CIRCOLARE TECNICA Prot. DC2023OC038 **DATA** Milano, 26-04-2023

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 DCI

Loro sedi

OGGETTO **Dipartimento Certificazione e Ispezione**

Circolare tecnica DC N° 22/2023 - Disposizioni in merito all'accreditamento per lo schema CMS - Compliance Management System, ai fini del rilascio di certificazioni UNI ISO 37301:2021 Compliance management systems — Requirements with guidance for use.

La presente annulla e sostituisce la precedente Circolare Tecnica DC N. 29/2021 del 07-07-2021.

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* UNI 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 UNI ISO 37301 porti un beneficio anche alla gestione dei Modelli di Organizzazione e Gestione (MOG) ai sensi del DLgs. 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 contribuendo a proiettare l'impresa verso un successo sostenibile e al passo con i tempi.

CONTESTO NORMATIVO

L'ISO - International Standard Organization ha inserito la norma UNI 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 37000:2021), *Anti-Bribery* (ISO 37001:2016) *Compliance* (UNI ISO 37301:2021) e *Whistleblowing* (ISO 37002), 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 UNI 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: c*omportamenti o prassi che impattano sugli esiti della *compliance* e hanno conseguenze sui clienti, collaboratori, fornitori, mercati e comunità.

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 e l'efficacia del sistema di gestione per raggiungere i propri obiettivi e conseguire il miglioramento continuo.

REGOLE DI CERTIFICAZIONE

Norma di Certificazione	UNI ISO 37301:2021
Soggetti che possono richiedere la certificazione	La certificazione UNI ISO 37301 può essere richiesta da qualunque tipo di organizzazione, di qualsiasi dimensione, di natura pubblica o privata.
Esclusioni di siti	Non sono ammesse esclusioni di siti.
Approccio per processi	Alla luce del fatto che la norma UNI ISO 37301 suggerisce di adottare un approccio progressivo, basato sul rischio degli obblighi di compliance applicabili all'organizzazione, è ammissibile che in prima istanza lo scopo di certificazione sia limitato ai processi aziendali coinvolti nella gestione dei rischi di compliance più rilevanti. Tali rischi e processi dovranno essere individuati dall'organizzazione attraverso la valutazione "compliance risk assessment" (rif. UNI ISO 37031 par. 4.6). Attraverso la valutazione l'organizzazione dovrà dimostrare all'OdC di avere: 1. individuato i rischi e le minacce legati alla mancata compliance e i processi aziendali maggiormente coinvolti; 2. analizzato in che misura potranno verificarsi e quali effetti potranno avere sui processi aziendali tali rischi e minacce; 3. stabilito per ciascun rischio la relativa "rilevanza" e stabilito/i il processo/i processi maggiormente coinvolti da tale rischio; 4. definito il campo di applicazione della certificazione. Nel caso in cui l'organizzazione richieda, sulla base del compliance risk assessment, di intraprendere un percorso progressivo di certificazione, dovrà presentare all'OdC il programma di estensione dello scopo di certificazione ai processi aziendali al fine di raggiungere la completa copertura degli ambiti di compliance. Nell'ambito del/i processo/i individuati, l'organizzazione dovrà però obbligatoriamente includere "tutti" gli ambiti di compliance (es. privacy e protezione dei dati, safety, antiriciclaggio, responsabilità amministrativa, security a altri) attinenti a quel processo. Eventuali elementi di rischio legati a specifici ambiti di compliance all'interno del processo oggetto di certificazione avranno quindi un impatto nell'ambito dei controlli messi in atto per la loro mitigazione. Tale programma di estensione progressiva e per processi della certificazione dovrà essere validato dall'OdC. Nel caso in cui si presentano le suddette situazioni di progressiva estensione, le attività di comunicazione, relative alla certificazione conseguita, dovranno chiarire l'ambito certificato.

	Salve espresse previsioni di legge, in nessun caso la certificazione sotto accreditamento dello standard UNI 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	I requisiti di competenza sono definiti nello standard UNI CEI ISO/IEC TS 17021-13: Valutazione della conformità — Requisiti per gli Organismi che forniscono audit e certificazione di sistemi di gestione – Parte 13: Requisiti di competenza per le attività di audit e di certificazione dei sistemi di gestione per la compliance. I requisiti di competenza del gruppo di verifica si ritengono soddisfatti se è possibile dimostrare che, nel complesso, le competenze e le abilità definite ai par. 5.1 fino a 5.4 dello standard UNI CEI ISO/IEC TS 17021-13 sono soddisfatte. I suddetti requisiti si considerano soddisfatti se, per esempio, nel gruppo di audit sono presenti le seguenti esperienze/competenze: • esperienza di audit in ambito anti-bribery o governance delle organizzazioni (almeno 3 anni di esperienza) e la partecipazione al corso di formazione di 16 ore sulla norma UNI ISO 37301, avendo già svolto un corso 40 ore sui sistemi di gestione; • esperienza maturata in ruoli di rilevante responsabilità nella gestione dei sistemi anticorruzione ovvero di legal compliance o corporate crime (per esempio, S&O, d.lgs. 231/2001, Legge 190/2012), ovvero esperienza nell'ambito dei modelli organizzativi ai sensi del d.lgs. 231/2001, ovvero dall'esercizio della professione di avvocato, commercialista o revisore, ex magistrato o giudice o funzionario di enti di autorità giudiziaria con comprovata esperienza in ambito compliance. Al fine di soddisfare i suddetti requisiti, nel caso in cui nel gruppo di audit non siano presenti tutte le competenze richieste, è possibile incaricare uno o più esperti. L'esperto incaricato deve anche dimostrare la conoscenza dello standard UNI ISO 37301.
Criteri di competenza del decision maker e del contract reviewer	I requisiti di competenza sono definiti nello standard UNI CEI ISO/IEC TS 17021-13. Il personale che conduce il riesame della domanda per determinare la competenza richiesta al gruppo di audit, per selezionare i membri del gruppo di audit e per determinare la durata dell'audit (contract reviewer) e quello che riesamina i rapporti di audit e che prende decisioni sulle certificazioni (decision maker) deve avere la competenza definite ai par. 6.1 e 6.2 della norma UNI CEI ISO/IEC TS 17021-13. I suddetti requisiti si considerano soddisfatti se il decision maker e il contract reviewer possono dimostrare di essere Team Leader per i sistemi di gestione UNI ISO 9001 o per i sistemi di gestione UNI ISO 37001 e di avere partecipato ad un corso sulla norma UNI ISO 37301.

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. 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). Al termine dell'analisi, l'OdC potrà adottare i 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	I tempi di audit si determinano, definita la categoria di complessità e il numero di addetti, attraverso l'annex B – EMS del documento IAF MD 05. <u>Categoria di complessità aziendale</u> Rientrano nella **categoria di complessità alta**: ▪ le organizzazioni coinvolte negli ultimi 5 anni in indagini giudiziarie; ▪ le organizzazioni che abbiano avuto nell'ultimo anno uno o più infortuni con prognosi superiore ai 40 giorni; ▪ le multinazionali, che operano in molteplici contesti giuridici; ▪ le organizzazioni "gruppo", ovvero "holding", ove vi sia una elevata complessità di "governance" e/o dove siano presenti diverse configurazioni, indipendenti o meno, del Sistema di controllo interno e dei rischi. In questo caso è inoltre possibile 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; ▪ 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. Se l'organizzazione ricadente nella categoria rischio alto ha una funzione interna di compliance e/o di internal audit ovvero ha attuato un Modello di Organizzazione Gestione e Controllo ex-D. Lgs.231/2001, il livello di rischio è da classificarsi come medio. Rientrano nella **categoria di complessità media** le piccole/Medie Imprese (PMI) con un numero di dipendenti compreso tra 50 e 249 e le organizzazioni che non hanno una funzione strutturata di Compliance. Rientrano nella categoria di **complessità bassa le organizzazioni che non rientrano nelle due precedenti categorie**. <u>Numero di addetti</u> Considerata la specificità del Sistema di gestione, che riguarda principalmente i processi di "Governance/Legal", ai fini del calcolo degli addetti (o FTE- Full Time Equivalent), occorre considerare le funzioni aziendali coinvolte direttamente nell'attuazione del Sistema di gestione con il seguente contributo: • contributo al 100% degli addetti facenti parte dei processi di governance aziendale (CdA, Ufficio Legale, uffici coinvolti nelle attività di compliance); • contributo al 100% degli addetti coinvolti nel processo/i a cui si applica il sistema di gestione della compliance certificato (o da certificare); • contributo al 10% per altri addetti facenti parte di altri uffici e/o dell'aree di produzione/servizi aziendali. Ad esempio, nel caso l'azienda volesse limitare il campo d'applicazione al processo "HR" si considererebbero al 100% le funzioni di governance, al 100% gli addetti dei processi/uffici/reparti e siti coinvolti nel processo compliance HR da certificare e al 10% gli addetti facenti parte di altri uffici e/o dell'aree di produzione/servizi aziendali. Nella definizione degli addetti è incluso il personale che offre all'impresa servizi di consulenza/collaborazione e il personale che offre servizi in outsourcing, riferiti o che influenzano il Sistema di gestione sulla Compliance. Si ricorda che il tempo di audit dei sistemi di gestione, determinato utilizzando le tabelle del documento IAF MD 05, non comprende il tempo degli auditor in training, degli osservatori o degli esperti tecnici (rif. par. 3.8 - IAF MD 05:2019).
Valutazione di organizzazioni multi-site	Ai fini della valutazione di una organizzazione multi-site è applicabile il documento IAF MD 01, sia per il metodo di calcolo del numero di addetti sia per il metodo di campionamento dei siti/legal entities.

	Si ricorda che la definizione di organizzazione multi-site (rif. par. 3.3 IAF MD 01) comprende sia le organizzazioni con stessa entità giuridica, sia organizzazioni con diverse entità giuridiche (in questo caso rientra la definizione di Gruppo), purché abbiano un legame contrattuale con la funzione centrale dell'organizzazione e il sistema di gestione multi-site sia unico e caratterizzato da una struttura centralizzata diretta dalla sede principale (holding) che gestisce e controlla la compliance di tutti i siti o legal entities. La definizione e l'allocazione dei tempi dedicati ai diversi siti e legal entities restano a capo dell'Organismo di Certificazione che dovrà pianificare audit di compliance efficaci e efficienti.
Modalità di svolgimento dell'audit	La documentazione di audit, deve riportare, fra le altre registrazioni, anche quanto segue: • il documento di valutazione del rischio "compliance risk assessment" definito dall'organizzazione in conformità a quanto richiesto dalla norma UNI ISO 37301 al par. 4.6; • il perimetro entro cui è applicato il Sistema di gestione per la compliance, indicando i processi i siti e gli uffici convolti; • il programma di estensione della certificazione a tutti i processi i siti e gli uffici aziendali coinvolti (ove applicabile); • 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 registrazioni riguardanti le modalità di gestione delle cause giudiziarie e dei provvedimenti in cui è coinvolta l'organizzazione e, ove applicabile, le evidenze del coinvolgimento e dell'intervento dell'Organismo di Vigilanza (secondo il D.Lgs. 231).
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, e altro), nel caso in cui queste rientrino nello scopo del certificato. Per chiarezza e trasparenza, nel certificato dovranno essere elencati i siti/uffici ricadenti nel perimetro della 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.

REGOLE PER L'ACCREDITAMENTO/ESTENSIONE

Norma di Accreditamento: UNI ISO/IEC 17021-1:2015

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 ed RG-01-03 per la concessione dell'accreditamento ed estensione, integrati dalle seguenti regole.

A	OdC già accreditato in conformità alla UNI 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	OdC già accreditato in conformità alla UNI ISO/IEC 17021-1:2015 per il rilascio di certificazioni ISO 9001, ma NON per il rilascio di certificazioni UNI 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	OdC NON accreditato in conformità alla UNI 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	OdC NON accreditato in conformità alla UNI ISO/IEC 17021-1:2015 e non accreditato per altre norme di accreditamento	• 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

- Procedura per la selezione la qualifica e il monitoraggio degli auditor, dei decision maker e dei e del contract reviewer.
- Curricula degli auditor, dei decision maker con la giustificazione della singola qualifica tramite ad es. scheda di qualifica.
- Linea guida o istruzione predisposta dall'OdC per i gruppi di audit.
- Regolamento di certificazione che contempli le condizioni contrattuali ai fini del rilascio e mantenimento della certificazione sotto accreditamento (compresi gli obblighi definiti dalla presente circolare).
- Procedure tecnico commerciali per la definizione della durata degli audit, il campionamento dei siti, la definizione dell'offerta commerciale.
- Facsimile del certificato rilasciato dall'OdC.
- Lista dei certificati già emessi, e delle prossime attività di verifica (dato necessario per poi pianificare la verifica in accompagnamento).
- Per gli OdC NON accreditati UNI 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 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
Limitazioni d'uso: Explicit Text: Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity
Data: 26/04/2023 17:40:00