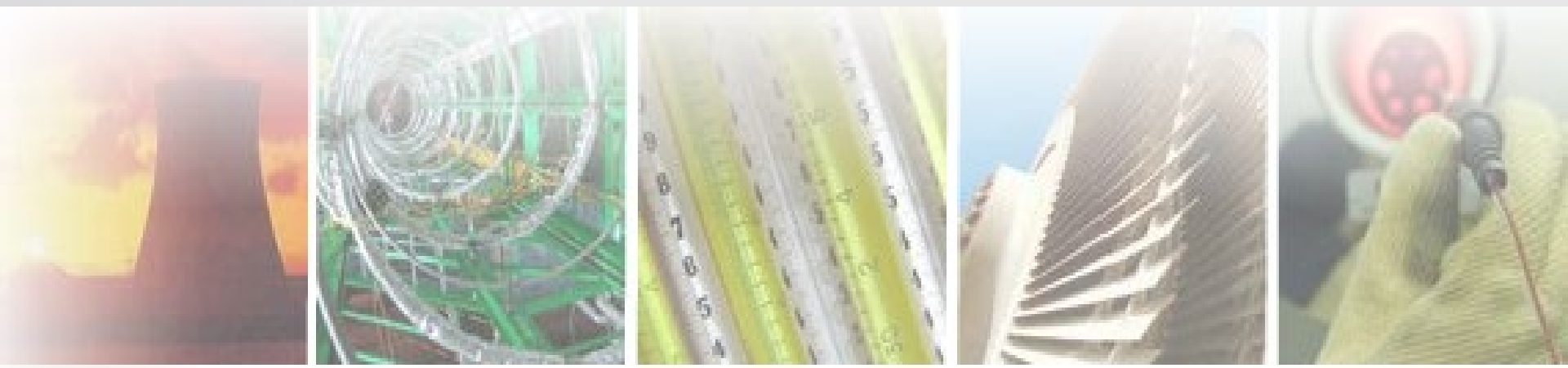


Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

Mauro Molinari

13/02/2026



Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

Gentile Cliente,

in qualità di Organismo di Certificazione, desideriamo informarLa dell'aggiornamento della norma internazionale **ISO/IEC 27006-1:2024**.

Questa norma definisce i requisiti per gli organismi che effettuano audit e certificazione dei Sistemi di Gestione per la Sicurezza delle Informazioni (ISMS) secondo la **ISO/IEC 27001**.

Sebbene la modifica riguardi principalmente le nostre procedure operative, essa introduce novità significative che impatteranno sulle modalità di calcolo delle giornate di audit e sulla gestione delle verifiche.

La transizione alla ISO/IEC 27006-1:2024 non deve essere confusa con la transizione alla ISO/IEC 27001:2022, sebbene le due evoluzioni siano strettamente correlate per garantire un audit efficace e moderno.

Didascalia



00124 Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

AUDIT DA REMOTO

Viene eliminato il limite rigido del 30% per le attività di audit condotte da remoto. È ora possibile una maggiore flessibilità basata sull'analisi del rischio e sulla natura dei processi del cliente.

Se l'organizzazione non ha sedi fisiche, il certificato dovrà indicare esplicitamente che le attività sono svolte da remoto.

Le modifiche riflettono l'evoluzione del mondo del lavoro post-pandemico e l'allineamento con la nuova ISO/IEC 27001:2022. Didascalia



00124 Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

CALCOLO DEI TEMPI DI AUDIT

Definizione di Personale: Il numero di persone coinvolte ora include esplicitamente non solo i dipendenti, ma anche i **collaboratori esterni e freelance** che operano sotto il controllo dell'organizzazione e rientrano nel perimetro del sistema (ISMS).

Esclusione del personale fuori perimetro:

Se l'organizzazione può dimostrare che determinate figure non hanno accesso ai dati, ai sistemi informatici o alle aree sensibili (es. addetti alle pulizie esterne, se non hanno chiavi o accesso libero), queste possono essere escluse dal conteggio iniziale.

Didascalia



Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

CALCOLO DEI TEMPI DI AUDIT

Attività Ripetitive e Gruppi Omogenei

Se un'organizzazione ha un numero elevato di persone che svolgono esattamente le stesse attività sotto lo stesso set di controlli di sicurezza, il rischio e la variabilità diminuiscono. Di conseguenza, è possibile applicare una riduzione al conteggio del personale totale per ottenere il Personale Effettivo su cui calcolare i giorni di audit.

Condizione: Le persone devono operare sotto lo stesso set di controlli tecnici (es. stessa immagine PC, stessi permessi di accesso, stessa formazione).

Esempi: Operatori di data entry, addetti ai call center, personale di magazzino, operatori di sportello bancario.

Didascalia



00134 Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

CALCOLO DEI TEMPI DI AUDIT

Focus sulla complessità: Il calcolo si sposta pertanto da un conteggio basato puramente sul numero di siti / dipendenti a una valutazione basata sul totale delle persone "effettive" e sulla complessità dei processi.

Compile con la massima precisione il modulo di aggiornamento dati inviato da SIET annualmente.

Didascalìa



00124 Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

ALLINEAMENTO DEI CONTROLLI

L'elenco dei controlli di sicurezza è stato aggiornato per riflettere i 93 controlli della ISO/IEC 27001:2022 (suddivisi nelle 4 nuove categorie: **Organizzativi, Personale, Fisici e Tecnologici**)



Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

CALCOLO DEI TEMPI DI AUDIT PER LE ESTENSIONI

Mentre nelle versioni precedenti le estensioni erano spesso lasciate alla discrezionalità dell'auditor, la versione 2024 è molto più prescrittiva: l'incremento non è più un'opzione, ma un requisito se si verificano determinate condizioni di complessità.

Il tempo aggiuntivo deve essere almeno:

- 0,5 giorni se l'audit di estensione è condotto insieme ad una visita di sorveglianza o re-certificazione;
- 1 giorno quando l'estensione è condotta come audit indipendente.

Il capitolo C.7 della ISO/IEC 27006-1:2024 disciplina le cosiddette "Audit time extensions", ovvero le situazioni in cui SIET è obbligata ad aggiungere tempo rispetto alla base calcolata con la Tabella C.1.



00124 Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

CALCOLO DEI TEMPI DI AUDIT PER SITI MULTIPLI

La versione 2024 impone una verifica rigorosa prima di applicare il campionamento.

- Edizione 2015: Il campionamento era generalmente permesso se i siti operavano sotto un unico Sistema di Gestione (ISMS) centralizzato.
- Edizione 2024: Il campionamento (basato sulla formula radice di N è consentito SOLO se i siti svolgono attività sostanzialmente identiche. Se i siti svolgono processi diversi (es. una sede fa sviluppo software, un'altra fa logistica, un'altra è un ufficio vendite), il campionamento non è applicabile. In questo caso, ogni sito deve essere considerato come un'entità separata nel calcolo del tempo.



00124 Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

CALCOLO DEI TEMPI DI AUDIT PER SITI MULTIPLI

Calcolo del Tempo per i Siti Campionati

La modalità di calcolo del tempo totale è stata resa più analitica per evitare che le giornate dedicate ai siti periferici siano insufficienti per una verifica reale.

Il tempo totale di audit a deve risultare dal calcolo basato sul numero delle persone che lavorano per l'organizzazione indipendentemente dalla loro sede.

Novità: Per ogni sito campionato, l'auditor deve ora considerare il personale effettivo specifico di quel sito per determinare la durata minima della visita, invece di spalmare un tempo generico su tutti i siti.



00124 Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

CALCOLO DEI TEMPI DI AUDIT PER SITI MULTIPLI

Calcolo del Tempo per i Siti Campionati

Alternativamente, per giustificato motivi il tempo totale di audit può essere ottenuto come somma di:

- Tempo calcolato per la Sede Centrale (dove risiede il governo dell'ISMS).
- Tempo calcolato per ciascuno dei siti selezionati tramite campionamento.

Metodo utilizzabile solo se il calcolo totale così ottenuto è maggiore del tempo totale ottenuto con il calcolo precedente.



00124 Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

COMPETENZE DEGLI AUDITOR

La norma rimuove i requisiti quantitativi fissi (es. anni minimi di esperienza lavorativa) a favore di una valutazione basata sulle competenze reali, permettendo all'Organismo di assegnare auditor più specializzati in base al contesto tecnologico del cliente.



Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

TEMPISTICHE DI TRANSIZIONE

Data

Evento

Marzo 2024

Pubblicazione della ISO/IEC 27006-1:2024.

31 Marzo 2025

Gli Organismi di Certificazione devono iniziare a utilizzare la nuova norma per tutti i nuovi audit iniziali e di rinnovo.

31 Marzo 2026

Termine ultimo di transizione.

Entro questa data, tutti i clienti certificati dovranno essere stati gestiti secondo i requisiti della nuova edizione 2024.

Tutte le certificazioni basate sulla ISO/IEC 27006-1:2015 scadranno e saranno ritirate alla fine del periodo di transizione.



Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

MODALITÀ DI AGGIORNAMENTO E IMPATTO CONTRATTUALE

Aggiornamento Contrattuale:

Poiché i criteri di calcolo del tempo di audit sono cambiati, SIET dovrà effettuare un nuovo calcolo delle giornate uomo.

- In alcuni casi, la durata dell'audit potrebbe subire variazioni (aumento o diminuzione) in base al nuovo conteggio delle persone in perimetro o alla semplificazione della gestione multi-sito.
- Qualora si rendessero necessarie modifiche alla durata degli audit, riceverete una **nuova offerta tecnica aggiornata**.

La transizione si svolge in modo fluido, solitamente in occasione della prima verifica pianificata (sorveglianza o rinnovo).



00124 Informativa per i Clienti: Transizione alla ISO/IEC 27006-1:2024

COSA DEVO FARE ORA?

Documentazione:

Non è richiesto alcun intervento diretto da parte Vostra sui documenti del Sistema di Gestione.

Come di consueto, durante i contatti per la pianificazione degli audit, il nostro ufficio programmazione vi richiederà i dati aggiornati sul personale (inclusi i collaboratori esterni) per confermare la correttezza della pianificazione secondo i nuovi standard.





Mauro Molinari
Phone: 3459917871
E-mail: molinari@siet.it

