Att.: A tutti gli Organismi di Certificazione accreditati e accreditandi operanti la certificazione di sistemi di gestione per la sicurezza delle informazioni

A tutti i Soggetti interessati
Loro sedi

Ns. rif.: DC2015TMF067 *Milano,* 30/12/2015

Oggetto: **Dipartimento di Certificazione e Ispezione Accredia – Circolare N° 28/2015**
Disposizioni in materia di transizione degli accreditamenti degli Organismi di Certificazione (OdC) di sistemi di gestione dalla norma ISO/IEC 27006:2011 alla norma ISO/IEC 27006:2015

In data 30 Settembre 2015, è stata pubblicata la Norma Internazionale ISO/IEC 27006:2015 "*Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems"*, applicabile agli Organismi che effettuano la certificazione dei sistemi di gestione SSI.

La norma ISO/IEC 27006:2015 sostituisce la ISO/IEC 27006:2011, che è stata contestualmente ritirata, ma che continua a valere nel periodo di transizione.

Lo IAF ha concordato il periodo di transizione di 2 anni dalla data di pubblicazione della norma; pertanto, entro il 30 Settembre 2017 tutti gli Organismi già Accreditati ISO/IEC 27006:2011 dovranno adeguarsi alla nuova norma al fine di evitare provvedimenti sanzionatori.

***IAF Resolution 2015–12** – (Agenda Item 10) Transitional Arrangement for ISO/IEC 27006:2015 - The General Assembly, acting on the recommendation of the Technical Committee, resolved that the transition period for ISO/IEC 27006:2015 Information technology - - Security techniques -- Requirements for bodies providing audit and certification of information security management systems will be two years from the date of publication of the standard, i.e. 30 September 2017.*

Nuove domande di Accreditamento

A partire dal 1 Gennaio 2016 Accredia non accetterà nessuna nuova domanda di accreditamento a fronte della ISO/IEC 27006:2011.

Organismi già accreditati ISO/IEC 27006:2011 – gestione della transizione

Tutti gli Organismi già accreditati ISO/IEC 27006:2011 dovranno predisporre un piano di transizione per definire le modifiche ritenute necessarie per l'adeguamento alla nuova norma. Il piano dovrà riportare una sintesi delle modifiche apportate al proprio Sistema di gestione, l'elenco delle procedure/istruzioni oggetto di modifica le risorse dedicate, i momenti di formazione rivolti al proprio personale, e tempi certi per completare le modifiche. Tale Piano potrà essere redatto utilizzando il modulo allegato, eventualmente integrato se ritenuto necessario.

Questo piano di transizione dovrà essere reso disponibile ad Accredia prima o in occasione della verifica di transizione.

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

Accredia, se non richiesto esplicitamente, verificherà lo stato di adeguamento alla nuova norma in occasione delle verifiche di sorveglianza e rinnovo già previste nel normale ciclo di Accreditamento. Salvo diversi accordi, tutte le verifiche condotte dopo il 30 settembre 2016 verranno condotte a fronte della nuova norma.

ACCREDIA intende evitare – in linea di massima - che il passaggio alla nuova norma costituisca un aggravio di costi per gli Organismi di certificazione, fatti salvi i casi particolari connessi a situazioni di persistente non allineamento alla norma e/o dovuti a richieste specifiche (es. di "transizione anticipata") che implichino attività ispettive supplementari o straordinarie, i cui costi aggiuntivi per l'OdC saranno comunque sempre oggetto di preventivo comunicato per accettazione, secondo le prassi usuali.

Eventuali Non Conformità emesse a fronte della nuova norma dovranno essere chiuse con esito positivo (verifica di attuazione ed efficacia) prima della concessione dell'accreditamento ISO/IEC 27006:2015.

Dal 30 Settembre 2017 tutti i restanti accreditamenti emessi a fronte della ISO 27006:2011 verranno revocati.

In considerazione del fatto che la ISO/IEC 27006:2015 si basa sulla ISO/IEC 17021-1:2015, non potrà essere completata la transizione alla ISO/IEC 27006:2015, se non contemporaneamente o in momento successivo alla transizione alla ISO/IEC 17021-1:2015.

Nuovi schemi di Accreditamento

Nel caso in cui, nei prossimi mesi, dovessero svilupparsi nuovi schemi di accreditamento basati sulla ISO/IEC 27006:2015, sarà subito applicata la nuova versione della norma.

Restando a Vostra disposizione per eventuali chiarimenti e approfondimenti, Vi inviamo i nostri cordiali

Il Direttore di Dipartimento
Dr. Emanuele Riva

Esempio di Piano di Transizione alla ISO/IEC 27006:2015

Ogni OdC deve compilare questo modulo (o predisporre un documento simile) e renderlo disponibile al Team di verifica ACCREDIA prima o in occasione della 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.	Come sarà gestita la comunicazione ai clienti relativamente alla gestione della transizione? Allegare le evidenze pertinenti.	Chiusura C ☐ A ☐ Se Aperto chiarire:
2.	Con quali modalità e tempistiche verrà svolta e valutata la formazione al personale addetto al riesame del contratto e ai Responsabili dei Programmi di audit?	Chiusura C ☐ A ☐ Se Aperto chiarire:
3.	Con quali modalità e tempistiche verrà svolta e valutata la formazione agli auditor?	Chiusura C ☐ A ☐ Se Aperto chiarire:
4.	Con quali modalità e tempistiche verrà svolta e valutata la formazione ai decision maker?	Chiusura C ☐ A ☐ Se Aperto chiarire:
5.	Quali documenti del Vs. organismo dovranno essere modificati, e con che tempistiche verranno distribuiti e resi applicabili? (Renderli disponibili al GVI Accredia)	Chiusura C ☐ A ☐ Se Aperto chiarire:
6.	Come avete gestito i nuovi requisiti di norma in tema di Imparzialità (compreso per le organizzazioni sotto il controllo del Vs. Odc)? Allegare le evidenze pertinenti.	Chiusura C ☐ A ☐ Se Aperto chiarire:
7.	Avete modificato le regole per l'uso del marchio / riferimento al sistema di Certificazione? Allegare le evidenze pertinenti.	Chiusura C ☐ A ☐ Se Aperto chiarire:
8.	Avete modificato le regole relative alla gestione del rinnovo? E le regole relative alla gestione di audit di Stage 1 con esito negativo? Allegare le evidenze pertinenti.	Chiusura C ☐ A ☐ Se Aperto chiarire:
9.	Ulteriori considerazioni che vogliate aggiungere per spiegare meglio come gestirete / avete gestito questa transizione	Chiusura C ☐ A ☐ Se Aperto chiarire:
10.	A fronte dei nuovi requisiti, ritenete necessario modificare i contratti in essere (es. tempi di audit ecc..)? Allegare evidenze delle modifiche ritenute necessarie a livello contrattuale	Chiusura C ☐ A ☐ Se Aperto chiarire:
11.	Quali "Network Assisted Audit Techniques" avete adottato? Allegare evidenze	Chiusura C ☐ A ☐ Se Aperto chiarire: