Prot. DC2019SPM368 Milano, 13/12/2019

A tutti gli Organismi di Certificazione accreditati o accreditandi per lo schema SSI

Alle Associazioni degli Organismi di valutazione della Conformità
Loro Sedi

Oggetto: **<u>Dipartimento DC - Circolare Tecnica N° 10/2019</u>**
Disposizioni in merito all'accreditamento norma ISO/IEC 27701

Nel mese di agosto del corrente anno è stata pubblicata la Norma ISO/IEC 27701, che fornisce i requisiti per integrare la Norma ISO/IEC 27001:2013 estendendo lo scopo di applicazione di quest'ultima al perimetro della gestione della Privacy [Privacy Information Management System].

Segnaliamo che, anche se molti argomenti trattati dalla Norma hanno riscontro in specifici requisiti di legge nazionali, sia in Italia, sia in altri Paesi dell'Unione Europea, disciplinati dal GDPR e dalle precedenti Leggi nazionali, la Norma, basandosi sulla ISO 17021-1, non è da considerarsi valida ai fini del GDPR, che prevede invece una certificazione accreditata IS0 17065.

La Norma, essendo una estensione della ISO/IEC 27001 deve tener conto della interpretazione della stessa alla luce della ISO/IEC 27002. Pertanto, l'applicazione della ISO/IEC 27701 non può essere a sé stante, ma deve appoggiarsi all'applicazione delle Norme citate.

Può essere utile, ai fini dell'interpretazione dei requisiti della Norma ISO/IEC 27701, tenere in conto anche le indicazioni delle Norme della serie ISO/IEC 29100 e di quanto prescritto per i processi gestiti con strumenti "cloud" delle indicazioni della Norma ISO/IEC 27018, la quale, a sua volta, poggia sui requisiti della Norma ISO/IEC 27017.

La Norma ISO/IEC 27701, a richiesta dei CAB accreditati nello schema SSI e interessati, può essere oggetto del processo di "Accreditamento Flessibile", per come indirizzato dal documento RT-37, entrato in vigore il 01 Gennaio 2018.

1) Norma e regole di Certificazione

Norma di Accreditamento	ISO/IEC 17021-1:2015, ISO/IEC 27006:2015
Norma di Certificazione	ISO/IEC 27701 La Norma ISO/IEC 27701 può essere oggetto di estensione della certificazione anche da sola, ma occorre che l'organizzazione sia già certificata a fronte della Norma ISO/IEC 27001, sotto accreditamento, anche da un differente organismo.
Criteri da adottare per la Certificazione	a) Ai fini della integrazione di un certificato ISO/IEC 27001 esistente, a fronte della norma ISO/IEC 27701, valgono i seguenti criteri: 1) L'estensione può essere garantita solo dopo una verifica che dovrà essere eseguita presso il sito/i siti interessati dell'organizzazione. 2) Se l'organizzazione è già in possesso di una certificazione ISO/IEC 27001, emessa dallo stesso CAB e con uno scopo di certificazione compatibile con i processi coperti dalle Norma ISO/IEC 27701, l'audit di estensione sarà condotto in un'unica fase, integralmente svolta presso la sede

Sede operativa e amministrativa: Via Tonale, 26 | 20125 Milano - Italy | Tel. +39 02 2100961 | Fax +39 02 21009637
Sede legale: Via Guglielmo Saliceto, 7/9 | 00161 Roma - Italy | Tel. +39 06 8440991 | Fax +39 06 8841199
milano@accredia.it | www.accredia.it | Partita IVA - Codice Fiscale 10566361001

	dell'organizzazione. La durata dell'audit di estensione dovrà essere di almeno il 30% del tempo di audit di un rinnovo di certificazione ISO/IEC 27001 (tempo necessario all'audit di ogni linea guida), con una durata minima di una giornata per il sito principale e mezza giornata per ogni sito interessato dall'estensione. 3) Se l'organizzazione è in possesso di altra certificazione ISO/IEC 27001 sotto MLA, dovrà richiedere il trasferimento della stessa al CAB accreditato ACCREDIA, per consentire l'emissione del certificato integrato. 4) Se l'organizzazione non è già in possesso di una certificazione valida e riconosciuta sotto accreditamento per la Norma ISO/IEC 27001, l'audit sarà svolto secondo i criteri di una nuova certificazione a fronte delle Norme ISO/IEC 27001, con l'aggiunta per la ISO/IEC 27701 di un incremento minimo del tempo di audit non inferiore al 30% del tempo per una prima certificazione ISO/IEC 27001 (tempo necessario per ogni linea guida che viene adottata per lo schema afferente alla protezione dati; quindi per organizzazioni che operano utilizzando servizi erogati con modalità "cloud" il tempo sarà quello relativo alle tre linee guida applicabili e mandatorie) e, comunque, non inferiore a un giorno per il sito principale e mezza giornata per ogni sito aggiuntivo campionato. 5) Per le sorveglianze, si applica sempre l'aumento di almeno una giornata per il sito principale e mezza giornata per ogni sito campionato, per linea guida. Se vengono adottati servizi "cloud" si sommano anche i tempi per le sorveglianze sulle linee guida ISO/IEC 27017 e 27018. 6) Le modalità di auditing dovranno sempre prevedere la registrazione delle evidenze necessarie a garantire la completa ed esaustiva applicazione sia dei requisiti della Norma ISO/IEC 27001, sia dei requisiti aggiuntivi pertinenti alla ISO/IEC 27701. 7) Si dovrà inoltre verificare se l'organizzazione si sottopone periodicamente a vulnerability assessment / penetration test, e con quali modalità (es. vulnerability assessment condotti da LAB accreditati, penetration test condotti da LAB che abbiano caratteristiche organizzative e gestionali equivalenti ai requisiti della Norma ISO/IEC 17025). 8) Occorre inoltre prevedere la verifica dell'adeguatezza dei data center attraverso, ad esempio, la verifica diretta dell'ambiente fisico, garanzie messe a disposizione da eventuali fornitori, rapporti di audit di prima o di seconda parte. Le modalità di auditing dovranno prevedere, inoltre, la verifica del mantenimento dei criteri adottati per la valutazione dell'adeguatezza dei data center. b) Estensioni incrementali:

	1) Non è ammessa l'estensione alla ISO/IEC 27701, per organizzazioni che utilizzano servizi erogati con modalità "cloud", senza il supporto della ISO/IEC 27017:2015 e della ISO/IEC 27018. 2) È comunque possibile che una organizzazione, già certificata ISO/IEC 27001, richieda l'estensione della certificazione alla ISO/IEC 27701 separatamente da una verifica di sorveglianza o rinnovo ISO/IEC 27001. c) Audit di sorveglianza e rinnovo: 1) Tali audit saranno condotti sempre su tutte le Norme applicabili di estensione alla ISO/IEC 27001:2013, prevedendo: 2) Sorveglianza: un incremento minimo del tempo di audit non inferiore al 30% del tempo di una sorveglianza (tempo necessario all'audit di ogni linea guida, pertanto per tre linee guida il tempo aggiuntivo sarà almeno tre volte il 30%) e non inferiore a mezza giornata per ogni sito aggiuntivo campionato ove adottata una sola linea guida o una giornata per le tre linee guida. 3) Rinnovo: dovrà prevedere un incremento minimo del tempo di audit non inferiore al 30% del tempo di una ricertificativa (tempo necessario all'audit di ogni linea guida, pertanto per tre linee guida il tempo aggiuntivo sarà almeno tre volte il 30%) e una mezza giornata per ogni sito aggiuntivo campionato ove adottata una sola linea guida o una giornata per le tre linee guida.
Criteri di competenza del Gruppo di Verifica dell'OdC	All'interno del gruppo di verifica devono essere disponibili queste competenze, facenti capo ad una persona singola, o al Team nel suo complesso: 1) auditor ISO/IEC 27001:2013, con esperienza specifica di audit nella ISO/IEC 27001 di almeno 5 anni, preferibilmente in possesso di certificazione professionale. 2) Per le organizzazioni che operano con servizi "cloud" deve inoltre essere data dimostrazione della conoscenza delle norme ISO/IEC 27017 e ISO/IEC 27018 e della normativa in tema di GDPR. Si ritiene soddisfatto questo requisito per il personale certificato sotto accreditamento a fronte della UNI 11697. 3) Conoscenza del GDPR (es: almeno 24 ore di formazione documentata in materia di protezione dei dati personali), o altra legislazione applicabile al Paese oggetto di audit. Per attività svolte in Italia, si ritiene soddisfatta questa condizione per figure professionali certificate sotto accreditamento in base alla UNI 11697, o altra normativa equivalente. 4) Conoscenza degli elementi caratterizzanti la gestione della qualità o dei servizi IT (es. ISO 9001, ITIL, ISO/IEC 20000-1).
Criteri di competenza del Decision maker	Per almeno un membro dell'Organo di Delibera è richiesta agli OdC la dimostrazione della:

	1) Qualifica come ispettore ISO/IEC 27001, rilasciata in conformità alla ISO/IEC 27006 2) Conoscenza della norma ISO/IEC 27701
Certificato	Deve fare sempre riferimento alla Norma ISO/IEC 27001 citando l'utilizzo della norma ISO/IEC 27701 nella sua applicazione. Devono essere indicati i prodotti / servizi / applicazioni / processi coperti dalla certificazione.
Documenti IAF e EA	Si applicano tutti i documenti IAF ed EA in vigore per lo schema ISO/IEC 27001.

2) Processo di Accreditamento ACCREDIA

Si potranno presentare diverse casistiche, in base agli accreditamenti ACCREDIA già posseduti dall'Organismo di Certificazione che presenta la domanda di accreditamento o estensione.

Rimangono invariati i prerequisiti previsti dal RG-01 ed RG-01-01 per la concessione dell'accreditamento ed estensione.
Per organismi già accreditati ISO/IEC 27001, non occorre che questi abbiano già rilasciato dei certificati in questo schema per fare domanda di estensione dell'accreditamento.

Il certificato di accreditamento non riporta settori di accreditamento.

Nel caso in cui l'OdC possegga già accreditamenti rilasciati da altri enti di accreditamento, dovrà essere fatta una valutazione caso per caso, in base agli accordi EA / IAF MLA applicabili.

A	OdC già accreditato per lo schema ISO/IEC 27001	Esame documentale di 0,5 giornate. 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
A1	OdC già accreditato per lo schema ISO/IEC 27001 con scopo flessibile	Esame documentale di 0,5 giornate. Lo scopo flessibile prevede l'estensione a nuove norme senza necessità di attività in campo da parte dell'Organismo di accreditamento. L'OdC puo' inserire nuove norme nel suo elenco e successivamente durante la sorveglianza Accredia verificherà come l'OdC ha gestito l'estensione dello scopo alla nuova norma nello scopo flessibile.
A1	OdC già accreditato per lo schema ISO/IEC 27001 da almeno 2 anni, ma non con scopo flessibile	È facoltà dell'organismo fare richiesta di scopo flessibile. Si rimanda per maggiori informazioni alla procedura RT-37 rev.00 – Prescrizioni per l'accreditamento con scopo di accreditamento flessibile. Per l'estensione allo scopo flessibile, occorre fare un esame documentale di 1 giornata.
B	OdC non ancora accreditato ISO/IEC 27001, ma accreditato ISO/IEC 17021 per altri schemi	È necessario aver prima conseguito l'accreditamento ISO/IEC 27001. Di seguito quindi le indicazioni per ottenere l'accreditamento ISO/IEC 27001 e ISO/IEC 27701. Esame documentale di 1 giornata (da svolgersi possibilmente presso l'OdC).

		Verifica ispettiva presso la sede dell'OdC di 2 giornate. 1 Verifica in accompagnamento ISO/IEC 27001 di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza. 1 Verifica in accompagnamento ISO/IEC 27701 di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.
C	OdC non ancora accreditato ISO/IEC 17021	È necessario aver prima conseguito l'accreditamento ISO/IEC 27001. Di seguito quindi le indicazioni per ottenere l'accreditamento ISO/IEC 27001 e ISO/IEC 27701. Esame documentale di 1 giornata (da svolgersi possibilmente presso l'OdC). Verifica ispettiva presso la sede dell'OdC di 4 giornate. 1 Verifica in accompagnamento ISO/IEC 27001 di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza. 1 Verifica in accompagnamento ISO/IEC 27701 di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accreditamento e le successive attività di sorveglianza.

Documentazione da presentare ad Accredia per l'esame documentale:

a) Lista di riscontro o linea guida o istruzioni eventualmente predisposte dall'Odc per il GVI;
b) Criteri di qualifica di chi svolge il riesame del contratto, degli auditor e dei decision maker;
c) Curricula degli ispettori e dei decision maker e giustificazione per la loro singola qualifica;
d) Procedura per la costituzione e gestione dei Gruppi di Audit;
e) Template di attestato/Certificato rilasciato dall'OdC;
f) Lista degli eventuali certificati già emessi e delle prossime attività di verifica (dato necessario per poi pianificare la verifica in accompagnamento);
g) Procedure / regolamenti contrattuali applicabili alla verifica, nonché le procedure interne per la gestione della pratica di certificazione (dall'offerta alla Certificazione);
h) Per gli OdC NON accreditati ISO/IEC 17021-1, oltre ai documenti sopra riportati, occorre inviare la documentazione richiesta nella domanda di accreditamento.

3) Mantenimento dell'Accreditamento

Per il mantenimento dell'accreditamento, durante l'intero ciclo di accreditamento, salvo situazioni particolari (Es: gestione reclami e segnalazioni, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'Organismo, implicazioni in cause giudiziarie…), verranno condotte le seguenti verifiche:

- se l'OdC ha emesso meno di 50 certificati nello schema di certificazione, devono essere fatte una verifica in accompagnamento e una verifica in sede;
- se l'OdC ha emesso tra 51 e 200 certificati nello schema di certificazione, devono essere fatte 2 verifiche in accompagnamento e 1 verifica in sede;
- se l'OdC ha emesso più di 201 certificati nello schema, devono essere fatte 2 verifiche in accompagnamento e 2 verifiche in sede.

Siamo a disposizione per chiarimenti e con l'occasione Vi porgiamo cordiali saluti.

Dott. Emanuele Riva
Direttore Dipartimento
Certificazione e Ispezione