

A tutti gli Organismi di Certificazione accreditati ISO 37001  
Att.: Responsabili di schema

Alle Associazioni degli organismi di valutazione della conformità

Ns. rif.: DC2017SSV335

Milano, 20/11/2017

Oggetto: **Circolare Tecnica N° 28/2017 - Dipartimento Certificazione e Ispezione  
Informativa in merito all'accreditamento per lo schema di certificazione ISO 37001  
Prevenzione della corruzione**

Questa comunicazione sostituisce la ns. **Circolare N° 33/2016**  
Questa circolare si applica dal 1.01.2018 per tutti i nuovi contratti di Certificazione e per tutti i rinnovi.

## Introduzione

In molti paesi, e in specifici settori, la corruzione, nei confronti del pubblico o fra privati, costituisce un fenomeno ormai diffuso, tanto da essere tollerata, in alcuni contesti merceologici o geografici, come una parte "necessaria" del *business*.

Tuttavia, la crescente consapevolezza dei danni causati dalla corruzione, anche grazie all'operato delle organizzazioni internazionali, delle autorità amministrative quali ANAC in Italia e delle varie magistrature nazionali, ha sollecitato la definizione di strategie ed azioni tese a ridurre il rischio e gli impatti, anche tenendo conto dell'utilità, a fronte della globalizzazione del crimine, di disporre di uno strumento normativo transazionale di contrasto alla corruzione.

La questione è cresciuta di importanza in ragione della combinazione di vari fattori:

- il cambiamento del contesto giuridico, nel quale la maggioranza dei Paesi criminalizza e persegue la corruzione;
- la crescente consapevolezza dei danni che la corruzione causa ai Paesi, all'economia ed agli individui;
- l'attenzione da parte delle organizzazioni verso la responsabilità sociale e all'approccio etico delle imprese (in Italia si veda il Decreto legislativo 231/ 2001 – che prevede specificatamente, fra i reati presupposto, la corruzione – attiva e passiva – verso la P.A. nonché la corruzione tra privati);
- l'estremo rischio finanziario e reputazionale, oltre che di veder compromessa la continuità aziendale, nel quale possono incorrere gli enti laddove si trovino implicati in fatti corruttivi.

ISO ha così sviluppato uno specifico *standard* in materia di prevenzione della corruzione, la ISO 37001 "Anti- Bribery Management Systems", strumento operativo che non si sostituisce, bensì si aggiunge, alle misure già previste – a livello normativo o regolamentare - dai singoli paesi. È il caso, ad esempio del *UK Bribery Act* e delle diverse misure italiane (il cosiddetto "Pacchetto Anticorruzione").

Questo nuovo *standard* contribuisce a definire le modalità in base alle quali le organizzazioni potranno dichiararsi "compliant" rispetto alla prevenzione del fenomeno corruttivo, ovvero potranno adottare misure di prevenzione ragionevoli e proporzionate al rischio di corruzione. La nuova norma è impostata secondo la *High Level Structure*, applicata tra l'altro anche alla nuova ISO 9001:2015 e all'ISO 14001:2015, ed è rivolta ad Aziende di qualsiasi dimensione o natura, sia pubbliche che private.

La ISO 37001 specifica le misure e i controlli adottabili da un'organizzazione per monitorare le proprie attività aziendali al fine di prevenire la corruzione. Rientrano tra questi la predisposizione di una politica anticorruzione, l'impegno in tal senso da parte dell'Alta Direzione, l'individuazione di un incaricato, la formazione di tutti gli interessati (vale la pena di ricordare che tale processo deve essere continuo e

predisposto in modo da far crescere la cultura organizzativa), la valutazione dei rischi specifici, la definizione di relative procedure, come ad esempio la regolamentazione di omaggi e regali, il monitoraggio dei fornitori e dei *partner* commerciali.

Essendo strutturata secondo la *high level structure*, la norma può essere integrata facilmente con gli altri sistemi di gestione, come la ISO 9001, e i suoi obiettivi possono essere inclusi nel piano di miglioramento continuo.

Il rispetto dello *standard* può essere oggetto di certificazione da parte di organismi terzi, ciò che potrebbe assumere anche rilevanza scriminante di eventuali responsabilità penali o para-penali in determinati ordinamenti giuridici.

## Contesto Normativo

Lo *standard* ISO 37001 si basa sul *British Standard* BS 10500, prima norma ad interessarsi a questo argomento già nel 2011. La norma ISO è stata pensata per aiutare le organizzazioni pubbliche, private o non governative di qualsiasi dimensione, a prevenire il compimento di atti corruttivi da parte dei propri dipendenti e collaboratori, o da qualunque soggetto agisca in suo nome, e per favorire il diffondersi di una cultura aziendale basata sull'etica e sulle buone pratiche commerciali.

Va sottolineato che il significato di "corruzione" cui fa riferimento la norma ISO 37001 comprende tutte le condotte o attività che, ancorché formalmente lecite, sono rilevanti (direttamente o indirettamente) sotto il profilo dei rischi di corruzione e si pongono come ostacolo rispetto al perseguimento delle finalità d'interesse generale cui sono preposte sia le organizzazioni pubbliche che quelle private (si pensi ad esempio al vastissimo mondo del non profit, della cooperazione sociale, della sanità e dell'istruzione private, delle imprese private appaltatrici di pubblici servizi, delle organizzazioni non governative).

Lo *standard* richiede l'adozione di alcuni elementi portanti, tra cui:

- una politica per la prevenzione della corruzione, procedure e controlli;
- comunicazione di tale politica e del relativo programma a tutte le parti interessate e/o associate;
- la *leadership*, l'impegno e la responsabilità;
- una procedura di sorveglianza;
- formazione relativa alla prevenzione della corruzione;
- valutazione dei rischi;
- *due diligence* su progetti e *business partner* dell'organizzazione;
- *reporting*, monitoraggio, indagine e riesame dell'Alta Direzione e, se presente, dell'Organo di *governance*;
- richiesta di sottoscrivere un impegno per la prevenzione della corruzione ai propri associati;
- implementare i controlli finanziari a ridurre i rischi di corruzione;
- azioni correttive e di miglioramento continuo.

La verifica circa la corretta implementazione dei requisiti posti dallo *standard* deve essere focalizzata sul controllo della corretta definizione ed applicazione delle procedure predisposte dall'organizzazione al fine di gestire i cosiddetti processi critici, così come emersi dall'analisi dei rischi e dalle eventuali *due diligence*, secondo quanto previsto dalla norma stessa. Infatti una descrizione formale delle attività sensibili è il primo passo per effettuare attività di controllo tramite *audit*.

## Elementi specifici dello schema ISO 37001 rispetto agli altri Sistemi di gestione.

Un elemento essenziale nel processo di certificazione è rappresentato dalle informazioni che l'ente sottoposto a verifica fornisce al CAB. Infatti, l'*audit* di prima certificazione avviene in organizzazioni delle quali il CAB non ha dati *ex ante*, se non quelli ricavati dalle dichiarazioni spontanee delle stesse organizzazioni, o per notizie apprese dai *media*. Questo aspetto è particolarmente critico, dal momento che non è sempre possibile comprendere se l'impresa, pur munita di corrette procedure (adottate o meno in applicazione alla legislazione applicabile in tema di *corporate crime*), rappresenti un "ambiente patologico" sotto il profilo della corruzione. Lo *standard* ha infatti finalità preventiva, che risulta incompatibile con un ambiente di impresa patologico, che necessita di correzione anziché di prevenzione.

Si osservi che qualsiasi ambiente contaminato da pratiche corruttive (con le connessioni criminali che spesso le accompagnano), anche se mai toccato da indagini di polizia giudiziaria, sarà comunque un contesto ove lo sviluppo ed efficace applicazione del sistema di gestione non potrà avere un approccio preventivo, ma correttivo, e sarà anche osteggiato, più probabilmente pilotato, proprio da quella compagine che ha interesse a creare una immagine di apparente legalità, funzionale alla perpetrazione delle pratiche di corruzione.

Diversamente, un'azienda che dichiari "spontaneamente" un'eventuale esistenza di situazioni "critiche" o già rilevanti a livello giudiziario, può essere un Cliente idoneo per il percorso di certificazione, con approccio "correttivo", ma anche di sviluppo di prassi "preventive". Infatti, in questo secondo caso, l'adozione del sistema di gestione anticorruzione sarà da intendere come azione finalizzata e coerente con un approccio "terapeutico" aziendale (azione ampia e strutturata a livello sistemico), che ci si augura (dovrà essere oggetto di valutazione) sia fortemente sponsorizzato dalla direzione.

Parliamo di "azione ampia e strutturata a livello sistemico" in quanto la cultura di "compliance" deve essere pervasiva di tutta l'organizzazione. Anche un sistema di gestione anticorruzione deve essere applicato a tutti i processi aziendali, pena l'esistenza di aree di grigio che possono rendere vana l'applicazione dello stesso sistema di gestione. La visione globale nell'applicazione del sistema di gestione dovrà coinvolgere tutti i processi organizzativi (e in *outsourcing*) almeno in fase di analisi preliminare di contesto e, solo dopo tale valutazione, potranno essere enucleati (con adeguate argomentazioni) i processi considerati non critici, per i quali la valutazione dei rischi potrà limitarsi a questo primo livello di approfondimento.

Ciò significa anche che occorre interpretare e relativizzare a seconda del caso concreto quanto indicato dalla guida di cui all'Allegato "A" della Norma, in particolare per quanto affermato al § A.4.1., relativo alla valutazione dei rischi.

Una metodologia occorre e, in sua assenza, ci si troverà di fronte a situazioni opinabili e per le quali la certificazione avrà delle aree di debolezza strutturale di credibilità; il tempo da allocare a tale verifica di conseguenza dovrà essere sufficiente a comprendere se ci si trovi di fronte a un sistema di gestione efficacemente applicato.

## 1) Regole di certificazione

Norma di accreditamento	UNI CEI EN ISO/IEC 17021:2015
Norma di certificazione	ISO 37001:2016
Criteri di competenza del Gruppo di verifica	<p>Si rimanda alla ISO/IEC 17021-9, <i>Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 9: Competence requirements for auditing and certification of anti-bribery management systems.</i></p> <p>A titolo di esempio, i requisiti di competenza si ritengono soddisfatti quando nel Gruppo di Verifica siano presenti uno o più auditor (o esperti tecnici) che rispettino nel loro insieme i seguenti requisiti</p> <ul style="list-style-type: none"> <li>a) Notevole esperienza, significativa competenza e seniority di settore, maturata attraverso il coinvolgimento in posizioni di rilevante responsabilità nella gestione dei sistemi anticorruzione o di <i>legal compliance</i> o <i>corporate crime</i> (per esempio, S&amp;O, Decreto legislativo 231/2001, Legge 190/2012);</li> <li>b) Conoscenza approfondita e documentata della normativa (legale, regolamentare e in materia di "buone prassi") in tema di prevenzione della corruzione attiva e passiva e di gestione dell'integrità aziendale applicabile al Paese in cui viene svolta l'attività aziendale e di <i>business</i> dell'organizzazione</li> <li>c) Formazione: Corso di 16 ore sulla norma ISO 37001, per chi ha già svolto un corso 40 ore sui sistemi di gestione.</li> </ul> <p>I primi due punti si considerano soddisfatti se la persona è certificata sotto accreditamento per schemi in tema di <i>anti-bribery</i> o Decreto legislativo</p>

	231/2001, oppure se esercita la professione di avvocato, commercialista o revisore, ex magistrato o giudice o funzionario di enti di autorità giudiziaria con esperienza specifica in tema di anti corruzione.
Criteri di competenza del <i>decision maker</i> e del <i>contract reviewer</i>	<p>Si rimanda alla ISO/IEC 17021-9, <i>Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 9: Competence requirements for auditing and certification of anti-bribery management systems.</i></p> <p>Per il <i>decision maker</i>, si richiede inoltre la conoscenza della normativa anticorruzione e <i>corporate crime</i> applicabile al Paese in cui viene svolta la verifica o dove si svolge il <i>business</i> coerentemente con il perimetro di influenza.</p>
Tipologie di soggetti che possono richiedere la certificazione e possibili esclusioni	<p>La certificazione ISO 37001 può essere richiesta da qualunque tipo di organizzazione, di qualsiasi dimensione o natura.</p> <p>La certificazione viene rilasciata ad una sola entità giuridica e comprende tutti i siti, filiali, sedi secondarie, attività e processi effettivamente svolti dall'organizzazione.</p> <p>Non sono ammesse esclusioni a processi / funzioni svolte in una stessa Nazione.</p> <p>È possibile però limitare l'applicazione a specifiche Nazioni, ma il campo di applicazione deve sempre includere <u>processi e attività sensibili</u><sup>1</sup> svolti all'estero quando svolti sotto la responsabilità e il diretto controllo dell'organizzazione (es. uffici di rappresentanza o sedi secondarie agenti o mediatori). Questo aspetto deve essere ben esplicitato nel certificato.</p> <p>Nel caso di gruppi di società, quando attività/processi sensibili siano svolti da altre società del gruppo (capogruppo e/o controllate), anche all'estero, si applica il paragrafo 8.5.della UNI ISO 37001.</p> <p>La conformità ai requisiti di modelli e sistemi di prevenzione previsti da norme di legge (es. Modelli Organizzativi ai sensi del D.Lgs. 231/2001, PTPC ai sensi della L. 190/2012 e simili) non è certificabile sotto accreditamento.</p>
Responsabilità degli OdC	<p>Una organizzazione certificata o in certificazione deve informare tempestivamente il proprio OdC nel momento in cui venisse coinvolta in qualche situazione critica tale da compromettere la garanzia della certificazione del sistema (esempio notizie di pubblico interesse, crisi o coinvolgimento in qualche procedimento giudiziario per fenomeni corruttivi o simili).</p> <p>Altrettanto l'organizzazione dovrà avvisare tempestivamente l'OdC di qualunque evento relativo a fenomeni di corruzione che possa aver coinvolto una o più delle proprie Risorse Umane, e le conseguenti azioni adottate per il contenimento degli effetti di tale evento, l'analisi delle cause radice, le relative azioni correttive.</p>

<sup>1</sup> Elenco non esaustivo di attività e processi sensibili: finanza e controllo, commerciale, agenti e rete vendita, approvvigionamento, figure istituzionali e organi sociali, Uffici di direzione e CdA, internal auditing, gestione licenze, gare e autorizzazioni, gestione risorse umane (compreso gestione, selezione, assunzioni e avanzamenti di carriera), amministrazione e gestione cassa, acquisti, gestione omaggi e liberalità, relazioni con autorità istituzionali ed enti di controllo, gestione patrocini e sponsor, gestione contenziosi e reclami, servizi informatici, gestione security, attività di controllo e collaudi.

	<p>Un OdC che venisse a sapere, direttamente dall'organizzazione o da altre fonti, che la stessa organizzazione è implicata con dei profili di responsabilità in qualche scandalo o in qualche procedimento giudiziario per fenomeni corruttivi, dovrà condurre tempestivamente delle valutazioni / approfondimenti specifici.</p> <p>In questi casi, si raccomanda di dare notizia al mercato del fatto che tale organizzazione è "soggetta a valutazione per gli specifici eventi" (fatti salvi gli obblighi di legge e dei mercati regolamentati – per esempio borsa).</p> <p>Finita l'analisi, l'OdC potrà adottare i consueti provvedimenti del caso (per esempio chiusura della valutazione con archiviazione, adozione dei provvedimenti previsti dai regolamenti di certificazione, rafforzamento della attività ispettive), definiti in funzione della adeguatezza della risposta e delle strategie adottate dall'organizzazione.</p>
<p>Tempi di verifica e periodicità delle verifiche</p>	<p>Si applicano i requisiti applicabili della ISO/IEC 17021-1. Si applica il documento IAF MD 05.</p> <p>Lo Stage 1 deve essere effettuato sempre c/o l'Organizzazione anche nel caso di realtà di piccole dimensioni.</p> <p>L'organizzazione deve fornire evidenza di aver effettuato la valutazione dei rischi su tutti i processi/attività.</p> <p><b><u>Valutazione degli addetti equivalenti</u></b> È necessario considerare la totalità degli addetti coinvolti in attività e processi ritenuti sensibili da parte dell'organizzazione, oltre ai processi / funzioni riportati alla nota 1. È possibile effettuare un adeguamento mediante <u>radice quadrata</u> per gli addetti equivalenti impiegati nei processi operativi di produzione o di erogazione dei servizi, solo nel caso in cui questi processi presentino bassi rischi di corruzione sulla base della valutazione dei rischi effettuata dall'organizzazione, e comunque sempre con esclusione degli addetti coinvolti nei processi / attività sensibili riportati alla nota 1. Parimenti, nel caso in cui processi/attività sensibili dell'organizzazione siano svolti in outsourcing (ad es. consorzi), il calcolo degli addetti deve tenere conto anche di tali soggetti. Nel corso dell'audit di stage 1, l'OdC deve riesaminare la ragionevolezza di tale adeguamento in funzione dei rischi di corruzione identificati e deve verificare la congruenza del numero di addetti comunicati dall'organizzazione in sede di definizione del contratto. Deve essere riportata nel verbale di verifica questa valutazione.</p> <p><b><u>Riduzione del tempo di audit (Decrease in audit time of MS)</u></b> Non sono applicabili fattori di riduzione.</p> <p><u>Si applica la tabella per lo schema EMS</u>, e per la scelta della tabella corretta tra quelle riportate deve essere valutato il livello di rischio in base a quanto segue:</p> <p><b><u>Rischio alto</u></b> Se l'organizzazione richiedente la certificazione sia stata coinvolta negli ultimi 5 anni in indagini giudiziarie relative a fenomeni corruttivi. Pubbliche Amministrazioni Enti pubblici economici Società in controllo pubblico o partecipate dal pubblico</p>

	<p>Associazioni, fondazioni e enti di diritto privato finanziati in modo maggioritario dalla PA o quelle in cui la totalità dei componenti degli organi di amministrazione e indirizzo siano designati dalla PA</p> <p>Enti del terzo settore (es. organizzazioni di volontariato, organismi per la cooperazione) e cooperative sociali</p> <p>Associazioni di categoria (inclusi partiti e sindacati) a rappresentanza nazionale</p> <p>Ordini professionali e collegi nazionali</p> <p>Le aziende dislocate in Paesi che abbiano una votazione CPI inferiore o uguale a 30. La classifica della corruzione percepita è realizzata da Transparency International. Nel caso di aziende dislocate su più Paesi, rientranti nello scopo del certificato, si applica l'indice del Paese con punteggio più basso.</p> <p>Le organizzazioni, non PMI, presenti nei seguenti settori:</p> <ul style="list-style-type: none"> <li>• Sanitario</li> <li>• Costruzioni</li> <li>• Bancario e assicurativo</li> <li>• Utilities (gas, energia termica, elettricità, acqua, trasporti, comunicazioni, servizi postali)</li> </ul> <p><b>Rischio medio</b></p> <p>Organizzazioni non a rischio alto che presentano almeno una delle seguenti condizioni:</p> <ul style="list-style-type: none"> <li>• ricevono contributi, fondi o finanziamenti pubblici, nazionali e internazionali in quota superiore al 30% sul fatturato;</li> <li>• ricevono da parte di Enti e Società Pubblici o istituzioni Internazionali qualsiasi tipo di compenso o retribuzione, compresi quelli derivanti dall'esecuzione di contratti pubblici, per una quota superiore al 30% sul fatturato;</li> <li>• dislocate in Paesi che abbiano una votazione CPI fra 31 e 59<sup>2</sup>.</li> <li>• società di trading, intermediazione e commerciali non classificabili per fatturato come PMI.</li> </ul> <p>Sono classificate a rischio medio le organizzazioni a rischio alto che risultano certificate da almeno 3 anni sotto accreditamento EA/IAF MLA per la ISO 37001. Questa condizione non si applica se l'organizzazione richiedente la certificazione sia stata coinvolta negli ultimi 5 anni in procedimenti relativi a fenomeni corruttivi.</p> <p><b>Rischio Basso:</b> se non rientra nelle due categorie precedenti.</p> <p><b>Rischio limitato:</b> non applicabile.</p>
Scopo del certificato	<p>I criteri per la formulazione dello scopo del certificato sono gli stessi già applicati per la ISO 9001, con particolare attenzione alle attività svolte. Deve essere chiarito nel campo di applicazione se l'organizzazione detiene il controllo su altre organizzazioni, specificando le caratteristiche di tale controllo (es. partecipazioni al capitale, vincoli contrattuali, etc.). Non è necessario riportare nel certificato il settore IAF.</p>
Documenti IAF	<p>Trovano applicazione tutti i documenti IAF relativi ai sistemi di gestione, fatto salvo quanto chiarito in precedenza sul documento IAF MD 05.</p> <p>Per i Multisite, si applicano i documenti IAF in vigore.</p> <p>Non possono essere esclusi dalla base del campionamento siti ove vengono svolti processi/attività a rischio corruzione (si veda la nota 1 e l'analisi rischi</p>

<sup>2</sup> L'Italia nel 2017 ha ottenuto un punteggio pari a 47, quindi, alla data di pubblicazione della circolare, i siti italiani sono tutti almeno a rischio medio

<p>Modalità di verifica e registrazioni</p>	<p><u>predisposta dall'organizzazione).</u></p> <p>Il Gruppo di verifica dovrà valutare con maggiore frequenza, impegno e profondità i processi/funzioni identificati dalla stessa organizzazione e/o dal Team di verifica come a maggior rischio, riportandone una spiegazione nella documentazione di verifica, oltre a quelli sensibili riportati alla nota 1.</p> <p>Il gruppo di verifica non deve limitarsi a prendere atto dell'esistenza dell'analisi dei rischi. E' necessario partire dalla definizione che l'organizzazione si è data di corruzione, che non può essere meno restrittiva di quella che è prevista per legge. Tale definizione deve essere coerente con l'analisi di contesto fatta.</p> <p>L'Organismo deve valutare la completezza ed esaustività dell'analisi dei rischi di corruzione, con riferimento ai requisiti applicabili della norma ISO 37001, e la robustezza del processo di internal auditing per la fattispecie della corruzione, che dovrà essere basato (pianificazione, programmazione ed esecuzione) sui risultati della valutazione dei rischi e della mitigazione adottata, sulle valutazioni di rischio residuo e sul testing dei controlli operativi.</p> <p>Si raccomanda inoltre di stabilire metodiche in grado di assicurare campionamenti rappresentativi in funzione dei rischi, di dedicare tempi adeguati non a controlli "in astratto" e sulla "carta" ma effettuando interviste, verifiche puntuali su transazioni, relazioni con business partner, processi a rischio, analisi delle notizie di pubblico dominio rilevanti, test sulla diffusione dei sistemi di controllo interno.</p> <p>La documentazione di audit (es. report di audit, check-list, ecc.)" deve inoltre riportare, tra le altre cose;</p> <ul style="list-style-type: none"> <li>• Il perimetro e l'applicabilità del Sistema di Gestione (4.3 della ISO 37001)</li> <li>• Definizione di corruzione prevista per l'organizzazione, sviluppata sulla base dell'analisi di contesto</li> <li>• Specifici dettagli in merito alle attività a rischio (riportando in dettaglio processi a rischio ed attività sensibili)</li> <li>• Mappatura dei soggetti (interni ed esterni) che sono coinvolti in attività a maggior rischio</li> <li>• Indicazione dei Partner in Affari e tipo di monitoraggio sugli stessi (tipo di gestione da questi adottata in ottica anticorruzione)</li> <li>• Le relazioni societarie</li> <li>• I riferimenti legislativi specifici</li> <li>• Specifiche indicazioni sulla formazione svolta</li> <li>• L'elenco delle commesse valutate</li> <li>• Analisi degli episodi di corruzione verificatisi e le contromisure adottate</li> </ul>
---	--

## 2) Processo di Accredimento

Si potranno presentare diverse casistiche, in base agli accreditamenti ACCREDIA già posseduti dall'Organismo di Certificazione che presenta la domanda di accreditamento o estensione.

Rimangono invariati i requisiti previsti dal RG-01 e RG-01-01 per la concessione dell'accREDITAMENTO ed estensione.

Per organismi già accreditati ISO/IEC 17021, non occorre che questi abbiano già rilasciato dei certificati in questo schema per fare domanda di estensione dell'accREDITAMENTO.

Il certificato di accREDITAMENTO non riporta i relativi settori di accREDITAMENTO.

Nel caso in cui l'OdC posseda già accreditamenti rilasciati da altri enti, dovrà essere fatta una valutazione caso per caso, in base agli accordi EA / IAF MLA applicabili.

A	OdC già accreditato per lo schema ISO/IEC 17021-1	Esame documentale di 1 giornata (da svolgersi possibilmente presso l'OdC).  1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accREDITAMENTO e le successive attività di sorveglianza.
B	OdC non ancora accreditato ISO/IEC 17021-1, ma accreditato per altri schemi di accREDITAMENTO	Esame documentale di 1 giornata.  Verifica ispettiva presso la sede dell'OdC di 2 giornate. 1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accREDITAMENTO e le successive attività di sorveglianza.
C	OdC non ancora accreditato in nessuno schema	Esame documentale di 1 giornata.  Verifica ispettiva presso la sede dell'OdC di 4 giornate.  1 Verifica in accompagnamento di durata congrua alla dimensione organizzativa del cliente. ACCREDIA si riserva di valutare caso per caso l'idoneità delle organizzazioni e dei Gruppi di Audit proposti per l'accREDITAMENTO e le successive attività di sorveglianza.

Documentazione da presentare ad Accredia per l'esame documentale

- a) Lista di riscontro o linea guida o istruzioni predisposte dall'OdC per il GVI;
- b) Criteri di qualifica di chi svolge il riesame del contratto, degli *auditor* e dei *decision maker*;
- c) *Curricula* degli ispettori e dei *decision maker* e giustificazione per la loro singola qualifica;
- d) Procedura per la costituzione e gestione dei Gruppi di *Audit*;
- e) Attestato/Certificato rilasciato dall'OdC;
- f) Lista dei certificati già emessi, e delle prossime attività di verifica (dato necessario per poi pianificare la verifica in accompagnamento);
- g) Procedure / regolamenti contrattuali applicabili alla verifica, nonché le procedure interne per la gestione della pratica di certificazione (dall'offerta alla Certificazione);
- h) Per gli OdC NON accreditati ISO/IEC 17021, oltre ai documenti sopra riportati, occorre inviare la documentazione richiesta nella domanda di accREDITAMENTO.

### 3) Mantenimento dell'AccREDITAMENTO

Per il mantenimento dell'accREDITAMENTO, durante l'intero ciclo di accREDITAMENTO, salvo situazioni particolari (Es: gestione reclami e segnalazioni, modifiche intervenute sullo schema di certificazione, cambiamenti nella struttura dell'Organismo, implicazioni in cause giudiziarie...), verranno condotte le seguenti verifiche:

- o se l'OdC ha emesso meno di 50 certificati nello schema di certificazione, devono essere fatte una verifica in accompagnamento e una verifica in sede;
- o se l'OdC ha emesso tra 51 e 200 certificati nello schema di certificazione, devono essere fatte 2 verifiche in accompagnamento e 1 verifica in sede;
- o se l'OdC ha emesso più di 201 certificati nello schema, devono essere fatte 2 verifiche in accompagnamento e 2 verifiche in sede.

Siamo a disposizione per chiarimenti.

Il Direttore di Dipartimento  
Dr. Emanuele Riva

