

Qualifica e certificazione degli auditor dei SGSI

(tra leggenda e realtà)

Ogni anno incontro tra le 100 e le 200 persone che affrontano il corso per "auditor/lead auditor dei sistemi di gestione per la sicurezza delle informazioni conformi alla norma ISO/IEC 27001:05", sia in Italia sia all'estero. Di queste solo l'1% completa il percorso raggiungendo la certificazione personale, il 10% lavora come auditor (senza certificazione), la restante parte svolge altre attività (in genere consulenza o management dell'InfoSec) sfruttando quanto appreso dal corso.

Quindi un vero "esercito" di professionisti, tutti mi hanno posto le stesse domande in materia di certificazione/qualifica degli auditor e lead auditor dei sistemi di gestione per la sicurezza delle informazioni (o come vengono più comunemente chiamati "auditor/lead auditor ISO 27001").

In questo articolo-intervista ho raccolto le domande più frequenti ed ho tentato di rispondere nel modo più chiaro possibile in modo da fornire principi guida generali, utili (spero) a chiarire i concetti di qualifica e certificazione, magari sfatando qualche mito su questa professione e sui titoli che la sostengono.

Pur essendo consapevole di non poter trattare in modo esaustivo un tema così complesso, spero che queste pagine possano essere d'aiuto al lettore per orientarsi nel mare magnum dei corsi, delle qualifiche e dei percorsi sul tema. La richiesta del mercato si va via via espandendo quindi chiarire i concetti alla base di questi temi ritengo sia utile per tutti.

Le definizioni, le lingue d'origine e l'accezione del mercato tendono a mescolare e confondere i termini, talvolta in modo assolutamente inconsapevole altre volte in modo "astuto".

È giusto che ognuno possa comprendere i fenomeni che incontra e prendere le dovute misure per raggiungere i propri obiettivi. Ecco perché nasce questo articolo-intervista.

Svolgo il lavoro di auditor da 15 anni e di docente dei corsi di qualifica da 10 anni, le domande rimangono le stesse. Penso quindi vi sia un continuo bisogno di rinfrescare concetti e termini per evitare confusione ed essere consapevoli dei passaggi necessari a raggiungere la certificazione.

Resto a disposizione di chiunque voglia sottoporre domande personali o specifiche, per questo a fine articolo troverete il mio indirizzo e-mail.

Buona lettura.

Fabrizio Cirilli

D. Quali sono i percorsi di certificazione per lead auditor in ambito Information Security? Può brevemente descriverli?

R. Esiste di fatto un unico corso di qualifica professionale: "Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC 27001:05". Il corso ha l'obiettivo di qualificare le persone, ovvero di verificare ed attestare che i partecipanti abbiano i "requisiti minimi per operare come auditor esterni, in audit di seconda e terza parte". Il che significa dimostrare la capacità di operare per conto terzi nell'audit dei Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma

ISO/IEC 27001:05 secondo quanto descritto nello standard per la gestione degli audit (ISO 19011:02).

Questa spiegazione apparentemente criptica dichiara semplicemente che si è frequentato un corso specifico e che si sono superati gli esami previsti conseguendo la "qualifica" di auditor/lead auditor. Diverso è il significato di "certificato" che, per il mondo ISO, significa aver dimostrato di essere in grado di *fare* una determinata cosa sottoponendo documenti ed evidenze ad un Organismo di Certificazione del Personale.

Auditor/lead auditor significa invece che si può operare nell'una o nell'altra posizione avendo dimostrato durante il corso tali capacità. Il ruolo di lead auditor ci deve essere ovviamente riconosciuto da un committente sulla base dei requisiti descritti dalla stessa ISO 19011:02. Nulla è lasciato al caso o all'arbitrio quando si tratta di certificazione delle competenze!

Dobbiamo ricordare che la certificazione, nel mondo ISO, si riferisce a: Sistemi di Gestione, prodotti, persone. Per quanto riguarda la certificazione delle persone dobbiamo precisare che esistono solamente tre figure professionali certificabili, una di queste è l'auditor/lead auditor dei sistemi di gestione.

Esistono appositi registri ed organismi di certificazione del personale in grado di controllare ed assicurare l'intera filiera, dalla qualificazione ed aggiornamento dei docenti alla verifica degli esami e del materiale didattico. La certificazione di un auditor/lead auditor è di fatto del tutto equivalente alla certificazione di un sistema di gestione aziendale.

Torniamo al nostro percorso formativo. Il corso standard, della durata di almeno 40 ore, viene suddiviso in due parti distinte:

- la prima parte (in genere di 2 giorni) è basata sullo standard ISO/IEC 27001:05 ed alcune linee guida della famiglia ISO 27000; questa parte del corso è orientata all'analisi dello standard per approfondirne i requisiti (che il discente deve già conoscere) dal punto di vista dell'auditor, acquisendo le capacità necessarie per analizzare come e con quale efficacia le organizzazioni abbiano adottato tali requisiti.
- La seconda parte (in genere di 3 giorni) è basata sullo standard ISO 19011:02 ed è orientata all'acquisizione delle tecniche di gestione degli audit.

In questi 5 giorni di corso viene simulato un intero audit, in modo da permettere a ciascun partecipante di cimentarsi nelle varie attività che dovrà poi affrontare come auditor/lead auditor nella realtà. Le simulazioni comprendono anche alcuni role playing utili a verificare le proprie capacità relazionali, interpersonali e tecniche.

Il corso "40 ore" (come viene normalmente chiamato), dando per acquisita la conoscenza della norma, rappresenta il primo step del percorso che una persona deve intraprendere per raggiungere la certificazione in qualità di auditor/lead auditor. I partecipanti vengono

formati con l'obiettivo di sviluppare le competenze necessarie per: pianificare ed organizzare un audit, raccogliere le evidenze (cioè le prove oggettive di come e se funziona un Sistema di Gestione), individuare le eventuali non conformità e opportunità di miglioramento, preparare il report finale, gestire le riunioni iniziali e finali dell'audit ecc.

In taluni casi il corso può prevedere l'audit su un Sistema Integrato, cioè i partecipanti vengono formati su un Sistema di Gestione Integrato (ad esempio: IT Service management, qualità e sicurezza delle informazioni). In questo modo non solo è possibile osservare "dal vivo" un sistema integrato ma è anche possibile ampliare le proprie competenze e comprendere le reali complessità applicative dello standard nelle aziende. Nel caso si parla di "corso integrato" con qualifica multipla come "lead auditor dei Sistemi di Gestione...". Ovviamente il numero di ore d'aula cresce in funzione degli standard che si vanno ad integrare. Ogni standard aggiuntivo incrementa di almeno 16-24 ore il lavoro di aula.

Da notare che, secondo la ISO 19011:02, avendo superato un corso per auditor/lead auditor dei sistemi di gestione (indipendentemente dalla norma di riferimento) sono sufficienti 3 gg di corso qualificato/regolato per acquisire la qualifica come auditor/lead auditor di un altro schema (o standard). Vale a dire che, una volta ottenuta la qualifica come auditor/lead auditor dei SGSI secondo la ISO/IEC 27001:05, posso frequentare un qualsiasi corso qualificato/regolato di almeno 3 giorni (con esame finale) per acquisire la qualifica equivalente in un altro standard (ad esempio per i sistemi di gestione per la qualità conformi a ISO 9001:08).

D. Quali sono le motivazioni che portano un professionista dell'InfoSec a certificarsi, o meglio qualificarsi, ISO/IEC 27001 Lead Auditor? Quali sono le motivazioni che nella realtà portano le persone a frequentare il corso?

R. Non "ISO/IEC 27001 lead auditor" ma "auditor/lead auditor dei Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC 27001:05". Non si tratta solo di una puntigliosa definizione ma della diversità con altri corsi ed attestazioni!

Come ho accennato prima, il corso e il superamento dell'esame potrebbero costituire il primo passo verso una carriera da auditor (per chi fosse interessato a tale professione). La qualifica di per sé permette alle persone di iniziare a muovere i primi passi nel mondo degli audit.

Il superamento del corso dà l'opportunità di eseguire audit (anche per organismi di certificazione) e di avviare così il percorso verso la certificazione individuale. C'è da precisare però che la certificazione prevede un'esperienza lavorativa minima di 5 anni di cui almeno 2 nell'ambito dell'InfoSec. Anche qui si tratta di precisazioni dovute che è bene fare da subito per evitare confusioni ed illusioni, soprattutto nei giovani che potrebbero trovare in questo lavoro opportunità e sbocchi professionali interessanti.

Torniamo al perché le persone partecipano al corso e sostengono l'esame, le motivazioni sono svariate e differenti: la richiesta del mercato (mi riferisco alle certificazioni richieste

come requisito per partecipare a numerose gare), per cultura personale, perché l'azienda vuole intraprendere un percorso di certificazione ISO 27001, per curiosità. Talvolta i partecipanti accedono al corso con proprie convinzioni e attese imprecise, spesso dovute a scarsa informazione su obiettivi e prerequisiti del corso. Tali convinzioni saranno modificate nel corso delle attività corsuali e talune persone comprenderanno di essere più o meno portate alla carriera di auditor. E' necessario ricordare che lo standard per la gestione degli audit delinea anche alcune caratteristiche personali e comportamentali che, nel corso della attività di aula, saranno verificate e sollecitate con specifici test ed esercitazioni, proprio per dare modo alle persone di valutare le proprie attitudini e capacità in materia di gestione degli audit.

Alla fine di un corso si potrebbe essere perfettamente in grado di svolgere un audit pur avendo valutato che non è questo l'obiettivo professionale che si intende perseguire. È come un esame di maturità: posso superarlo ma non è detto che questo sia il mio lavoro o la mia ambizione futura.

D. Ci sono due punti in particolare su cui vorremmo chiederle spiegazioni, il primo riguarda la differenza tra qualifica e certificazione. Quali sono gli step per raggiungere i due traguardi? Dopo aver raggiunto uno dei due traguardi, quali sono i vincoli per mantenere aggiornato il valore della qualifica/certificazione?

R. Una precisazione prima di risponderle: è assolutamente indispensabile ricordare che la certificazione è (e rimane) un processo volontario, sia essa riferita alle aziende o alle persone. Pertanto un auditor può essere qualificato e non certificato senza violare alcuna legge o regola. Sono gli organismi di certificazione che potrebbero avere qualche problema qualora non disponessero di auditor/lead auditor certificati, dico potrebbero poiché molto dipende dal sistema di accreditamento. Quindi, il lettore deve aver ben chiaro che la certificazione personale *non è un obbligo né può essere imposta*. Può essere invece utilizzata come elemento contrattuale per la selezione e scelta del fornitore dell'audit (come avviene in molte gare). Questo ovviamente se il termine certificazione è inteso nell'accezione ISO del termine!

La qualifica si ottiene con il semplice superamento del corso (e quindi delle prove ed esami in esso contenuti).

Anche gli Organismi di Certificazione effettuano una propria "qualifica interna" degli Auditor. Questo è un processo di valutazione del singolo professionista che, normalmente, non dà luogo né all'ottenimento di un attestato, né alla pubblicazione di tale "status". Serve, però, all'Organismo di Certificazione stesso per dare evidenza delle modalità con le quali seleziona e valuta costantemente le Risorse Umane che impiega come Auditor presso le organizzazioni clienti.

La certificazione è un processo successivo, basato sulla dimostrazione (ad un Organismo di Certificazione del Personale, possibilmente accreditato da un Ente di Accreditamento

riconosciuto) che si ha l'esperienza di conduzione e gestione di audit nella misura minima prevista dagli standard.

La ISO 19011:02 fissa, ad esempio, un numero minimo di giornate e di audit per la certificazione degli auditor e dei lead auditor. Tali audit devono rientrare in determinate "fasce", cioè devono essere stati eseguiti in condizioni predeterminate per poter essere considerati validi ai fini della certificazione. In generale sono validi tutti gli audit svolti in nome e per conto di un organismo di certificazione o comunque svolti sull'intero sistema di gestione (purché non si abbia avuto un ruolo nel Sistema valutato, cioè si possa dimostrare la propria indipendenza ed estraneità con le attività valutate). Ogni registro ha le proprie regole quindi è utile documentarsi a priori per non incappare in spiacevoli sorprese durante il processo di certificazione.

Il discorso del mantenimento è più articolato e diventa più complesso se bisogna mantenere una certificazione.

La certificazione comporta alcuni obblighi tra i quali: il mantenimento delle competenze, il rispetto del codice etico e la raccolta/gestione di eventuali reclami sul proprio operato. Inoltre le certificazioni scadono triennialmente ed ogni anno richiedono alcuni adempimenti formali (raccolta delle evidenze di audit svolti, regolarizzazione dell'iscrizione, raccolta evidenze dell'aggiornamento professionale, dichiarazioni inerenti eventuali reclami ecc.). Ogni registro utilizza proprie regole di dettaglio che possono variare leggermente tra registri nazionali (CEPAS, KHC, SICEV) ed internazionali (IRCA, RICEC).

Diciamo che tutti gli attestati di qualifica hanno una scadenza predeterminata, in genere tre anni dalla data di conseguimento, salvo aggiornamento degli standard, in tal caso è necessario seguire almeno un corso di aggiornamento secondo quanto indicato dal sistema ISO. Questo vale sia per auditor qualificati sia per auditor certificati. Per questi ultimi però c'è l'obbligo di frequenza e superamento esame se si vuole mantenere la certificazione attiva.

Per gli auditor certificati sono previsti dei requisiti minimi di aggiornamento (l'aggiornamento continuo delle competenze). Anche qui ogni registro decide quali e quanti tipi di formazione accettare. In genere si parla di crediti formativi raccolti nel corso di seminari, corsi di varia natura (sempre attinenti l'InfoSec) nell'arco del triennio di validità della certificazione.

Come avrete capito la differenza sostanziale tra auditor qualificati e certificati è nella obbligatorietà dei passaggi: un auditor qualificato può cessare di aggiornarsi quando vuole senza alcuna conseguenza diretta; per un auditor certificato sospendere la formazione continua può significare perdere il certificato e ricominciare da zero!

D. In un contesto articolato come quello presentato risulta importante poter verificare la significatività del corso e di chi eroga il corso. Può fornirci elementi per valutare la validità dei corsi e raccontarci come e da chi i corsi vengono accreditati?

R. Da quello che abbiamo detto finora possiamo riassumere quanto segue: per certificarci abbiamo bisogno di essere prima qualificati, la qualifica si ottiene solo partecipando e superando un corso a sua volta riconosciuto per l'iscrizione ad un registro.

In Italia operano 3 organismi di certificazione del personale (CEPAS, KHC, SICEV), ognuno è accreditato in Italia da Accredia (ex Sincert) per vari standard.

A livello internazionale operano invece almeno altri 2 organismi di certificazione del personale (IRCA e RICEC). Solo RICEC dispone di accreditamento che permette il mutuo riconoscimento, anche in Italia, dei titoli rilasciati. IRCA invece è da sempre considerato "standard de facto" per effetto della sua esperienza e visibilità a livello mondiale e non è accreditato (sebbene ultimamente si parli di accordi con alcuni organismi di accreditamento per avvicinare IRCA al mutuo riconoscimento).

In generale, è opportuno riferirsi ad organismi accreditati per assicurare che i nostri sforzi siano riconosciuti sempre e comunque e che, quindi, la mia certificazione sia spendibile in tutto il mondo senza ulteriori esami o aggiustamenti.

L'accREDITAMENTO, in Italia assicurato da Accredia, permette ad un Organismo di Certificazione del Personale di garantire che i corsi "riconosciuti" soddisfano standard internazionali (come ad es.: ISO 17024) e che le professionalità, qualificate per mezzo di tali corsi, godano della riconoscibilità ed affidabilità internazionale necessaria. In definitiva, l'accREDITAMENTO permette ad un professionista di essere qualificato/certificato e di poter operare a livello internazionale per mezzo di meccanismi di mutuo riconoscimento del titolo. Da sottolineare che gli Organismi di Certificazione del Personale, comunque, non progettano né erogano corsi di addestramento. Si limitano a qualificare i corsi che ritengono "idonei allo scopo".

Se un corso non è qualificato da un Organismo di Certificazione del Personale accreditato allora c'è da valutarne l'utilizzabilità futura. Ciò non significa che il corso sia più o meno valido, significa invece che potrò o meno spendermi la qualifica per una futura certificazione o per eseguire audit in Italia e all'estero.

Per riassumere, il corso *deve* essere "riconosciuto" o "qualificato" dall'Organismo di Certificazione del Personale che a sua volta dovrebbe essere accreditato (possibilmente all'interno del Multi Lateral Agreement) dall'organismo di accREDITAMENTO nazionale (Accredia in Italia). Questo corso "qualifica" auditor/lead auditor per i Sistemi di Gestione per la Sicurezza delle Informazione secondo lo standard ISO/IEC 27001:05. Le successive attività di iscrizione al registro, gestito dal medesimo Organismo di Certificazione del Personale, permetteranno di raggiungere la certificazione i qualità di Provisional, Auditor, Lead auditor (in funzione delle esperienze e competenze effettivamente dimostrate all'apposito comitato di valutazione).

Si tratta non tanto di un gioco di parole quanto di una "catena di riferibilità" che permette a ciascuno di essere sicuro del cosa sta acquistando, da chi, quali caratteristiche ha, cosa garantisce, dove e come ci si può registrare e certificare successivamente.

Ipotizziamo un "giro" per verificare le credenziali di un corso:

1. ogni corso dovrebbe disporre di un codice identificativo che permette di risalire alla "qualifica/riconoscimento" da parte di un Organismo di Certificazione del Personale. Il codice in genere è associato al "provider" del corso, cioè all'organizzazione proprietaria del corso. Il codice del corso dovrebbe essere chiaramente scritto ed identificabile nelle locandine e/o nei moduli di adesione al corso.
2. Nel sito dell'Organismo di Certificazione del Personale cerchiamo quindi il codice del corso, associato a chi lo eroga (il provider).
3. Sul sito di Accredia verifichiamo se l'Organismo di Certificazione del Personale è accreditato per quel tipo di schema di certificazione.
4. Se conosciamo il nome dei docenti verifichiamo che loro stessi siano inseriti in almeno uno dei registri per auditor/lead auditor di quello standard (non essere certificati come lead auditor significa che la competenza e l'esperienza non viene verificata e che quindi la stessa conoscenza della norma potrebbe essere debole o addirittura inadatta alla docenza in questo tipo di corsi!). In definitiva, se il corso è qualificato da un Organismo di Certificazione del Personale, i docenti dovranno essere in possesso della relativa certificazione.
5. Se, e solo se, tutti i controlli hanno dato esito positivo possiamo tranquillamente iscriverci altrimenti è necessario inviare richieste di chiarimento al provider ed evitare di ottenere titoli che poi non saranno utilizzabili per la certificazione ed l'iscrizione ai registri.

D. Quali sono le peculiarità dei corsi per auditor/lead auditor di cui abbiamo parlato? Come si svolgono gli esami di questi corsi?

R. Una nota fondamentale da considerare prima dell'iscrizione a questi corsi: non si tratta di corsi dove apprendere la norma bensì si tratta di corsi di "abilitazione" per auditor. L'accesso a questi corsi, in genere, è subordinato al possesso di competenze ed esperienze minime pregresse nell'InfoSec, ed in particolare nell'audit.

Quindi è indispensabile verificare quali siano i requisiti minimi richiesti e se siamo in grado di soddisfare tale richiesta. Più siamo allineati ai prerequisiti più sarà elevata la probabilità di successo nell'esame finale.

Tutti i corsi prevedono un esame finale, in genere nell'ultimo giorno di corso. Sono previste varie prove intermedie e la valutazione continua dei discenti ma il vero esame è uno solo.

La correzione può avvenire in aula (come in genere prevedono gli organismi di certificazione del personale italiani) o a posteriori (nel caso degli organismi internazionali).

L'esame può includere sezioni a risposta multipla, a risposta aperta e/o interviste a seconda dei casi. Un solo elemento è sempre comune: la presenza di "scenari" nei quali identificare, formulare e classificare le eventuali non conformità (in pratica il "cuore" di questi corsi).

La durata complessiva va dalle due ore e mezza alle quattro ore. La correzione è in genere assicurata da esaminatori (singoli o commissioni) diversi dal docente per assicurare l'indipendenza di giudizio ed evitare qualsiasi potenziale compromissione o inquinamento delle prove d'esame.

Il mancato superamento dell'esame non deve impressionare né scoraggiare, è un incidente di percorso in cui più o meno siamo tutti incappati almeno una volta. L'importante è capire "perché e dove ho sbagliato". Tutti i corsi prevedono la possibilità di ripetere il solo esame entro un anno solare. Le motivazioni principali per il mancato superamento dell'esame, a mio avviso, possono essere sintetizzate in questo modo:

- Scarsa conoscenza della norma di riferimento.
- Totale inesperienza negli audit, interni o esterni che siano.
- Ricerca di soluzioni alternative rispetto alle domande del testo o errata comprensione delle domande d'esame.
- Mancato completamento degli esercizi corsuali o incompleta comprensione delle tematiche d'aula.
- Incapacità di redigere una checklist riconducibile alla norma mantenendo l'approccio per processi richiesto in tutti gli audit.
- Assenza superiore al 10% delle ore di corso.

Per i corsi con riconoscimento internazionale (IRCA e RICEC) il 50% di insuccessi ed oltre può essere normale. I corsi con riconoscimento nazionale in genere hanno un più alto indice di successo, direi oltre il 70% nella mia esperienza. Ciò è dovuto alle modalità di gestione ed erogazione del corso e non al contenuto del corso. Per i corsi internazionali non avere i prerequisiti d'ingresso può effettivamente essere un problema sebbene il risultato finale di tali corsi sia spesso una preparazione eccellente ma molto dipende dall'aula nel suo insieme e dall'abilità del docente di far "recuperare" chi è meno preparato.

Interessante notare che non esiste al momento la necessità che il docente abbia seguito corsi specifici per formatori/trainer d'aula. Anche questo entra nella discrezionalità e nella serietà professionale di ciascun docente. L'abilità e la "dote" naturale potrebbero non essere sufficienti.

D. Ha qualche suggerimento per chi volesse intraprendere questa professione a valle di un corso di qualifica?

R. Senza dubbio continuare ad esercitare la professione originale mantenendo così il giusto equilibrio con gli eventuali audit. Un auditor professionista può eseguire tra 70 e 100 audit l'anno, in ogni caso non si dovrebbero superare le 100 giornate di audit l'anno per evitare di perdere di vista lo "sviluppo" dell'InfoSec. Non si possono fare audit se non si è aggiornati e non si opera nell'InfoSec! La velocità di cambiamento del settore non permette di "assentarsi" per lunghi periodi dall'operatività della sicurezza delle informazioni.

Un secondo consiglio che mi sento di dare è lo sviluppo di argomenti quali: il project management (l'audit è di fatto un progetto da gestire), il public speaking, la gestione delle tensioni, il team building e la conoscenza approfondita di almeno una lingua straniera (possibilmente inglese).

Insomma, la costituzione di un "soft skill" che possa supportare il tecnicismo dell'InfoSec durante le interviste e la gestione operativa dell'audit.

D. *Stando a queste sue affermazioni sembra importante la cura di conoscenze complementari. Quali altre potrebbero essere utili ad un auditor/lead auditor dei Sistemi di Gestione per la Sicurezza delle Informazioni?*

R. Ad oggi sembra impossibile poter operare senza conoscere i modelli dell'IT più diffusi, come ad esempio: ITIL e COBIT. Anche altre certificazioni come CISA, CISM, CISSP, EUCIP ecc. possono costituire una valida base di partenza.

A questi dobbiamo aggiungere l'indispensabile conoscenza della madre di tutte le norme ISO, la oramai arcinota ISO 9001:2008, alla quale quasi tutte le norme si ispirano o riconducono. La recente ISO/IEC 20000-1:05 direi sia da considerare tra le cose indispensabili da mettere nell'elenco delle conoscenze complementari, considerando che la relazione esistente con l'InfoSec.

Una particolare attenzione deve essere prestata al tema della valutazione dei rischi. Oggi disponiamo della ISO/IEC 27005:08 per l'applicazione nell'InfoSec e della più generale ISO 31000 per gli aspetti generali. Entrambe *indispensabili* per assicurare un'esatta comprensione delle tematiche connesse alla valutazione e gestione dei rischi. Da non dimenticare la Norma nazionale UNI 11230 che è di introduzione all'argomento del Risk Management che mi sento di porre all'attenzione dei lettori.

Per l'InfoSec direi che possano essere utili anche competenze in materia di incident handling, disaster recovery, business continuity e così via.

Un'occhiata al cyber crime, al social engineering, alle infrastrutture critiche ed ai tool di intrusione direi sia scontata per qualsiasi auditor del settore. L'approccio organizzativo non deve distogliere dai temi di attualità del mercato, vedi il più recente cloud computing che sta guadagnando sempre maggior visibilità e che pone non pochi dubbi in tema di sicurezza delle informazioni.

Indispensabile, anche se poco compresa, la conoscenza delle leggi e direttive comunitarie riferibili all'InfoSec, io ne cito alcune come base di partenza e solo a titolo di esempio: privacy, responsabilità amministrativa, reati informatici. Poi in funzione del mercato e del tipo di organizzazione da auditare possiamo trovarci di fronte a leggi inerenti le Pubbliche Amministrazioni, le telecomunicazioni, la sanità, i trasporti ecc.

Gli auditor vengono certificati anche in relazione alle loro competenze operative e professionali nell'InfoSec, secondo i codici EA/NACE. È quindi probabile che ciascun auditor abbia approfondito la conoscenza di leggi e direttive nel lavoro di tutti i giorni, queste competenze torneranno utili negli audit per l'esatta comprensione dei fenomeni intorno a noi e nelle applicazioni inerenti lo standard ISO/IEC 27001:05 .

Quindi mai cessare di documentarsi e studiare l'evoluzione sia dello standard sia del mercato.

Vale la pena ricordare che esistono molte associazioni cui è possibile aderire per mantenere aggiornate le proprie competenze, accumulando anche gli eventuali crediti necessari a dimostrare l'aggiornamento continuo. A titolo puramente esemplificativo ne cito alcune (non me ne vogliano tutte le altre che ho dimenticato di citare): Clusit, AIEA, ISACA Roma, AIPSI, INFORAV, AICA, AIIC ecc.

L'adesione a queste associazioni assicura vari servizi ma soprattutto la possibilità di confrontarsi con altri professionisti del settore ed imparare dalle esperienze altrui (tra l'altro è una delle contromisure suggerite nella ISO/IEC 27001:05!).

Gli stessi registri degli organismi di certificazione del personale spesso organizzano eventi tecnici e non per l'aggiornamento delle competenze degli auditor.

In ultimo, per noi italiani, varrebbe la pena di dare un contributo allo sviluppo stesso dello standard, aderendo ad UNINFO. Ognuno di noi è in grado di fornire un contributo significativo allo sviluppo dello standard, aderire al Gruppo di Lavoro ISO 27000 di UNINFO significherebbe partecipare ai lavori di aggiornamento dello standard (e delle guide ad esso collegate), condividendo esperienze ed iniziative con altri professionisti che volontariamente mettono a disposizione le loro competenze per lo sviluppo dell'InfoSec in Italia e per il riconoscimento del ruolo dell'Italia nella crescita dello standard. L'adesione ha un costo contenuto ma i benefici che se ne traggono sono infinitamente superiori!

D. Torniamo per un momento ai titoli rilasciati nei corsi per auditor/lead auditor. Ad oggi vi sono molti provider, come possiamo verificare la validità di un titolo da noi posseduto ed avviare le eventuali pratiche di certificazione?

R. Domanda pertinente ed estremamente interessante. Tornando al nostro "giro" direi di verificare innanzitutto quale sia il provider evidenziato nell'attestato e l'eventuale numero di registrazione del corso. Con questi elementi, via internet, verifico che il provider abbia provveduto alla qualifica/registrazione del corso. Questa verifica deve essere fatta

prima sul sito del provider e poi sul sito dell'Organismo di Certificazione del Personale che ha qualificato/registrato il corso. Successivamente posso verificarne l'eventuale accreditamento sul sito dell'organismo di accreditamento nazionale (quelli del multilateral agreement si trovano su internet o sul sito di Accredia).

Se tutte le ricerche hanno dato esito positivo possiamo contattare l'Organismo di Certificazione del Personale che ha qualificato/registrato il corso e dare il via alle pratiche di certificazione ed iscrizione al registro.

In caso contrario è opportuno contattare il provider del corso e chiedere chiarimenti per le eventuali carenze rilevate o per dichiarazioni integrative utili al nostro percorso (talvolta accreditamenti, qualifiche, registrazioni sono pubblicate in ritardo su internet oppure possono incontrare lungaggini burocratiche che inficiano l'esito delle nostre ricerche).

D. Quali sono i passi successivi all'ottenimento della qualifica? Spesso il "cosa succede dopo" non viene trattato nei corsi oppure resta avvolto nell'incertezza. Lei cosa suggerisce?

R. Purtroppo durante i corsi si dà enfasi all'oggetto del corso e il tempo non è mai a sufficienza. Ecco perché, sebbene previsto, al termine del corso non si abbia chiaro "cosa succede dopo". C'è anche da sottolineare che l'interesse delle persone durante il corso è legittimamente orientato al superamento del corso. Il "cosa succede dopo" sembra lontano in quei momenti pertanto, anche parlandone, spesso se ne perde il reale contenuto.

Dopo l'ottenimento dell'attestato (che dichiara la mia qualifica di auditor/lead auditor) inizia il vero lavoro certosino della raccolta delle evidenze necessarie per la certificazione.

Vediamo però i requisiti *minimi* per essere certificati ed iscritti in un registro (meglio se accreditato):

- Diploma di scuola media superiore
- Superamento di un corso qualificato/registrato (è l'attestato che abbiamo in mano a questo punto)
- Esperienza lavorativa generale di almeno 5 anni di cui almeno 2 nell'InfoSec.

A questi dobbiamo aggiungere l'esperienza in qualità di auditor/lead auditor, infatti la certificazione differisce in funzione dell'esperienza specifica nel ruolo (e non nella qualifica ottenuta in aula!):

- Come auditor: almeno 20 giornate di audit distribuite su almeno 5 audit nei quali si è ricoperto il ruolo di auditor, per tutte le fasi dell'audit, accanto ad un lead auditor già certificato dallo stesso organismo del personale che detiene il registro cui sto chiedendo la certificazione. In questo ruolo, il Lead Auditor dovrà sempre affiancare il candidato Auditor.
- Come lead auditor occorre aggiungere: almeno 15 giornate di audit distribuite su almeno 3 audit nei quali si è ricoperto il ruolo di lead auditor, per tutte le fasi

dell'audit, accanto ad un lead auditor già certificato dallo stesso organismo del personale che detiene il registro cui sto chiedendo la certificazione. In questo ruolo, il candidato Lead Auditor potrà lavorare in autonomia, stante il fatto che verrà giudicato per la capacità di condurre le riunioni con l'organizzazione cliente, per la capacità di pianificazione degli Audit, per la capacità di sintetizzare le risultanze di Audit e di predisporre il relativo Rapporto, comprensivo dei rilievi. Saper scrivere un rilievo è tutt'altro che una banalità!

Queste specifiche possono cambiare leggermente in relazione all'Organismo di Certificazione del Personale ed al paese in cui risiede il registro. Per maggiori dettagli occorre sempre scaricare i regolamenti dai siti ufficiali.

Alcuni registri (soprattutto quelli italiani) prevedono un esame aggiuntivo all'atto dell'accettazione della richiesta di iscrizione. In questi casi i regolamenti spiegano i contenuti e le modalità di partecipazione.

Quindi, subito dopo l'arrivo dell'attestato, inizia il lungo percorso (che comunque non può superare i tre anni, oltre i quali scade lo stesso attestato) di raccolta delle evidenze che testimoniano l'esperienza in qualità di auditor/lead auditor ed il possesso dei requisiti minimi generali.

Qui arriva la domanda faticosa: *se non sono certificato come faccio a svolgere audit?*

Domanda legittima e testimonianza di quanto il mercato abbia confuso le idee.

Non devo essere certificato per svolgere gli audit! Posso svolgere gli audit dal momento stesso in cui ricevo l'attestato di qualifica.

La certificazione abbiamo detto essere un processo successivo e volontario. Posso esercitare senza essere certificato. La certificazione è qualcosa che aggiungo per consolidare e rendere "visibile" la mia competenza e specializzazione, così come il mio impegno a gestire in modo pro-attivo gli eventuali reclami e l'adesione ad un codice deontologico che garantisce il mercato.

Quindi, una volta ottenuto l'attestato, via agli audit. Importante è registrarne i dati per poi sottoporli all'Organismo di Certificazione del Personale. I dati minimi indispensabili per ciascun audit sono:

- Dati del committente dell'audit (ragione sociale, indirizzo, telefono/fax, e-mail del referente)
- Dati del valutando (ragione sociale, indirizzo, telefono/fax, e-mail del referente del SGSI, numero di occupati, numero dei siti)
- Data e durata dell'audit
- Criteri dell'audit (soprattutto norme/standard utilizzati)
- Numero di auditor nel team

- Riferimenti al lead auditor garante (per intenderci quello che ha eventualmente supervisionato il mio operato, così come richiesto dal registro)

Alcuni organismi di certificazione del personale (ad es. IRCA) predispongono appositi moduli scaricabili dal sito, in altri casi può bastare un file excel o la dichiarazione del committente. L'importante è che i dati minimi di cui sopra siano evidenti e chiaramente esplicitati.

Una volta terminata la raccolta posso avviare le pratiche per la mia certificazione.

Una volta ottenuta la certificazione e l'inserimento nel registro otterrò le informazioni per il mantenimento (inclusi i criteri di aggiornamento e raccolta dei crediti formativi e quindi per il rinnovo triennale).

Come tutte le competenze si ha quindi l'obbligo dell'aggiornamento continuo che può condurre all'innalzamento della qualifica ottenuta (da provisional ad auditor, da auditor a lead auditor) per mezzo della dimostrazione delle esperienze di audit cumulate nel triennio di validità della certificazione. Ovviamente è anche possibile il "downgrade" qualora non riuscissimo a dimostrare il mantenimento/raggiungimento delle competenze minime richieste per il ruolo certificato.

D. Quali sono le differenze sostanziali con le altre certificazioni di cui ci ha parlato?

R. Esistono, almeno per quanto io ne sappia, due grandi raggruppamenti di certificazioni: quelle accreditate e quelle non accreditate secondo standard ISO.

Quelle accreditate (ad es.: CISA, CISM di ISACA, CISSP di ISC²) hanno valenza in tutto il mondo essendo state sottoposte al controllo di un organismo di accreditamento secondo la ISO 17024. Ciò significa che un organismo indipendente dal provider ne verifica i contenuti e la conformità ad uno schema preciso, con cadenza periodica, assicurandone così l'efficacia e il miglioramento continuo nel tempo.

Quelle non accreditate (ad es. EUCIP, LoCSI ecc.) pur mantenendo il loro valore e serietà, non hanno un riconoscimento omogeneo a livello nazionale ed internazionale. Inoltre il sistema che le supporta non è basato su standard comuni e/o pubblici verificati in maniera indipendente da organismi accreditati secondo schemi internazionali. Ciò non ne inficia la validità rispetto al mercato ma ne limita il riconoscimento e l'utilizzazione al di fuori di determinati contesti.

Un'altra classificazione prevede la distinzione tra certificazioni proprietarie e pubbliche. Laddove per pubbliche si intende riferibili a schemi internazionali, liberi da vincoli e da associazioni che le controllano. In questo caso gli esempi precedenti (CISA, CISM, LoCSI ecc.) rientrano in quelle proprietarie e quindi prevedono proprie regole per affrontare il percorso di certificazione. La certificazione del lead auditor è indipendente (essendo basata

su standard ISO) e non prevede l'appartenenza a nessuna associazione per poter essere affrontata né tanto meno l'aderenza ad uno standard proprietario.

Ciò non toglie che io possa comunque essere associato ad altre organizzazioni e certificarmi come lead auditor (personalmente aderisco ad una decina di associazioni nazionali ed internazionali e possiedo 6 certificazioni distribuite in 3 diversi registri tra nazionali ed internazionali). La mia competenza è proprio dovuta al continuo aggiornamento che deriva da questo mix.

Altra sostanziale differenza tra la certificazione come auditor/lead auditor ISO sta nell'obbligo di utilizzare la ISO 19011 per la gestione e conduzione dell'audit, cosa non vera nelle altre certificazioni. Ciò assicura al committente ed al valutando, non solo la professionalità e verificabilità del mio operato, ma anche il rispetto di principi e norme per la raccolta delle evidenze, per la stesura del piano di audit e del rapporto finale ecc.

Le certificazioni non ISO sono percorsi complementari e non alternativi per un auditor professionista. Non siamo in competizione con schemi tipo CISA, semmai ne apprezziamo le differenze e complementarità. Io tenderei a considerarle entrambe sapendo però che mirano a risultati diversi.

La mia qualifica è valida per operare per conto di un organismo di certificazione, in audit di parte terza, le altre certificazioni no. Hanno altri ambiti ed obiettivi, ad esempio per CISA l'InfoSec copre un dominio su 5 mentre per la ISO/IEC 27001:05 l'InfoSec è l'unico argomento in discussione. Modelli diversi, scopi diversi, stili diversi. Ecco perché un CISA non può fare un audit su un SGSI ed un auditor SGSI non può sfruttare appieno CISA. Salvo avere entrambe le qualifiche e certificazioni! Un esempio può essere costituito dallo studio di AIEA nella comparazione del modello COBIT con lo standard ISO/IEC 27001:05.

Se però scelgo di stare fuori dagli organismi di certificazione allora questa differenza viene sfumata e rimane solo la garanzia delle modalità di conduzione e gestione dell'audit assicurate dall'applicazione della ISO 19011:02. Non dovendo assicurare neanche il rispetto di quest'ultima, la differenza tra un corso ISO e qualsiasi altra certificazione/qualifica, viene meno ed i corsi iniziano ad essere equivalenti (almeno sul piano formale). Nel senso che fuori del mondo della certificazione ISO la necessità di un approccio basato sulla ISO 19011 potrebbe non essere significativo e non influenzare l'esito di un audit.

Un auditor/lead auditor per i sistemi di gestione per la sicurezza delle informazioni dispone delle competenze specifiche per gestire e condurre audit su sistemi di gestione conformi alla ISO/IEC 27001:05, e l'audit è gestito secondo lo standard ISO 19011:02 per poter assicurare la ripetibilità e la tracciabilità dei risultati ottenuti.

Il fatto che sia certificato ed inserito in un registro testimonia l'impegno dell'auditor al mantenimento delle competenze, alla verifica continua e indipendente delle sue competenze e credenziali.

E' di fatto il termine "certificazione" a creare confusione: nel mondo ISO/accreditato la si utilizza come attestazione della competenza del personale (rilasciata da un organismo indipendente) rispetto ad uno standard di riferimento mentre nel resto del mondo la si usa spesso come attestazione del superamento di un esame.