CIRCOLARE TECNICA Prot. DC2023OC022 **DATA** Milano, 02-03-2023

A tutti gli Organismi di certificazione accreditati/accreditandi MS (ISMS)

Alle Associazioni degli Organismi di valutazione della conformità

A tutti gli Ispettori/Esperti del Dipartimento DC

Loro sedi

OGGETTO **Dipartimento Certificazione e Ispezione**

Circolare tecnica DC N° 13/2023 - Disposizioni in materia di transizione delle certificazioni accreditate a fronte della norma ISO/IEC 27001 e relativo adeguamento degli accreditamenti degli Organismi di Certificazione accreditati per lo schema MS (ISMS) per l'edizione 2022.

La presente circolare annulla e sostituisce la circolare tecnica DC N° 04 / 2023

In data 25 Ottobre 2022 è stata pubblicata la norma ISO/IEC 27001:2022 Norma Internazionale ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, norma di riferimento per le certificazioni rilasciate dagli Organismi accreditati per lo schema MS (ISMS)

In accordo con le policy ISO pertinenti, la norma ISO/IEC FDIS 27001:2022 è stata preparata mediante l'integrazione delle ISO/IEC 27001:2013 con la ISO/IEC 27001:2013/COR 1:2014, ISO/IEC 27001:2013/ COR 2:2015 e la ISO/IEC 27001:2013/DAmd1 del luglio2022.

In aggiunta a ciò, ISO ha richiesto che la norma ISO/IEC FDIS 27001:2022 fosse allineata con la struttura armonizzata degli standard per i sistemi di gestione definito nell'allegato SL della ISO/IEC directives parte 1, supplemento ISO consolidato, 2022.

ISO ha pubblicato lo standard ISO/IEC 27001:2022 il 25 Ottobre 2022 a fronte del ballottaggio della FDIS citata: questa sostituisce tutte le norme citate che sono state contestualmente ritirate, ma che continuano a valere nel periodo di transizione della durata di 36 mesi dalla data del ritiro (scadenza 31 ottobre 2025).

In data 15 febbraio 2023 è stata pubblicata la revisione 2 del documento mandatorio IAF MD26, il quale introduce alcune puntualizzazioni sopra riportate circa l'iter di approvazione ed allega un elenco particolareggiato dei cambiamenti chiave (vedi §2.2)

Introduce, detta revisione 2, anche un aggiornamento delle tempistiche che è sotto riportato.

ATTIVITÀ DI CERTIFICAZIONE

Certificazioni già rilasciate a fronte della ISO/IEC 27001:2013

Tutte le certificazioni emesse sotto accreditamento a fronte della ISO/IEC 27001:2013 dovranno essere transitate al nuovo standard entro il 31 ottobre 2025, in caso contrario l'OdC dovrà provvedere alla loro revoca.

Nuove Certificazioni e rinnovi a fronte della ISO/IEC 27001:2022

Dal 30 aprile 2024, tutte le nuove certificazioni ed i rinnovi dovranno essere emesse esclusivamente a fronte della ISO/IEC 27001:2022.

L'attività di adeguamento deve prevedere una durata minima di 0,5 giorni/uomo aggiuntivi se effettuata attraverso un audit di sorveglianza o con un audit dedicato.

ATTIVITÀ DI ACCREDITAMENTO

Nuove domande di Accreditamento

A partire dal **1° maggio 2023** Accredia non accetterà nessuna nuova domanda di accreditamento nello schema MS (ISMS) che faccia riferimento alla norma di certificazione ISO/IEC 27001:2013 ed emetterà nuovi accreditamenti nello schema MS (ISMS) solo a fronte della norma di certificazione ISO/IEC 27001:2022.

Organismi già accreditati MS (ISMS) con riferimento alla ISO/IEC 27001:2013 – gestione della transizione.

Accredia, come richiesto dallo IAF MD:26, verificherà l'adeguamento del processo di certificazione alla nuova norma (verifica di transizione) attraverso un esame documentale della durata minima di 0,5 giorni/uomo.

La verifica documentale potrà, all'occorrenza, essere sostituita con una verifica presso la sede dell'organismo, congiunta ad attività di sorveglianza/rinnovo dell'accreditamento se pianificate entro Luglio 2023.

Gli obiettivi dell'esame documentale prenderanno in considerazione almeno i seguenti elementi:

a) una Gap Analysis delle novità introdotte dalla ISO/IEC 27001:2022;
b) un piano di adeguamento al nuovo standard;
c) le modalità di transizione e le evidenze di implementazione;
d) le registrazioni dell'aggiornamento delle competenze;
e) altri documenti ritenuti pertinenti.

Nel caso siano necessari ulteriori approfondimenti per il completamento della transizione, Accredia si riserva la possibilità di svolgere un'attività supplementare, a carico dell'Odc, di durata adeguata alle carenze riscontrate.

L'OdC dovrà pertanto rendere disponibile ad ACCREDIA:

a) il completamento del piano di aggiornamento;
b) l'aggiornamento dei processi di certificazione;
c) l'aggiornamento delle competenze del personale e dei valutatori;
d) la comunicazione con i clienti circa l'iter di passaggio definito;
e) la pianificazione degli audit di transizione.

A tal proposito si riporta in allegato un documento di esempio.

Solo a fronte del completamento con esito positivo delle attività di adeguamento dell'accreditamento sarà possibile presentare la pratica al comitato settoriale di accreditamento per la delibera di transizione e successivo aggiornamento del certificato di accreditamento.

Gli Odc potranno svolgere audit (iniziali, sorveglianze, rinnovi) ed emettere certificazioni secondo il nuovo standard, solo a completamento positivo dell'iter di transizione (o accreditamento) ivi compresa la delibera da parte del Comitato Settoriale di Accreditamento.

A partire dal **1° novembre 2023**, gli accreditamenti che faranno ancora riferimento alla ISO/IEC 27001:2013 saranno revocati.

L'occasione è gradita per porgere cordiali saluti.

Dott. Emanuele Riva

Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da:
EMANUELE RIVA
Data: 02/03/2023 13:47:25

ALLEGATO

Esempio di Piano di Transizione alla ISO/IEC 27001:2022

Ogni OdC deve compilare questo modulo (o predisporre un documento simile) e renderlo disponibile al Team di verifica ACCREDIA in occasione della verifica di transizione.

È necessario inoltre allegare la documentazione che riporti le evidenze richieste per rispondere alle domande del questionario.

N°	Domanda	Spazio riservato ad ACCREDIA
1.	Piano di transizione È stato predisposto un piano di adeguamento al nuovo standard che comprenda almeno: a) le modifiche previste dal nuovo standard ed una gap analysis; b) le necessità di aggiornamento dei processi di certificazione, documentazione, sistemi IT per la gestione delle attività di certificazione; c) l'aggiornamento delle competenze dei valutatori ai nuovi controlli previsti dalla ISO/IEC 27002:2022 e la loro implementazione (secondo ISO/IEC 27006:2015, 7.1.2.1.3.b); d) una comunicazione al cliente circa il programma di transizione che evidenzi tempistiche, modalità di aggiornamento, e le eventuali conseguenze nel caso la valutazione della transizione abbia risultato negativo entro il periodo di transizione (vedi punto 2)? Allegare evidenze.	Chiusura C ☐ A ☐ Se A, chiarire
2.	Comunicazione al cliente Riguardo l'audit di transizione il cliente è stato informato del fatto che a) l'audit di transizione non si baserà solo sulla revisione dei documenti, in particolare per la revisione dei controlli tecnologici; b) l'audit di transizione deve includere, almeno, quanto segue: – la gap analysis della ISO/IEC 27001:2022, nonché la necessità di modifiche allo schema MS (ISMS); – l'aggiornamento della Dichiarazione di Applicabilità (SoA); – se applicabile, l'aggiornamento del piano di trattamento dei rischi; – l'implementazione e l'efficacia dei controlli nuovi o modificati scelti dai clienti; c) l'OdC può condurre l'audit di transizione da remoto se garantisce il raggiungimento degli obiettivi dell'audit di transizione; d) l'OdC prenderà la decisione di transizione in base al risultato dell'audit di transizione; e) tutte le certificazioni basate su ISO/IEC 27001:2013 scadranno o saranno ritirate alla fine del periodo di transizione;	Chiusura C ☐ A ☐ Se A, chiarire

	f) quando il documento di certificazione viene aggiornato al completamento con successo dell'audit di transizione, la scadenza del suo attuale ciclo di certificazione non verrà modificata, a meno che la transizione venga verificata nell'audit di rinnovo. Inoltre, i clienti certificati sono stati informati della tempistica per la presentazione della domanda di transizione a fronte del programma di audit di transizione? Allegare le evidenze	
3.	Formazione. È stato redatto ed attuato un piano di formazione per il personale addetto al riesame del contratto, i Responsabili dei Programmi di audit, gli Auditor, i Decision Maker?	Chiusura C ☐ A ☐ Se A, chiarire