

Impatti sulle qualifiche di Lead Auditor a seguito dell'aggiornamento degli standard ISO/IEC 17021, ISO 19001, ISO/IEC 27006 e ISO/IEC 27007

A cura di Fabrizio Cirilli, Lead Auditor di TÜV Italia

L'aggiornamento dello scenario normativo per la gestione e conduzione degli audit, ha determinato un sostanziale cambiamento delle qualifiche/certificazioni per gli auditor/lead auditor dei Sistemi di gestione, siano esse riferite a ISO 9001, OHSAS 18001, ISO 14001, ISO/IEC 27001, ISO/IEC 20000-1 ecc.

Per chiarire le modifiche e gli impatti sul mercato occorre fare un po' di ordine.

Nel 2011 è stata emessa la nuova versione della ISO 19011:2011 (UNI EN ISO 19011:12 nella versione italiana): una linea guida per la gestione e conduzione degli audit. Nel contempo è stata aggiornata la ISO/IEC 17021:11 che definisce i requisiti essenziali per gli Organismi di Certificazione dei sistemi di gestione (secondo qualsiasi schema di certificazione).

L'insieme dei due standard definisce uno scenario, in precedenza meno netto, soprattutto per gli auditor/lead auditor e per i relativi processi di formazione e qualificazione. Prima di tale aggiornamento quasi tutti i corsi per auditor/lead auditor (da qui in avanti A/LA per brevità) poggiavano quasi esclusivamente sulla ISO 19011:02 (UNI EN ISO 19011:03 in Italia), associata allo schema di certificazione (ad es. ISO 9001, ISO 14001 ecc.). Qualsiasi attestato rilasciato fino a tutto il 2011 era quindi costruito su questa accoppiata: linea guida 19011:02 + schema di certificazione.

Tali corsi qualificavano gli A/LA nella gestione e conduzione degli audit esterni (o di seconda/terza parte). La durata dei corsi era normalmente prefissata in 40 ore, comprensive anche del relativo esame finale, da sostenere per ottenere la relativa qualifica di Auditor/Lead Auditor dei sistemi di gestione, il tutto secondo un determinato schema di certificazione: qualità, sicurezza delle informazioni e dei lavoratori, ambiente ecc. L'eventuale certificazione veniva rilasciata dagli Organismi di Certificazione del Personale,

sulla base di competenze definite dalle norme oggetto del corso nonché da alcuni parametri aggiuntivi dipendenti dallo schema di certificazione e dal settore specifico.

Le nuove norme ridefiniscono questo sistema di qualifiche, determinando regole distinte a seconda della destinazione d'uso della qualifica di A/LA (audit di prima, seconda o terza parte):

- Auditor di terza parte (cioè quei professionisti destinati alla conduzione e gestione degli audit per gli Organismi di Certificazione): hanno l'obbligo di conoscenza dei contenuti della ISO/IEC 17021, con particolare riferimento ad alcuni capitoli requisiti (4, 7, 9 e appendice A). Da notare che la ISO/IEC 17021 è una norma internazionale contenente i requisiti essenziali che ogni Organismo di Certificazione deve necessariamente possedere, allo scopo di assicurare a tutte le parti interessate che i sistemi di gestione da esso certificati soddisfino i requisiti definiti dalla norma di riferimento ed i principi delineati dalla stessa ISO/IEC 17021. In sostanza garantire la credibilità delle certificazioni. Per questi auditor la ISO 19011 (essendo una linea guida) non assume valore prescrittivo, cioè non è necessaria per condurre audit di terza parte. Può comunque essere utilizzata qualora l'Organismo di Certificazione ne ravveda l'opportunità.
- Tutti gli altri auditor (ovvero i professionisti operanti nella conduzione e gestione degli audit di prima e/o seconda parte) possono adottare quanto descritto nella ISO 19011:11 senza alcun obbligo. Anche per questi la ISO 19011:11 assume un carattere volontario e non prescrittivo.

Potrebbe però essere richiesta in ambito contrattuale (ad esempio in audit di parte seconda).

Affinché le qualifiche di A/LA possano mantenere la loro validità occorre quindi che siano rispettati i requisiti e gli orientamenti appena descritti.

Particolare attenzione va posta alle qualifiche degli A/LA dei sistemi di gestione per la sicurezza delle informazioni (ISO/IEC 27001:05). Per questi ultimi le regole sono state ulteriormente rivisitate:

- per gli Auditor di terza parte: alle precedenti prescrizioni occorrerà aggiungere la conoscenza della ISO/IEC 27006:11 che delinea i requisiti per gli Organismi di Certificazione nel campo della sicurezza delle informazioni.
- Per gli auditor di prima e seconda parte: occorrerà tenere conto della ISO/IEC 27007:11 (per la gestione degli audit interni) e della ISO/IEC TR 27008:11 (per la verifica dei controlli - o contromisure - adottati in un sistema di gestione per la sicurezza delle informazioni). Anche in questo caso queste linee guida non assumono carattere di obbligatorietà ma potrebbero essere richieste a livello contrattuale.

Le prescrizioni emesse da Accredia nell'aprile del 2011 pongono la fine del periodo di transizione al 1 febbraio 2013, periodo entro il quale ogni auditor di terza parte, in possesso di qualifiche/certificazioni per qualsiasi schema di certificazione, dovrà aggiornare la propria qualifica/certificazione.

Gli Organismi di Certificazione avranno inoltre l'onere di affrontare la definizione delle "aree tecniche" (cioè delle competenze tecniche specifiche per gli auditor da loro utilizzati), in funzione non solo dello schema e del settore di impiego ma anche degli aspetti specifici dei sistemi di gestione. Quindi un A/LA che opererà per un Organismo di Certificazione dovrà essere valutato secondo criteri che ne dimostrino ed assicurino le competenze

tecniche del settore di impiego.

Nel campo della sicurezza delle informazioni, ad esempio, gli A/LA dovranno dimostrare la conoscenza della ISO/IEC 17021:11, ISO/IEC 27006:11 nonché conoscenze tecniche specifiche del settore quali :valutazione e gestione dei rischi, business continuity, disaster recovery, cloud computing, sicurezza delle reti ecc. in funzione del tipo di impiego e di processi da valutare.

Tenendo conto di queste premesse, le organizzazioni impegnate nella formazione degli A/LA dovranno rivedere i loro programmi formativi al fine di garantire che i corsi soddisfino il nuovo quadro normativo (in particolare i requisiti prescrittivi per gli A/LA di terza parte) delegando la definizione e la verifica delle aree tecniche agli Organismi di Certificazione.

Siamo dunque di fronte ad una mutazione significativa del panorama formativo ed operativo per gli A/LA.

Per quanto riguarda l'impiego delle qualifiche/certificazioni in gare ed appalti, l'attuale richiesta di "auditor/lead auditor certificati" dovrà necessariamente specificare:

- La destinazione d'uso delle competenze richieste (tipo di audit, schema di certificazione, specializzazioni richieste ecc.), essendo profondamente modificate le regole in funzione del tipo di audit da condurre.
- La data di ottenimento del titolo, essendo cambiati i contenuti minimi formativi in funzione del tipo di audit da condurre.
- La verifica che l'ente erogatore del corso per A/LA abbia (o abbia avuto) le idonee credenziali alla data di erogazione del corso di qualifica.
- Lo stato di aggiornamento del "registro" che ha rilasciato la certificazione al A/LA.

Ogni A/LA dovrà quindi rivalutare le proprie competenze e qualifiche per determinare se occorre o meno avviare un processo di aggiornamento delle proprie credenziali. L'aggiornamento è indispensabile per gli A/LA

di terza parte in possesso di titoli (qualifiche e certificazioni) rilasciate prima del 2012, soprattutto se rilasciate da organizzazioni prive di accreditamento.

Le organizzazioni che erogano corsi di formazione per A/LA hanno avviato (o

dovranno avviare quanto prima) il processo di revisione dei contenuti didattici dei corsi (norme, esercitazioni, materiale didattico ecc.) e delle credenziali dei propri docenti per poter rispondere in modo adeguato al nuovo quadro normativo.