CIRCOLARE INFORMATIVA Prot. DC2021OC011 **DATA** Milano, 20-01-2021

A tutti gli Organismi di certificazione accreditati/accreditandi 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 informativa DC N° 02/2021 - Disposizioni in materia di transizione degli accreditamenti degli Organismi di Certificazione (OdC) di sistemi di gestione a fronte della norma ISO/IEC 27006:2015 con integrazione della ISO/IEC 27006:2015/Amd 1:2020

In data 27 Marzo 2020 è stata pubblicata la Norma Internazionale ISO/IEC 27006:2015/Amd 1:2020 *"Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems — Amendment 1"*, applicabile agli Organismi che effettuano la certificazione dei sistemi di gestione SSI.

Riportiamo di seguito la IAF resolution:

The General Assembly, acting on the recommendation of the Technical Committee, resolved that the Transitional Arrangement associated with ISO/IEC 27006:2015 AMD 1:2020 - Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems – Amendment 1, will be two years from the last day of the month of publication of the amended standard.

Lo IAF ha concordato un periodo di transizione di 24 mesi dall'ultimo giorno del mese di pubblicazione della norma.

A seguito della pubblicazione da parte dello IAF delle FAQ relative alle disposizioni a causa dell'emergenza sanitaria, la scadenza della presente transizione è stata posticipata di 6 mesi; pertanto entro il **30 Settembre 2022** tutti gli Organismi già Accreditati ISO/IEC 27006:2015 dovranno adeguarsi alla nuova norma al fine di evitare provvedimenti sanzionatori.

Nuove domande di Accreditamento

A partire dal 31 Maggio 2021 Accredia accetterà solo nuove domande di accreditamento a fronte della ISO/IEC 27006:2015 con integrazione della ISO/IEC 27006:2015 AMD 1:2020.

Organismi già accreditati ISO/IEC 27006:2015 – Gestione della transizione

Tutti gli Organismi già accreditati ISO/IEC 27006:2015 dovranno apportare le opportune modifiche al proprio Sistema di gestione, incluso l'aggiornamento delle procedure/istruzioni pertinenti ai documenti contrattuali, incluso il regolamento di certificazione, e la formazione al personale interessato (tramite sessioni d'aula, circolari informative, affiancamenti…).

Accredia verificherà l'adeguamento alla nuova norma in occasione delle verifiche di sorveglianza e rinnovo già previste nel normale ciclo di Accreditamento senza costi aggiuntivi.

Su esplicita richiesta da parte dell'organismo, la verifica della transizione può svolgersi offsite con un esame documentale di 0,5gg/u.

Per facilitare questo processo di transizione, viene allegato a questa circolare un esempio di come possa essere strutturato un Piano di Transizione.

Tale Piano dovrà essere reso disponibile al Gruppo di verifica ACCREDIA in occasione della verifica di transizione, con i relativi allegati.

Il GVI ACCREDIA allegherà, quindi, il Piano di Transizione al proprio rapporto di verifica e vi annoterà la propria valutazione.

Salvo diversi accordi, tutte le verifiche condotte dopo il 31 Maggio 2021 verranno condotte con l'integrazione della nuova norma.

Eventuali Non Conformità emesse a fronte della nuova norma dovranno essere chiuse con esito positivo prima della concessione dell'accreditamento alla ISO/IEC 27006:2015/Amd 1:2020.

Restando a Vostra disposizione per eventuali chiarimenti e approfondimenti, Vi inviamo cordiali saluti.

Dott. Emanuele Riva

Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da: EMANUELE RIVA
Data: 19/01/2021 18:07:22

Esempio di Piano di Transizione alla ISO/IEC 27006:2015/Amd.1:2020(E)

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

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

N°	Emendamento		Spazio riservato ad ACCREDIA
1.	7.2.1.1 d) Replace the text by the following: d) has gained experience of auditing ISMS prior to acting as an auditor performing ISMS audits. This experience shall be gained by performing as an auditor-in-training **monitored by an ISMS evaluator** (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audit days and performed in the last 5 years. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting.	Valutate di dover modificare i requisiti nonché il processo di qualifica degli auditor già qualificati? Allegare evidenze.	C ☐ A ☐ Se Aperto chiarire:
2.	7.2.1.1 Add a new bullet point g) as follows: g) has competence in auditing an ISMS in accordance with ISO/IEC 27001.	Valutate di dover modificare i requisiti nonché il processo di qualifica degli auditor già qualificati? Allegare evidenze.	C ☐ A ☐ Se Aperto chiarire:
3.	8.2.1 Replace the last paragraph by the following: The certification documents may reference national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability in accordance with ISO/IEC 27001:2013, 6.1.3 d). The reference on the certification documents shall be clearly stated as being only a control set source for	Valutate di dover modificare la documentazione pertinente come ad esempio il regolamento di schema, ed anche e non solo quella pertinente alle estensioni dello standard ISO/IEC 27001 alle linee guida ed allo scopo flessibile, se adottati? Allegare evidenze.	C ☐ A ☐ Se Aperto chiarire:

	controls applied in the Statement of Applicability and not a certification thereof.		
4.	9.3.1.1 Replace the third paragraph by the following: The results of stage 1 shall be documented in a written report. **The certification body shall review the stage 1 audit report before deciding on proceeding with stage 2 and shall confirm if the stage 2 audit team members have the necessary competence;** this may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate. NOTE Independent review (i.e. by a person from the certification body not involved in the audit) is one measure to mitigate the risks involved when deciding if and with whom to proceed to stage 2. However, other risk mitigation measures can already be in place achieving the same goal.	Valutate di dover modificare il regolamento la procedura di certificazione? Allegare evidenze.	C ☐ A ☐ Se Aperto chiarire:
5.	B.2.1 Replace the first paragraph by the following: The total number of persons doing work under the organization's control for all shifts within the scope of the certification is the starting point for determination of audit time.	Valutate di dover modificare i template dei contratti, il regolamento e gli algoritmi cablati nel sistema informativo? Allegare evidenze.	C ☐ A ☐ Se Aperto chiarire:
6.	B.3.6 Replace the first paragraph by the following: It is expected that the time calculated for planning and report writing combined should not typically reduce the total on-site "audit time" to less than 70 % of the time calculated in accordance with B.3.3 and B.3.4. Where additional time is required for planning and/or report writing, this shall not be a justification for reducing on-site audit time. Auditor	Valutate di dover modificare i template dei contratti, il regolamento e gli algoritmi cablati nel sistema informativo? Allegare evidenze.	C ☐ A ☐ Se Aperto chiarire:

	travel time is not included in this calculation and is additional to the audit time referenced in the chart.		
7.	B.6 Replace the first paragraph by the following: The number of total on-site auditor days – as calculated for the scope following the procedure stated in B.3.3 – shall be distributed amongst the different sites based on the relevance of the site for the management system and the risks identified. **The justification for the distribution shall be recorded by the certification body**. The total time expended on initial audit and surveillance is the total sum of the time spent at each site plus the central office and **shall never be less** than that which would have been calculated for the size and complexity of the operation if all the work had been undertaken at a single site (i.e., with all the employees of the company in the same site).	Valutate di dover modificare i template dei contratti, il regolamento e gli algoritmi di calcolo dei giorni-uomo anche eventualmente cablati nel sistema informativo? Allegare evidenze.	C ☐ A ☐ Se Aperto chiarire:
8.	Tutti	È stata pianificata la comunicazione ai clienti relativamente alla modifica allo schema? Allegare evidenze. Fornire evidenze	C ☐ A ☐ Se Aperto chiarire:
9.	Tutti	È stato stilato un piano di formazione per il personale coinvolto? Fornire evidenze	C ☐ A ☐ Se Aperto chiarire:
10.	Tutti	É stato stilato un piano guida per l'attuazione delle modifiche individuate? Fornire evidenze	C ☐ A ☐ Se Aperto chiarire: