CIRCOLARE TECNICA Prot. DC2024SPM123 **DATA** Milano, 26-11-2024

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 **Dipartimento Certificazione e Ispezione**

Circolare tecnica DC N° 39/2024 - Disposizioni e aggiornamenti in merito all'accreditamento ISO/IEC 17021-1 degli Organismi di Certificazione a fronte della ISO/IEC 27001 e ISO/IEC 27701

Le presenti disposizioni annullano e sostituiscono quanto riportato nei documenti:

- Circolare Tecnica N° 02/2018;
- Circolare Informativa N° 01/2019;
- Circolare Tecnica N° 10/2019;
- Circolare Informativa DC N° 02/2021.

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. diversi standard o linee guida sono attualmente in fase di sviluppo e aggiornamento, es.: ISO/IEC DIS 27701, ISO/IEC FDIS 27706, ISO/IEC CD 27017, ISO/IEC DIS 27018, ISO/IEC 27011, ISO/WD 27799. Altri risultano già pubblicati: ISO/IEC 27019:2017, ISO/IEC 27035-1:2023, ISO/IEC 27032:2023.

Restano ferme tutte le disposizioni espressamente previste dallo standard di livello 3 (ISO/IEC 17021-1), di livello 4 (ISO/IEC 27006-1 oggetto di transizione e ISO/IEC TS 27006-2), di livello 5 (ISO/IEC 27001 e ISO/IEC 27701) e dei Regolamenti Accredia pertinenti.

Transizione ISO/IEC 27006-1:2024

In data 20 marzo 2024 è stata pubblicata la norma internazionale ISO/IEC 27006-1:2024 che sostituisce la precedente ISO/IEC 27006 del 2015 ed incorpora l'Amd. 1:2020.

I principali cambiamenti contenuti nella ISO/IEC 27006-1:2024 sono:

1. una migliore precisazione in merito ai requisiti per gli audit da remoto (si veda par. 9.1.3 e 9.4.3.2);
2. aggiornamento del requisito di calcolo del tempo di audit (si veda Allegato C);
3. aggiornamento dell'Allegato D della versione 2015, che è stato allineato ai controlli di sicurezza delle informazioni elencati nell'allegato A della norma ISO/IEC 27001:2022 e trasferito come Allegato E nella versione 2024;
4. precisazione in merito al riferimento ad altri standard nei documenti di certificazione dell'ISMS (si veda par. 8.2.3);
5. rimozione delle ridondanze con lo standard di Livello 3 ISO/IEC 17021-1:2015. Si veda ad esempio i punti 5.2, 7.1.3, 9.3.2.2 e 9.4 della ISO/IEC 27006-1:2024;
6. eliminazione del requisito minimo in termini di anni di esperienza lavorativa e per la formazione degli auditor dell'ISMS, ad esempio, esperienza pratica sul posto di lavoro a tempo pieno di 4 anni.

Per ulteriori dettagli sulle modifiche si fa espresso rimando al documento IAF MD 29, dal quale è possibile, inoltre, trarre le seguenti disposizioni sul periodo transitorio:

Transizione accreditamenti	• 01.12.2024: avvio delle attività di valutazione a fronte della nuova norma da parte di ACCREDIA-DC. • 30.03.2025: termine ultimo per la gestione delle attività di accreditamento o di estensione di accreditamento a fronte della ISO/IEC 27006:2015+Amd1:2020. • 31.03.2026: termine ultimo per il completamento della transizione degli accreditamenti. A partire dal 01.04.2026, gli accreditamenti non ancora adeguati saranno revocati.
Transizione certificazioni	• Dall'ottenimento dell'accreditamento adeguato al nuovo standard, l'OdC può utilizzare la versione superata dello standard solo per le attività di sorveglianza. • 31.03.2026: termine ultimo per il completamento della transizione delle certificazioni.

Sempre in accordo al documento IAF MD29, ACCREDIA-DC verificherà l'adeguamento del processo di certificazione alla nuova norma (verifica di transizione) attraverso un esame documentale off-site della durata di 1 gg/u. Per la conduzione dell'esame documentale verranno richiesti e valutati i documenti previsti dal par. 4.2 del documento IAF MD29, si veda inoltre l'Allegato "Self Assessment Piano di transizione".

Si rappresenta da ultimo che la nuova ISO 27006-1 conferma nuovamente la raccomandazione (req. 10.1.2) per l'OdC, affinché anch'esso implementi un sistema di gestione della sicurezza delle informazioni in accordo alla ISO/IEC 27001. Visto il contesto storico attuale, si invitano gli OdC a valutare attentamente tale aspetto.

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, 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 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 degli standard di livello 4 (ISO/IEC 27006-1 e ISO/IEC 27006-2). 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,

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

	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 degli standard di livello 4 (ISO/IEC 27006-1 e ISO/IEC 27006-2). 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 dimostrazione 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.
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). Tale norma è certificabile secondo le regole già note e consolidate in accordo ai Regolamenti di accreditamento. 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 27701	Si applica a sistemi di gestione per la sicurezza delle informazioni progettati per consentire l'aggiunta di requisiti specifici per la gestione dei dati personali. Si tratta di uno standard di Tipo A, che tuttavia non segue la struttura HS. Tale norma è certificabile quale estensione della ISO/IEC 27001, quindi non sono ammesse certificazioni stand-alone.

	Pertanto, il certificato di conformità ISO/IEC 27701 deve essere espressamente collegabile al certificato ISO/IEC 27001 di cui è una estensione. Esempio scopo: *"Sistema di gestione dei dati personali, in qualità di Titolare e Responsabile, in relazione ai seguenti processi.* • *progettazione ed erogazione di servizi ICT infrastrutturali di Data Center quali Housing, Networking, Disaster Recovery;* • *progettazione ed erogazione di servizi di call center inbound e outbound in modalità IaaS (Infrastructure as a Service) SaaS (Software as a Service) e PaaS (Platform as a Service* • *progettazione, sviluppo e mantenimento dei servizi di banking online, di strumenti e di servizi a supporto della progettazione e dello sviluppo applicativo e della gestione dei sistemi e delle reti informatiche siti nella Server Farm* *secondo lo specifico Statement of Applicability riportato nel certificato n. xxxxx"* [con "xxxxx" si intende il numero del certificato ISO 27001 collegato]
ISO/IEC 27017, 27018 e altre Linee guida o standard di Tipo B della serie ISO/IEC 27000	Si tratta in alcuni casi di standard Tipo B, in altri 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 27017:2015 e ISO/IEC 27018:2019."*

In merito alla gestione degli scopi flessibili, fermo restando le disposizioni del Regolamento Tecnico RT-37, gli unici standard che possono rientrarvi sono quelli di Tipo A, ovvero ad oggi, la ISO/IEC 27001 e la ISO/IEC 27701.

Per gli adeguamenti sugli accreditamenti e certificazioni rilasciate si applicano i seguenti criteri:

- gli accreditamenti rilasciati a fronte della ISO/IEC 27017, ISO/IEC 27018 o altre linee guida saranno revocati a far dalla data del 01.03.2025;
- 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;
- tutte le disposizioni riportate nel presente documento si intendono pienamente in vigore a far dalla data del 1.1.2025.

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 gli schemi ISO/IEC 17021-1:2015 e ISO/IEC 27001	• Esame documentale di 0,5 g/u da svolgersi in parte in modalità sincrona da remoto; • 1 Verifica in accompagnamento di durata adeguata per l'estensione ISO/IEC 27701.
B	OdC già accreditato per lo schema 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 per ciascuno schema richiesto (es.: ISO/IEC 27001 e ISO/IEC 27701). A ciascuna verifica in accompagnamento si applica 1 g/u di rapportazione qualora le attività siano svolte disgiuntamente.
C	OdC non ancora accreditato 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 per ciascuno schema richiesto (es.: ISO/IEC 27001 e ISO/IEC 27701). A ciascuna verifica in accompagnamento si applica 1 g/u di rapportazione qualora le attività siano svolte disgiuntamente.

D	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 per ciascuno schema richiesto (es.: ISO/IEC 27001 e ISO/IEC 27701). A ciascuna verifica in accompagnamento si applica 1 g/u di rapportazione qualora le attività siano svolte disgiuntamente.

	N. Certificati rilasciati	N. Verifiche nel ciclo di accreditamento
Mantenimento dell'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.

Dott.ssa Mariagrazia Lanzanova

Vice Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da: MARIAGRAZIA LANZANOVA
Data: 26/11/2024 14:28:36