Newsletter
Luglio 2017

CERTIFICAZIONE E FORMAZIONE DEGLI AUDITOR/LEAD AUDITOR PER LA ISO/IEC 27001:

C'È ANCORA TROPPA CONFUSIONE!

Care Colleghe, Cari Colleghi,

prosegue la serie di Newsletter legate agli Schemi di Certificazione di AICQ SICEV che ci ha messo a disposizione il nostro Referente di Schema sulla *Business Continuity*. L'argomento trattato, anche se riferito ad una norma per il momento poco applicata dalle Organizzazioni italiane, è di tipo trasversale per diverse altre norme sui Sistemi di Gestione e contribuisce a fare chiarezza su una tematica che interessa tutti gli Iscritti nei Registri AICQ SICEV: la certificazione.

Buona lettura e buon lavoro.

Roberto De Pari

Direttore AICQ SICEV

Know how in pillole:

Quando si parla di "certificazione" spesso si utilizzano termini impropri e questo genera grande confusione sul mercato.

La certificazione, per definizione, è quell'attività svolta da un Organismo terzo indipendente che attesta che un'Organizzazione, una persona o un prodotto/servizio risponda a requisiti definiti.

Gli Organismi indipendenti (o anche Organismi di Certificazione) sono Organizzazioni a loro volta accreditate per poter svolgere tali attività nel loro insieme o per singoli Schemi di Certificazione.

L'accreditamento è regolato, a livello internazionale, dallo IAF (*International Accreditation Forum* – www.iaf.nu) e gli accreditamenti sono soggetti al mutuo riconoscimento per effetto del *Multilateral Recognition Arrangement*. I firmatari degli accordi ottengono il mutuo riconoscimento nei paesi a loro volta sottoscrittori degli accordi.

In modo del tutto equivalente anche a livello europeo, per effetto di un Regolamento CE[1], sono stati definiti appositi *Multilateral Agreement* a livello di EA (*European Accreditation* – http://www.european-accreditation.org). Anche in questo caso i firmatari ottengono il mutuo riconoscimento nei paesi europei sottoscrittori degli accorsi.

Da notare che un paese può aver sottoscritto accordi a tutti i livelli o anche ad uno solo dei livelli sopracitati.

[1] "*Attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità*» ***REG (CE) N. 765/2008.***

A livello nazionale, esiste Accredia (www.accredia.it), unico Organismo Italiano di accreditamento. Accredia è sottoscrittore di accordi di mutuo riconoscimento sia a livello Europeo (EA) sia a livello mondiale (IAF).

È chiaro da questi primi elementi che l'accreditamento non sempre è obbligatorio (salvo i casi specificati da leggi o direttive). Così come non lo è la certificazione, anche qui con le dovute eccezioni.

Inoltre, la certificazione - essendo per definizione concessa da una terza parte indipendente - non può essere concessa da entità che hanno avuto parte attiva nei processi soggetti a certificazione. Ad esempio, consulenti che hanno condotto l'organizzazione alla certificazione, *training center* che hanno formato la persona, organizzazioni che hanno prodotto un bene o che erogano un servizio.

Da qui la prima considerazione fondamentale di questa newsletter: chi eroga un corso per la formazione di auditor/lead auditor non emette la *certificazione di competenza* ma solo l'attestato di superamento del corso (all'estero detto *certificate* e da qui il caos con le nostre definizioni!). Una persona al superamento dell'esame ottiene quindi una qualificazione[2] e non una certificazione.

La certificazione delle competenze della persona[3] avviene solo da parte degli Organismi di Certificazione del Personale in specifiche sessioni di esame e secondo criteri definiti in appositi *standard* e norme.

Al superamento dell'esame si ottiene il certificato di competenza specifico e si viene iscritti al relativo registro, sempre gestito dagli Organismi di Certificazione del Personale.

La certificazione delle competenze degli auditor/lead auditor dei Sistemi di Gestione è regolata dalla ISO/IEC 17024:2012 alla quale vanno aggiunti gli schemi di riferimento (cioè le norme per cui il candidato chiede il riconoscimento della competenza ad es. la ISO/IEC 27001:2013).

Per gli auditor/lead auditor dei Sistemi di Gestione per la Sicurezza delle Informazioni l'elenco delle competenze richieste è specificato nel documento IAF MD13:2015 (al momento issue 1 version 2 con data di applicazione 26 maggio 2015 – reperibile a questo link: http://www.iaf.nu/upFiles/IAFMD13ISMSABcompetenceIssue1Version228052015.pdf).

In definitiva, la certificazione di un auditor/lead auditor che operi per lo schema ISO/IEC 27001:2013 per un Organismo di Certificazione (quindi in audit di parte terza) prevede necessariamente la conoscenza, abilità e competenza nell'applicazione delle norme[4]:

- ISO/IEC 17021 – 1:2015
- ISO/IEC 27006:2015

[2] ISO/IEC 17024:2012 – req. 3.7 Qualification
[3] ISO/IEC 17024:2012 – req. 3.5 Certificate
[4] Edizioni delle norme aggiornate al 23/11/2016

- ISO/IEC 27001:2013
- ISO/IEC 27000:2016
- ISO/IEC 27007:2011
- ISO/IEC TR 27008:2011

Da questa lista appaiono chiari alcuni punti che devono essere presi in considerazione dai candidati ed dagli Organismi di Certificazione (dei Sistemi di Gestione e del Personale):

1. La ISO 19011:2011 non è parte delle norme/linee guida richieste da IAF. Può essere utilizzata proprio perché linea guida, e non norma di requisiti, a supporto della ISO/IEC 17021 (vedi paragrafo *Introduction* della ISO 19011:2011 con relativo specchietto riassuntivo per la sua applicabilità in relazione alla ISO/IEC 17021). In Italia, gli Organismi di Certificazione dei Sistemi e del Personale chiedono che gli auditor/lead auditor abbiano anche questa competenza che *non può in alcun modo sostituire la conoscenza ed esperienza sulla ISO/IEC 17021!*
2. La non conoscenza della ISO/IEC 27006:2015 potrebbe inficiare l'attività di audit, in particolare per le modalità di gestione e conduzione degli audit secondo la ISO/IEC 27001:2013.
   A mio avviso la non conoscenza della norma, ed in particolare dei relativi annex, può inficiare significativamente sul lavoro in campo e rendere un auditor/lead auditor incapace di pianificare e gestire un audit in modo efficace (ad es. comprensione della complessità di un Sistema di Gestione, criteri di dimensionamento di un audit, campionamento *multisite* ecc.).
3. La non conoscenza della linea guida ISO/IEC 27007:2011 e del documento tecnico ISO/IEC TR 27008:2011 potrebbe inficiare la capacità dell'auditor/lead auditor di condurre un audit orientato alla sicurezza delle informazioni, infatti, in assenza di queste competenze, l'auditor potrebbe far "virare" l'audit in modalità non idonee a considerare le specificità dello schema (ad es. il peso e l'importanza dell'Annex A della ISO/IEC 27001:2013, le opzioni per la verifica dei controlli selezionati ecc.).
4. I corsi frequentati dai candidati dovrebbero aver considerato i fattori sopra esposti (sia per la parte teorica sia per la parte pratica/esercitativa) e quindi i relativi attestati di superamento del corso dovrebbero esplicitare in chiaro se e quali *standard* (inclusa la versione/edizione) siano stati utilizzati durante il corso. Da considerare gli eventuali *transition period*, cioè i periodi di transizione in caso di aggiornamento delle norme. In questo caso, corsi ed attestati potrebbero essere riferiti a norme in fase di transizione, tuttavia, è però possibile verificare quando scade il periodo di transizione e quindi la validità dei corsi e degli attestati.
   Il periodo di transizione delle norme è verificabile nei siti ufficiali, per esempio per la ISO/IEC 17021 la transizione è definita nel sito IAF nel documento IAF ID 11:2015 (http://www.iaf.nu/upFiles/IAFID11_ISO170211TransitionPublicationVersion06032015.pdf).
   Anche attraverso il sito Accredia è possibile verificare i periodi di transizione. A questo link troverete il periodo di transizione per la ISO/IEC 27006:2015 http://www.accredia.it/UploadDocs/6167_DC2015TMF067.pdf .

Fin troppo spesso in audit di affiancamento o nelle attività di formazione incontro persone con corsi "parziali" o addirittura "vecchi" rispetto al documento IAF, persone completamente ignare di queste semplici regole. Altrettanto spesso queste persone mi dicono che durante il corso nessuno ha

spiegato loro questi meccanismi né che si siano cimentati in esercitazioni pratiche sulla conduzione e gestione dell'audit.

Qui si aprono quindi due possibili ipotesi:

- I corsi erogati non sono "adeguati, sebbene registrati (o qualificati) dagli Organismi di Certificazione del Personale.
- I partecipanti si fanno "abbindolare" dal prezzo o dal titolo del corso che intendono frequentare senza analizzare in dettaglio la validità dello stesso.

In realtà, tutti i corsi qualificati dagli Organismi di Certificazione del personale dovrebbero avere le caratteristiche sopraelencate anche se distribuite in modo diverso nell'arco delle giornate formative (in genere cinque), minima formazione prevista per la prima qualificazione di un auditor (nel caso di seconda qualificazione il corso può essere ridotto a 24 ore ma questo non sempre è riconosciuto da tutti i registri per la ISO/IEC 27001).

Basta quindi una lettura attenta dei contenuti del corso per capire se quello che ho davanti è un corso qualificato da un Organismo di Certificazione (accreditato da ACCREDIA per la certificazione di personale). I dati di un corso possono essere richiesti all'Organismo di Certificazione del Personale che ha qualificato il corso oppure al *provider* del corso (in ogni caso è bene chiedere informazioni per iscritto per eventuali successive verifiche e ricorsi in caso di problemi).

Un ulteriore requisito per la scelta è la possibilità di iscriversi al Registro corrispondente (*provisional* auditor, auditor, lead auditor) gestito dallo stesso Organismo di Certificazione del Personale o avere la garanzia che il titolo ottenuto con il superamento del corso sia valido ad iscriversi in uno dei Registri equivalenti gestiti da altri Organismi di Certificazione (accreditati da Accredia).

Se poi vogliamo essere sicuri dell'efficacia e della qualità del corso è opportuno chiedere il nome del docente e verificare che questo operi possibilmente come lead auditor per almeno uno degli Organismi di Certificazione (accreditati in Italia per la certificazione dei Sistemi di Gestione per la Sicurezza delle Informazioni) e/o se esso stesso è iscritto in almeno uno dei Registri per i lead auditor dei Sistemi di Gestione per la Sicurezza delle Informazioni. Queste due informazioni ci dicono che saremo formati da un professionista la cui competenza è confermata dalla sua presenza nel Registro di pertinenza e che lo stesso opera effettivamente nelle materie oggetto del corso.

Cosa succede se frequento un corso che non ha queste caratteristiche? La risposta a questa domanda è molto complessa, possiamo avere varie casistiche:

- **corsi che non rientrano nel circuito di Organismi di Certificazione del Personale accreditati** (l'Organismo di Certificazione è accreditato da un paese che non ha sottoscritto gli accordi internazionali o non ha copertura in Italia): in questo caso, a parte l'efficacia e la qualità del corso, il titolo ottenuto potrebbe non essere riconosciuto dagli Organismi di Certificazione dei Sistemi di Gestione. Per eseguire audit di prima o seconda parte la qualificazione ottenuta potrebbe comunque essere valida. Può essere opportuno in questi

casi candidarsi per un esame, presso uno degli Organismi di Certificazione del Personale accreditati in Italia, per ottenere la conversione della qualifica.

- **corsi che non hanno alcuna registrazione/qualificazione presso Organismi di Certificazione del Personale accreditati**: questi corsi dovrebbero essere assolutamente evitati! Infatti, in questo caso, tutta la catena di riferibilità, spiegata nei paragrafi precedenti, viene meno ed è quindi di fatto impossibile assicurare che il corso sia stato erogato secondo criteri validi ai fini della qualificazione degli auditor/lead auditor dei Sistemi di Gestione anche in termini di contenuti. Qui l'unica soluzione è iscriversi nuovamente ad un corso qualificato da uno degli Organismi di Certificazione accreditati in Italia.
- **corsi che hanno registrazioni/qualificazioni non riferiti alla normativa ISO** (sistemi proprietari): in questi casi occorre fare domande dirette al *provider* (meglio in forma scritta) per capire se e come il titolo ottenuto possa essere utilizzato per una eventuale futura certificazione come auditor/lead auditor. In alcuni casi esiste, infatti, un accordo scritto tra questi *provider* e gli Organismi di Certificazione per una sorta di riconoscimento di crediti parzialmente utili per future attività di certificazione delle competenze. In genere, questi corsi non sostituiscono i corsi standard ma li integrano e/o supportano.

Normalmente i corsi qualificati per auditor/lead auditor contengono:

- una sezione dedicata all'analisi delle norme di riferimento
- una sezione riservata ad esercitazioni pratiche di simulazione di un audit di terza parte (almeno pianificazione dell'audit, identificazione-strutturazione-classificazione delle non conformità, report dell'audit).

I tempi dedicati per le due sezioni possono differire ma la loro somma in genere è di 40 ore (in prima qualificazione) o almeno 24 ore in seconda qualificazione (laddove ammesso a livello nazionale).

Con queste informazioni alla mano abbiamo almeno gli elementi formali per verificare la credibilità e validità del corso e del relativo attestato.

Ovviamente, le considerazioni sul prezzo sono assolutamente personali ed insindacabili!

Un ultimo chiarimento per chi fosse interessato a questi corsi e comunque per tutti coloro che possano ancora nutrire qualche dubbio: per operare come auditor/lead auditor è importante aver frequentato e superato l'esame di un corso qualificato da un Organismo di Certificazione del Personale accreditato da uno degli Organismi di Accreditamento firmatari degli accordi di mutuo riconoscimento IAF e/o EA così come è altrettanto importante avere eseguito audit in affiancamento ad auditor/lead audiotr già qualificati o certificati. Quindi NON è necessario essere iscritti ad un Registro (e quindi certificati da un OdC di terza parte) per esercitare la professione di auditor/lead auditor. Ovviamente essere iscritti ad un Registro è un'opportunità per il professionista e per coloro che utilizzano le loro competenze essendo queste garantite dal sistema internazionale di certificazione ed accreditamento. La certificazione di terza parte indipendente fornisce, pertanto, agli auditor/lead auditor un valore aggiunto in termini di trasparenza e credibilità, derivante dalla

dimostrazione di conformità delle loro competenze ad una norma di valenza internazionale ed al rispetto di un codice deontologico correlato alla professione svolta.

A questo punto, una nota per i colleghi che già operano in audit di parte terza e/o che sono iscritti ad uno dei vari Registri accreditati: avete verificato di essere in linea con questi *standard*? Il corso da Voi frequentato ed il Vostro attestato sono allineati coni citati standard? Il Vostro certificato di terza parte indipendente è aggiornato? Solo garantendo la professionalità e la competenza possiamo condurre audit efficaci, proteggere il nostro lavoro e la nostra credibilità! Non dimentichiamo che proprio questo è uno dei principi della ISO/IEC 17021 che guida la nostra professione.

Buon lavoro a tutti.

Fabrizio Cirilli (cirillif@tin.it)

Referente AICQ SICEV per lo Schema *Business Continuity* ed esperto di tematiche relative alla Sicurezza dell'Informazione.