CIRCOLARE TECNICA Prot. DC2021SPM091 **DATA** Milano, 07/07/2021

A tutti gli Organismi di certificazione accreditati e in corso di accreditamento

Alle Associazioni degli Organismi di valutazione della conformità

A tutti gli Ispettori/Esperti di Accredia

Loro sedi

OGGETTO **Circolare Tecnica DC N. 29/2021 – Disposizioni in merito all'accreditamento per lo schema CMS, ai fini del rilascio di certificazioni ISO 37301: 2021**

INTRODUZIONE

La necessità di stare al passo con l'evolversi dello scenario normativo dei mercati globalizzati impone di adottare un approccio gestionale in riferimento alla *compliance*, in grado di rispondere all'esigenza di una efficace *governance* dei relativi rischi organizzativi.

A questa esigenza può rispondere lo *standard* ISO 37301:2021 per la certificazione dei sistemi di gestione per la *compliance*, capace di indirizzare le organizzazioni nell'adozione di un efficace complesso di misure organizzative, con l'obiettivo di governare i rischi aziendali in maniera integrata e permettere di fare dialogare le procedure ed i controlli, riferibili anche a sistemi normativi differenti, evitando sovrapposizioni e reciproche interferenze.

In un'ottica di *compliance* integrata, ci si attende che la norma ISO 37301 porti un beneficio anche alla gestione dei Modelli di Organizzazione e Gestione (MOG) ai sensi del D. Lgs. 231/2001.

In tale contesto, il mantenimento sotto controllo della *compliance* assume una connotazione positiva, non solo perché è alla base della conformità legale/legislativa, ma anche perché rappresenta un'opportunità, per la crescita sostenibile e duratura (successo durevole) dell'impresa.

Se incorporata in tutti i processi e nella cultura delle persone che lavorano nell'impresa, la *compliance* rappresenta uno strumento di successo per minimizzare il rischio di una violazione di legge e i relativi costi e danni alla reputazione, aumentando la fiducia delle parti interessate e proiettando l'impresa verso un successo sostenibile e al passo con i tempi.

CONTESTO NORMATIVO

L'ISO - International Standard Organization ha inserito la norma ISO 37301 in un contesto normativo molto interessante, una nuova *Road Map*, che propone alle imprese le basi oggettive su cui strutturare e implementare i sistemi di *Governance* (ISO 37000, norma prevista per settembre 2021), *Anti-Bribery* (ISO 37001:2016) *Compliance* (ISO 37301:2021) e *Whistleblowing* (ISO 37002, norma prevista per luglio 2021), integrando dunque i presidi di gestione della *compliance* con i presidi di governo aziendali tale da costituire un unico sistema.

In tale sistema (integrato), tutte le scelte strategiche e di *business*, di breve, medio e lungo periodo, saranno valutate, in funzione della loro appropriatezza, anche in termini di *compliance*.

La ISO 37301:2021 ha una struttura basata su HLS - *High Level Structure* e rappresenta l'evoluzione della Linea guida ISO 19600:2014, da sistema di gestione di tipo B, ossia non certificabile, a sistema di gestione di tipo A, certificabile.

Questo permetterà che i modelli di *compliance*, ad oggi prevalentemente affidati a *best practice* e linee guida proprietari, possano essere finalmente riferiti ad una norma internazionale, a fronte della quale sarà possibile conseguire una certificazione rilasciata da un organismo di terza parte.

ELEMENTI SPECIFICI DELLA NORMA

Nella norma il significato di "*compliance*" comprende il rispetto di molteplici disposizioni: requisiti di legge, regolamenti, specifiche e codici di condotta aziendali.

Il testo del documento, infatti, introduce alcuni nuovi termini e ne approfondisce la natura e il significato.

Il termine "*compliance*" può essere considerato quindi sotto diverse sfumature, ad esempio:

- *compliance obligations:* i requisiti di natura mandatoria, che un'organizzazione *deve* rispettare ma anche di natura volontaria, che un'organizzazione *sceglie* di rispettare;
- *compliance culture*: i valori, l'etica ed i comportamenti che permeano l'organizzazione;
- *conduct:* il comportamento o la violazione della *compliance*, che producono conseguenze su soggetti interni o esterni e anche sull'ambiente e contesto organizzativo, a scapito della sostenibilità.

Gli aspetti che la Norma propone alle imprese, come basi oggettive su cui strutturare e attuare il proprio sistema di gestione per la *compliance*, riguardano:

- *l'analisi del contesto*, per l'individuazione dei fattori interni ed esterni, con espresso riferimento alle esigenze e aspettative delle parti interessate rilevanti e al quadro di regolamenti e leggi di riferimento;
- *il campo di applicazione (scope) del sistema di gestione;*
- *la valutazione dei rischi* di *compliance*;
- *l'individuazione di ruoli, responsabilità e autorità per la gestione della compliance*, con specifici requisiti e attribuzione di compiti e poteri necessari per supervisionare e assicurare la conformità del sistema di e relazionare al *top management* sull'effettiva attuazione ed efficacia del sistema stesso;
- *l'adozione di una Compliance Policy*, che possa incoraggiare anche *the raising concerns,* ossia le segnalazioni di sospetti di violazioni e ritorsioni;

- la definizione e l'attuazione di controlli e procedure finalizzate ad assicurare il raggiungimento *degli obiettivi per la compliance* (incluse procedure di *raising concerns*/segnalazioni);
- *gli audit interni per il monitoraggio* sull'attuazione del sistema;
- *il riesame del governing body e del top management* circa l'idoneità, adeguatezza ed efficacia del sistema di gestione per raggiungere i propri obiettivi e conseguire il miglioramento continuo.

Processo di Certificazione

REGOLE DI CERTIFICAZIONE	
Norma di Certificazione	ISO 37301:2021
Soggetti che possono richiedere la certificazione	La certificazione ISO 37301 può essere richiesta da qualunque tipo di organizzazione, di qualsiasi dimensione, di natura pubblica o privata.
Possibili esclusioni	La certificazione viene rilasciata ad una sola entità giuridica o, con le precisazioni di seguito descritte, a "un gruppo di società", e deve considerare tutti i siti, filiali, sedi secondarie, attività e processi effettivamente svolti dall'organizzazione. E' possibile rilasciare una certificazione di "gruppo" che ricomprenda diverse entità giuridiche, ma solo in presenza di una struttura organizzativa "centralizzata" che gestisce e controlla la compliance per tutte le società del gruppo (si veda IAF MD01). Non sono ammesse esclusioni di processi/funzioni. Considerato però che la norma ISO 37301 suggerisce di adottare un approccio progressivo basato sul rischio degli obblighi di conformità applicabili all'organizzazione, è ammissibile che in prima istanza lo scopo di certificazione sia limitato ad affrontare i rischi di conformità più rilevanti (es. compliance penale). In questo caso l'ODC dovrà comunque richiedere evidenza all'organizzazione dell'identificazione degli obblighi di conformità cui sono associati i rischi più rilevanti con un programma di progressiva estensione dello scopo di certificazione a tutti gli altri, ove applicabile e pertinente. Salve espresse previsioni di legge, in nessun caso la certificazione sotto accreditamento dello standard ISO 37301 determina una presunzione di idoneità e/o di efficacia dei modelli o dei sistemi di controllo dei rischi di compliance adottati dall'organizzazione in forza di norme di legge (es. Modello di Organizzazione, gestione e controllo adottato ai sensi del D. Lgs 231/2001)

Criteri di competenza del Gruppo di verifica	Si rimanda alla ISO/IEC 17021-13 *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 13: Competence requirements for auditing and certification of compliance management systems* 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: • Notevole esperienza, significativa competenza e seniority di settore, maturata attraverso il coinvolgimento in posizioni di rilevante responsabilità nella gestione dei sistemi anticorruzione o di legal compliance o corporate crime (per esempio, S&O, D. Lgs. 231/2001, Legge 190/2012); • Conoscenza approfondita e documentata della normativa (legale, regolamentare e in materia di "buone prassi") applicabile al Paese in cui viene svolta l'attività aziendale e di business dell'organizzazione; • Formazione: Corso di 16 ore sulla norma ISO 37301, per chi ha già svolto un corso 40 ore sui sistemi di gestione. I primi due punti si considerano soddisfatti se per esempio la persona è certificata sotto accreditamento per schemi in tema di anti-bribery o D. Lgs. 231/2001 (es: *UNI 11753:2019 Attività professionali non regolamentate - Professionista della Conformità e Etica - Compliance and Ethics - operante nel settore bancario, finanziario e assicurativo-previdenziale*), oppure se esercita la professione di avvocato, commercialista o revisore, ex magistrato o giudice o funzionario di enti di autorità giudiziaria.
Criteri di competenza del decision maker e del contract reviewer	Si rimanda alla ISO/IEC 17021-13 *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 13: Competence requirements for auditing and certification of compliance management systems* Per le competenze del decision maker, si rimanda ai requisiti di formazione sulla ISO 37301 previsti al punto precedente.
Responsabilità dell'ODC	Una organizzazione certificata o in certificazione deve informare tempestivamente il proprio ODC nel caso in cui venisse coinvolta in qualche situazione critica tale da compromettere la garanzia della certificazione del sistema (esempio notizie di pubblico interesse che ledono la reputazione dell'impresa, o coinvolgimento in procedimento giudiziario per la violazione della compliance). Altrettanto l'organizzazione dovrà avvisare tempestivamente l'ODC di qualunque procedimento giudiziario in corso, e delle conseguenti azioni adottate per il contenimento degli effetti di tale evento, quindi dell'analisi delle cause radice e delle relative azioni correttive.

	L'informativa è dovuta anche se le vicende dovessero coinvolgere figure apicali per altri ambiti o siti/processi non certificati. 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, dovrà condurre tempestivamente delle valutazioni/approfondimenti specifici. 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 la Borsa). 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.
Tempi di audit	Si applicano i requisiti della ISO/IEC 17021-1. Si applica il documento IAF MD 05. Si applica la tabella per lo schema EMS, e per la scelta della tabella corretta tra quelle riportate deve essere valutato il livello di rischio in base a quanto segue: **Rischio alto** Se l'organizzazione richiedente la certificazione sia stata coinvolta negli ultimi 5 anni in indagini giudiziarie. Se l'Organizzazione è una multinazionale, che opera in contesti giuridici diversi. Se l'Organizzazione è identificata come "gruppo di società", ovvero "holding", ove vi sia una elevata complessità di "governance" e/o dove siano presenti diverse configurazioni, ancorché facenti capo a una gestione centralizzata, del Sistema di controllo interno e rischi. È possibile quindi rilasciare una certificazione di "gruppo" che ricomprenda diverse legal entities, ma solo in presenza di una struttura organizzativa "centralizzata" che gestisce e controlla la compliance per tutte le società del Gruppo (si veda IAF MD01). Le organizzazioni con 250 o più dipendenti oppure ogni organizzazione, anche con meno di 250 dipendenti, con un fatturato superiore a 50 milioni di euro e un bilancio superiore (valore patrimoniale netto) ai 43 milioni di euro.

	Sono in ogni caso da considerarsi a rischio alto: • le aziende di servizi finanziari; • le aziende che gestiscono servizi di pubblica utilità quali servizi di comunicazione elettronica, postali, di trasporto, di energia elettrica, di gas, di acqua; • le imprese che producono beni o erogano servizi soggetti ad accreditamenti, autorizzazioni o permessi dello Stato e di altre Autorità competenti; • le aziende del settore socio sanitario; • le Pubbliche Amministrazioni; • gli enti pubblici economici; • le società in controllo pubblico o partecipate dal pubblico; • le fondazioni e associazioni, riconosciute o meno; • gli enti del terzo settore (es. organizzazioni di volontariato, organismi per la cooperazione) e cooperative sociali. Se l'organizzazione che ricade nella categoria rischio alto ha una funzione interna di compliance e/o di internal audit, il livello di rischio è da classificarsi come medio. **Rischio medio** Se l'Organizzazione ricade nella categoria delle Piccole/medie imprese (PMI) che abbia tra 50 e 249 dipendenti e che non abbia una funzione strutturata di Compliance. **Rischio Basso** Se l'organizzazione non rientra nelle due precedenti categorie. **Rischio limitato** Non applicabile.
Modalità di svolgimento dell'audit	La documentazione di audit deve riportare, fra le altre registrazioni, anche quanto segue: ▪ il perimetro e l'applicabilità del Sistema di Gestione ISO 37301, con indicati i settori/aree con maggiore esposizione al rischio ▪ l'analisi di contesto; ▪ la mappatura dei processi (interni ed esterni) e l'elenco delle relative leggi, norme e regolamenti applicabili; ▪ le relazioni societarie con terzi e i riferimenti legislativi specifici; ▪ l'indicazione delle imprese terze e la relativa compliance, nonché le modalità di gestione; ▪ l'analisi degli episodi o minacce di violazione della compliance e le contromisure adottate;

	▪ le cause giudiziarie e i provvedimenti in cui è eventualmente coinvolta l'organizzazione.
Scopo del certificato	I criteri per la formulazione dello scopo del certificato sono gli stessi già applicati per la ISO 9001, con particolare attenzione al campo di applicazione del sistema di gestione. 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.), nel caso in cui queste rientrino nello scopo del certificato. Per chiarezza e trasparenza, in caso di esclusioni (es: certificazione limitata alla compliance penale), deve essere riportato nel certificato l'ambito che viene escluso dalla certificazione. Non è necessario riportare nel certificato il riferimento ai settori IAF.
Documenti IAF applicabili	Trovano applicazione tutti i documenti IAF relativi ai sistemi di gestione, fatto salvo quanto chiarito in precedenza sul documento IAF MD 05.

PROCESSO DI ACCREDITAMENTO

Le verifiche necessarie per il rilascio di certificazioni ISO 37301 devono essere condotte da organismi di certificazione accreditati secondo la norma UNI ISO/IEC 17021-1.

Il certificato di accreditamento è rilasciato senza alcuna limitazione settoriale.

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

Nel caso in cui l'ODC possegga già accreditamenti rilasciati da altri Enti di Accreditamento, dovrà essere effettuata una valutazione caso per caso, in base agli accordi EA / IAF MLA applicabili.

Rimangono invariati i prerequisiti previsti dal RG-01 e dal RG-01-03 per la concessione dell'accreditamento ed estensione, integrati dalle seguenti regole.

ITER DI ACCREDITAMENTO/ESTENSIONE		
A	L'ODC già accreditato in conformità alla ISO/IEC 17021-1:2015 per il rilascio di certificazioni ISO 9001 e ISO 37001	Esame documentale di 0,5 giornata (da svolgersi, almeno in parte, in remoto). 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	L'ODC già accreditato in conformità alla ISO/IEC 17021-1:2015 per il rilascio di certificazioni ISO 9001, ma NON per il rilascio di certificazioni ISO 37001	Esame documentale di 1 giornata (da svolgersi, almeno in parte, in remoto). 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	L'ODC NON accreditato in conformità alla ISO/IEC 17021-1:2015 ma già accreditato per altre norme di accreditamento	Esame documentale di 1 giornata (da svolgersi, almeno in parte, in remoto). Verifica ispettiva presso la sede dell'ODC di 2 Giornate + rapportazione 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.
D	L'ODC NON accreditato in conformità alla ISO/IEC 17021-1:2015 e non accreditato per altre norme di accreditamento	Esame documentale di 1 giornata (da svolgersi, almeno in parte, in remoto). Verifica ispettiva presso la sede dell'ODC di 4 Giornate + rapportazione 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

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.

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 o altre situazioni similari), verranno condotte le seguenti verifiche:

- se l'ODC ha emesso meno di 50 certificati nello schema di certificazione, il programma di mantenimento dell'accreditamento prevederà una verifica in accompagnamento e una verifica presso la sede dell'ODC;
- se l'ODC ha emesso tra 51 e 200 certificati nello schema di certificazione, il programma di mantenimento dell'accreditamento prevederà svolte 2 verifiche in accompagnamento e 1 verifica presso la sede dell'ODC.

L'occasione è gradita per porgere cordiali saluti.

Dott. Emanuele Riva

Direttore Dipartimento
Certificazione e Ispezione

Firmato digitalmente da: EMANUELE RIVA
Data: 07/07/2021 17:30:21