CIRCOLARE TECNICA

Prot. DC2026SPM088 **Milano**, 17-06-2026

A tutti gli Organismi di certificazione accreditati/accreditandi MS - SSI
Alle Associazioni degli Organismi di valutazione della conformità
A tutti gli Ispettori/Esperti del Dipartimento DC

Loro sedi

OGGETTO: Circolare tecnica DC N° 22/2026 - Disposizioni e aggiornamenti in merito all'accreditamento UNI CEI EN ISO/ IEC 17021 - 1 degli Organismi di Certificazione a fronte della ISO/ IEC 27001

Le presenti disposizioni annullano e sostituiscono quanto riportato nella Circolare tecnica DC N°39/2024.

Premessa

Il presente documento fornisce disposizioni e indirizzi a seguito degli aggiornamenti intercorsi negli ultimi anni nel mondo afferente agli standard relativi alla sicurezza dell'informazione, al loro accreditamento e certificazione. Tra gli elementi salienti in particolare ricordiamo:

1. Lo schema ISMS (ex SSI) è diventato parte integrante dello scopo del certificato unico dei sistemi di gestione (rif. Circolare ACCREDIA DC n.1/2023);
2. Nel febbraio 2024 è stata pubblicata la Norma Internazionale ISO/IEC 27001:2022/Amd 1:2024, che ha integrato i punti norma 4.1 e 4.2 con riferimento ai c.d. "Climate action changes" (rif. IAF/ISO Joint Communication del 22.02.2024);
3. Nel marzo 2024 è stato pubblicato il nuovo standard di livello 4 ISO/IEC 27006 -1:2024, *Information security, cybersecurity and privacy protection, Requirements for bodies providing audit and certification of information security management systems, Part 1: General*, che sostituisce la precedente versione del 2015 emendata ulteriormente nel 2020. Nel presente documento sono delineate le modalità operative per la transizione in recepimento del documento IAF MD29 "Transition Requirements for ISO/IEC 27006 -1:2024";
4. Diverse linee guida normative sono attualmente in fase di sviluppo e aggiornamento, es.: ISO/IEC DIS 27000, ISO/IEC 27017 (in fase di pubblicazione), ISO/IEC FDIS 27090.

Restano ferme tutte le disposizioni espressamente previste dallo standard di livello 3 (UNI CEI EN ISO/IEC 17021-1), di livello 4 (ISO/IEC 27006 -1), di livello 5 (ISO/IEC 27001) e dei Regolamenti Accredia pertinenti.

Regole di Certificazione

La serie ISO/IEC 27000 è ormai popolata di standard di varia natura, taluni di tipo A, altri di tipo B in relazione alla classificazione ISO[1]. Alla luce di ciò, si ritiene di dover fornire ulteriori precisazioni in merito alle modalità applicabili per la certificazione sotto accreditamento.

Prescrizioni generali

- Con riferimento al req. 6.1.2, 8.2 e A.8.8 della ISO/IEC 27001 e al, l'OdC deve accertare se l'Organizzazione si sottopone periodicamente a vulnerability assessment e/o penetration test tenuto conto del livello di rischio a cui l'infrastruttura e l'Organizzazione tutta è esposta. Ciò vale anche per la valutazione della frequenza temporale con la quale tali valutazioni devono essere ripetute. A fronte di tali attività, il CAB deve verificare che siano conservate opportune registrazioni sulla qualifica del personale e/o del laboratorio incaricato e sulle azioni adottate per ridurre l'esposizione alle minacce;

- Ove applicabile, l'OdC deve verificare come l'Organizzazione cliente garantisce la sicurezza delle informazioni relativa alle infrastrutture utilizzate per l'elaborazione dei dati, sia che si tratti di semplici server fisici proprietari residenti presso la sede dell'organizzazione, sia che si tratti di servizi Cloud (privato, ibrido, esterno) o di housing o di hosting presso specifici Data Center di fornitori esterni. Le modalità di auditing dovranno prevedere, inoltre, la verifica del mantenimento nel tempo dei livelli di affidabilità ed efficacia, con riferimento alla sicurezza delle informazioni e cybersecurity, delle soluzioni individuate;

  Si rappresenta che la sussistenza di certificati di conformità accreditati in ambito EA/MLA che coprano le infrastrutture e i servizi esterni (es. Cloud) è presunzione di conformità ai requisiti applicabili, diversamente l'OdC deve sottoporre ad audit lo specifico sito e mantenere le relative registrazioni;

- In merito ai criteri di competenza del personale dell'OdC si applicano le prescrizioni dello standard di livello 4 (ISO/IEC 27006-1). Si rende, in ogni caso, necessario richiamare gli OdC in merito alla valutazione del continuo aggiornamento delle competenze degli auditor, con speciale riferimento alle aree tecniche nelle quali gli stessi sono impiegati (sanità, automobilistico, aerospazio e difesa, medicale, alimentare, etc.) A questo proposito un riferimento utile può essere rappresentato dagli elenchi riportati nei settori merceologici cui fa riferimento la Direttiva NIS2;

- In merito ai criteri di calcolo delle durate degli audit si applicano le prescrizioni dello standard di livello 4 (ISO/IEC 27006-1). Le riduzioni dei tempi di audit devono essere giustificate in maniera dettagliata e supportate da evidenze documentate. Si rappresenta inoltre che la sussistenza di certificazioni per altri sistemi di gestione, anche se rilasciate dello stesso CAB, non è – da sola – motivo per considerare il sistema di gestione "maturo", se non vi è evidenza di risultanze (assenza di non conformità) e conclusioni positive dall'ultimo audit di III parte svolto, che diano

[1] https://www.iso.org/management-system-standards-list.html

evidenza di audit interni efficaci da parte dell'Organizzazione in grado di rilevare le problematiche di sicurezza e le azioni di miglioramento continuo.

Si tenga infine in considerazione che il numero di addetti da considerare nel calcolo g/u deve tener conto anche dei servizi che l'organizzazione intende inserire nel campo di applicazione oggetto di certificazione, in tal senso si sottolinea che l'efficacia del sistema di gestione non è responsabilità esclusiva delle figure deputate alla gestione dell'infrastruttura ICT, ma di chiunque gestisca, a diverso titolo, le informazioni.

In particolare, la ISO/IEC 27001 si applica a sistemi di gestione della sicurezza delle informazioni senza limitazioni, è uno standard di Tipo A che segue la struttura HS di ISO (c.d. Harmonized Structure). Lo scopo di certificazione rilasciato dall'OdC deve contenere espresso riferimento alla SoA ed al suo stato di aggiornamento, coerentemente ai processi inseriti nel perimetro del sistema di gestione oggetto di certificazione. Esso deve essere completamente riportato in Banca dati Accredia delle certificazioni rilasciate dall'OdC secondo le regole già note.

Esempio scopo:

"*Progettazione ed erogazione di servizi di Housing, hosting, disaster recovery, business continuity. Progettazione ed erogazione dei servizi di cloud computing, IaaS, PaaS e SaaS. Erogazione di servizi di sviluppo, gestione e manutenzione di applicazioni. Erogazione di servizi di gestione dell'identità digitale e di sicurezza applicativa erogati in modalità sia as a service sia on premise secondo lo Statement of Applicability Rev.0 del gg/mm/aaaa.*"

ISO/IEC 27017, 27018

e altre Linee guida o standard di Tipo B della serie ISO/IEC 27000

Si tratta principalmente di standard Tipo B, in altri casi di linee guida, a tutti gli effetti utili per individuare i controlli operativi ritenuti necessari nell'ambito dello ISMS. Tali standard non sono certificabili.

Tuttavia, qualora l'Organizzazione richiedente fosse in grado di dimostrare la corretta applicazione di tali standard, l'OdC deve accertarne l'applicazione dei controlli.

In tali casi, per il calcolo della durata dell'audit di estensione dello scopo, l'OdC deve considerare un tempo aggiuntivo (al netto delle riduzioni applicabili), per ogni verifica e in qualsiasi fase, di almeno 1 g/u per standard ulteriore applicato.

Resta a carico dell'OdC dimostrare la competenza, e relativo mantenimento, degli auditor che conducono attività di valutazione a fronte di tali standard.

Lo scopo di certificazione rilasciato dall'OdC deve contenere espresso riferimento alla SoA, al suo stato di aggiornamento ed agli ulteriori standard presi a riferimento per i controlli. Il certificato, in ogni caso, deve chiarire la conformità unicamente allo standard di Tipo A. Esempio scopo:

"*Progettazione, sviluppo, manutenzione e assistenza software, erogazione di servizi SaaS (software as a service) secondo lo Statement of applicability Rev.0 del gg/mm/aaaa integrato dai controlli previsti dalle linee guida ISO/IEC 27017:xxxx e ISO/IEC 27018:xxxx.*"

Le certificazioni che inglobano la ISO/IEC 27017 e ISO/IEC 27018 o altre Norme dello stesso tipo, restano valide fino alla naturale scadenza del certificato o alla prima modifica utile (es.: estensione o modifica scopo). Successivamente dovranno essere adeguate alle indicazioni del presente documento.

Gestione dello scopo flessibile

Con la pubblicazione della ISO/IEC 27701:2025, tale norma assume la configurazione di standard autonomo per la certificazione dei sistemi di gestione per la privacy — Privacy Information Management System, PIMS — e non costituisce più una mera estensione della certificazione ISO/IEC 27001. Per effetto di tale evoluzione normativa, nell'ambito della famiglia ISO/IEC 27000 non risultano più presenti ulteriori norme di sistema di gestione di tipo A certificabili come schemi dipendenti o direttamente collegati alla ISO/IEC 27001, fatta salva la ISO/IEC 27001 stessa quale norma di riferimento per la certificazione dei sistemi di gestione per la sicurezza delle informazioni. Ne consegue che non sussistono più le condizioni per il mantenimento di scopi di accreditamento flessibili riferiti alla famiglia delle norme ISO/IEC 27000. Pertanto, a decorrere dal 1° luglio 2026, ACCREDIA non accetterà nuove domande di accreditamento o estensione dell'accreditamento con scopo flessibile riferito a tale famiglia normativa. Gli Organismi già accreditati con scopo flessibile per la famiglia ISO/IEC 27000 dovranno procedere alla rinuncia dello scopo flessibile e richiedere il riallineamento dello scopo di accreditamento in forma fissa alla ISO/IEC 27001 nella versione vigente.

Il termine ultimo per il completamento del processo di rinuncia dello scopo flessibile per le norme della famiglia ISO/IEC 27000 è il 31 ottobre 2027. Dal 1° novembre 2027 tutti gli accreditamenti con scopo flessibile per le norme della famiglia ISO/IEC 27000 saranno revocati.

Banca dati ACCREDIA delle certificazioni rilasciate

Come noto, gli OdC sono tenuti a trasmettere ad ACCREDIA-DC tramite il servizio web – SIAC i dati relativi ai soggetti in possesso di certificazioni da essi rilasciate, secondo le procedure definite da ACCREDIA-DC e i relativi Regolamenti (RG01 §1.10.7).

Le certificazioni devono essere tracciate in Banca dati con espresso riferimento alle sole norme quali standard di ISO di tipo A, ovvero ISO/IEC 27001 e ISO/IEC 27701. Qualora vi sia l'utilizzo di altri standard della serie ISO 27000, questi devono essere riportati nella descrizione dello scopo di certificazione, come precedentemente esemplificato. Tali prescrizioni si applicano anche agli accreditamenti concessi con scopo flessibile.

Regole di Accreditamento

A	OdC già accreditato per lo schema UNI CEI EN ISO/IEC 17021-1:2015	• Esame documentale di 0,5 g/u; • Verifica ispettiva presso la sede dell'OdC della durata di 1 g/u; • 1 (una) Verifica in accompagnamento di durata adeguata a coprire l'analisi degli elementi salienti del processo di audit condotto dal CAB. A ciascuna verifica in accompagnamento si applica 1 g/u di rapportazione qualora le attività siano svolte disgiuntamente.

B	OdC non ancora accreditato UNI CEI EN ISO/IEC 17021-1:2015 ma accreditato per altri schemi di accreditamento (Livello 3)	• Esame documentale di 1 g/u; • Verifica ispettiva presso la sede dell'OdC della durata di 2 g/u; • 1 (una) Verifica in accompagnamento di durata adeguata a coprire l'analisi degli elementi salienti del processo di audit condotto dal CAB. A ciascuna verifica in accompagnamento si applica 1 g/u di rapportazione qualora le attività siano svolte disgiuntamente.
C	OdC non accreditato	• Esame documentale di 1 g/u da svolgersi in parte in modalità sincrona da remoto; • Verifica ispettiva presso la sede dell'OdC della durata di 4 g/u; • 1 (una) Verifica in accompagnamento di durata adeguata a coprire l'analisi degli elementi salienti del processo di audit condotto dal CAB. A ciascuna verifica in accompagnamento si applica 1 g/u di rapportazione qualora le attività siano svolte disgiuntamente.

Mantenimento dell'Accreditamento

N. Certificati rilasciati	N. Verifiche nel ciclo di accreditamento
0÷50	4 Verifiche in sede 1 Verifiche in accompagnamento
51÷150	4 Verifiche in sede 2 Verifiche in accompagnamento
>150	4 Verifiche in sede 4 Verifiche in accompagnamento

Documentazione da presentare ad ACCREDIA-DC per l'esame documentale

Oltre a quanto elencato nella domanda di accreditamento DA-01 si richiede l'invio di:

a. Liste di riscontro, linea guida, istruzioni predisposte dall'OdC per il GVI;
b. Criteri di qualifica e curricula del personale addetto al riesame del contratto, degli auditor e dei decision maker;
c. Template di Certificato rilasciato dall'OdC;
d. Procedure applicabili al processo commerciale per la definizione dei tempi di audit, nonché le procedure per la gestione della pratica di certificazione.

L'occasione è gradita per porgere cordiali saluti.

Firmato digitalmente da: MARIAGRAZIA LANZANOVA
Data: 17/06/2026 16:26:36