ARTICOLO **Novembre 2023**

COMPLIANCE E CONFORMITÀ: LA SFIDA DELLE ORGANIZZAZIONI

Emanuele Riva – Vice Direttore Generale e Direttore Dipartimento Certificazione e Ispezione Accredia

Il concetto di compliance è diventato sempre più importante per le Organizzazioni che ambiscono a un successo sostenibile nel lungo periodo. Tuttavia, la differenza tra conformità e compliance non è sempre chiara, e ciò può generare incertezze e confusioni. In questo articolo, analizzeremo il significato di questi due concetti ed il loro rapporto con il processo di certificazione, fornendo alcune riflessioni utili alle organizzazioni che desiderano sviluppare una cultura della compliance.

INTRODUZIONE

Le Organizzazioni moderne devono affrontare una sfida importante: quella di mantenere una cultura della compliance e della conformità alle normative, ai requisiti regolamentari e contrattuali, ai codici di settore e alle specifiche organizzative. È utile quindi riflettere sui concetti di compliance e conformità, evidenziando le differenze tra i due termini e il loro utilizzo all'interno delle Organizzazioni.

DIFFERENZA LESSICALE TRA I TERMINI *CONFORMITY* E *COMPLIANCE*

Secondo la Treccani, il termine compliance deriva dal latino "*complere*", ovvero "compiere". Nel linguaggio medico, la compliance sarebbe il grado di collaborazione che il paziente presta nel seguire le prescrizioni del medico curante. In ambito aziendale, il concetto di compliance si basa sulla capacità dell'Organizzazione di definire *ex ante* la condotta di azione da seguire ed i criteri con cui le singole azioni verranno valutate; realizzando controlli operativi capaci di limitare i relativi rischi e le verifiche in grado di evidenziare il grado di compliance/"conformità" del proprio Sistema.

Nel mondo delle Organizzazioni, il termine ha assunto quindi un significato più ampio, che comprende non solo la conformità alle norme di legge, ma anche quelle di natura etica, sociale e ambientale. La conformità, invece, indica semplicemente il rispetto delle norme volontarie e delle relative disposizioni attuative. La differenza tra i due concetti è stata in effetti introdotta ufficialmente nel 2006, con la norma UNI EN ISO 17021:2006, che ha introdotto il concetto di compliance chiarendone la differenza rispetto alla conformità, con riferimento alla certificazione dei sistemi di gestione.

Mentre la conformità si riferisce quindi alla capacità dell'Organizzazione di rispettare i requisiti normativi (standard volontari), la compliance implica il rispetto delle prescrizioni cui un'Organizzazione deve conformarsi, indipendentemente dalla loro natura (standard volontari, cogenti e regolamenti interni). La compliance si basa sulla capacità dell'Organizzazione di definire ex ante la condotta di azione da seguire ed i criteri con cui le singole azioni verranno valutate; realizzando controlli operativi capaci di limitare i relativi rischi e le verifiche in grado di evidenziare il grado di compliance/"conformità" del proprio Sistema.

La compliance, quindi, non si limita al rispetto delle prescrizioni legali, ma si estende a tutte le prescrizioni cui un'Organizzazione deve conformarsi. Tuttavia, non esiste una traduzione univoca del termine compliance in italiano.

Inoltre, il concetto di *conformity* è strettamente legato al processo di certificazione, ovvero la verifica da parte di un Ente terzo indipendente che l'Organizzazione rispetti i requisiti stabiliti dalle norme e dai regolamenti applicabili. Tuttavia, la distinzione tra *conformity* audit e compliance audit non è sempre chiara.

Ci viene in aiuto, la normativa che ha introdotto il concetto di responsabilità amministrativa dell'Ente per gli illeciti dipendenti da reato (D.Lgs. 8 giugno 2001, n. 231), perché ha rivoluzionato il panorama giuridico, creando un nuovo tipo di responsabilità d'impresa, dalla quale si può essere esenti soltanto definendo un modello organizzativo idoneo a prevenire i reati riconducibili alla specifica attività dell'impresa stessa. In altri termini, si potrebbe dire che una Organizzazione che rispetta la ISO 37001 è conforme, mentre se rispetta il D.Lgs. 231 è in compliance.

Si ricorda che la UNI ISO 37301:2021 che fornisce alle Organizzazioni lo strumento di governance per individuare sistemi di controllo per raggiungere la conformità. Tuttavia, la UNI ISO 37301:2021 non sostituisce altre norme, come la ISO 9001, ma si integra con esse per allargare lo scopo della ISO 9001 in modo flessibile e personalizzato. In sintesi, la compliance rappresenta un concetto fondamentale per le Organizzazioni che ambiscono ad avere successo nel lungo periodo. Tuttavia, è importante che le Organizzazioni comprendano la differenza tra conformità e compliance e adottino un approccio chiaro e coerente alla cultura della compliance. Solo in questo modo, le Organizzazioni potranno dimostrare il proprio impegno a conformarsi alle leggi, ai requisiti regolamentari e contrattuali, ai codici di settore e alle specifiche organizzative e garantire il proprio successo e la propria sostenibilità nel tempo.

DIFFERENZA OPERATIVA TRA I TERMINI *CONFORMITY* E *COMPLIANCE*

Le Organizzazioni che ambiscono ad avere successo nel lungo periodo devono stabilire e mantenere una cultura della compliance, che consideri non solo le esigenze e le aspettative delle Parti interessate, ma anche quelle cogenti su tutte. La compliance deve essere incorporata nella cultura dell'Organizzazione e nei comportamenti e attitudini delle persone che lavorano al suo interno. Un Sistema di Gestione per la compliance efficace rappresenta non solo la base, ma anche un'opportunità per un'Organizzazione di successo e sostenibile, per dimostrare il proprio impegno a conformarsi a leggi, requisiti regolamentari e contrattuali, codici di settore e specifiche organizzative. Tuttavia, la gestione dei sistemi di certificazione rappresenta una sfida per le Organizzazioni, che devono affrontare non solo i requisiti normativi, ma anche quelli etici e sociali.

Negli ultimi decenni, il concetto di compliance ha assunto sempre maggiore importanza nell'ambito delle Organizzazioni, in particolare in relazione alle leggi, ai requisiti regolamentari e contrattuali, ai codici di settore e alle specifiche organizzative. Proviamo allora a farci delle ulteriori domande, per uscire dal mero esercizio linguistico e capire se dietro i due termini esiste una differenza oltre che lessicale anche operativa.

Per esempio, l'approccio alla verifica cambia se valuto un requisito cui l'azienda ha dichiarato la *conformity* oppure la compliance?

Che differenza c'è tra compliance audit / *conformity* audit. E legal compliance?

Cosa cambia nei due casi? Il metodo d'indagine? La responsabilità dell'Ispettore? La responsabilità dell'Azienda? Il campionamento? Le registrazioni? Ed ancora. Un certificato a fronte della norma UNI ISO 37301:2021 è un certificato di *conformity* o di compliance? Oppure è di legal compliance?

E per continuare, che relazioni ci sono tra norme cogenti italiane e standard volontari?

- D.Lgs. n. 231/20021 – UNI ISO 37301:2021;
- Legge anticorruzione n. 3/19 - ISO 37101;
- Decreto n. 81 - ISO 45001;

Dobbiamo verificare il rispetto di uno standard (i.e. "conformity"), o il rispetto di una legge (i.e. "legal compliance")?

Forse, al momento attuale non abbiamo tutte le risposte.

Quello che è certo, è che un Sistema certificabile deve essere un Sistema reale, non un castello di carte (certificazione e non *cartificazione*). Quando ciò si verifica, vuol dire che l'avere adottato il Modello proposto dalla UNI ISO 37301:2021 come strumento per la gestione della compliance aziendale non ci si è limitati al solo "Compiere il proprio dovere", ma al "Compiere il proprio dovere con consapevolezza e competenza"!

Un Modello a norma 231 deve essere adottato ed efficacemente attuato per avere efficacia esimente della responsabilità amministrativa. L'efficacia esimente non dipende dalla certificazione UNI ISO 37301:2021 del Sistema ma dalla serietà / efficacia con la quale il Sistema è stato concepito e applicato. La certificazione UNI ISO 37301:2021 è una conseguenza, non il fine ultimo.

CONCLUSIONI

Lo schema di certificazione UNI ISO 37301:2021 è complesso. Molto.

Pertanto, è utile riflettere se non occorra prevedere un tempo di audit aggiuntivo rispetto alle altre certificazioni, da stabilire a seconda del tipo e complessità dell'organizzazione.

Basta quanto indicato dalla tabella EMS dello IAF MD 05? Forse sarebbe utile partire da 1 giorno in più di stage 2?

Ci sono poi situazioni specifiche che potrebbero essere disciplinate.

È possibile cambiare il team di audit tra lo stage 1 e lo stage 2 senza incrementare il tempo di audit? Inoltre, al manifestarsi di situazioni di Stage 1 molto deficitarie, quanto tempo dovrebbe essere concesso all'azienda per procedere con lo Stage 2? Dopo quanto tempo è possibile certificare un Sistema di Gestione da quando il Sistema è stato avviato? Sei mesi minimo?

La qualifica in questo schema, anche per gli Esperti Tecnici (che siano Avvocati e non altro!) dovrebbe prevedere che gli stessi siano esperti almeno di normativa 231. Diversamente non avrebbero gli strumenti per rilevare alcune criticità.

Un buon "Sistema di Compliance" dovrebbe essere a coronamento di un approccio maturo di gestione dei rischi che possono compromettere l'integrità dei comportamenti. Quando si usa il termine "integrità" si fa naturalmente riferimento alla comprensione del proprio ruolo nella società, con riferimento a tutte le Parti Interessate e alla comprensione del contesto normativo cogente e volontario. Giacché sottoscrivere un contratto presuppone l'assunzione di doveri specifici e generali (devo fare una macchinetta per il caffè che dia un caffè buono, ma anche che sia sicura!). Quindi, Compliance viaggia assieme ad Integrità a conoscenza dei Rischi ed allo sviluppo di un Sistema di Controllo Interno per la loro mitigazione. Ciò, unito alla definizione delle relative regole e delle logiche di reporting significa "governance". Analizziamo le tre linee di controllo, tipiche delle Società più strutturate:

1. i processi operativi sono supportati dalla Funzione di compliance, che aiuta la progettazione dei processi (i.e. i Senior Manager ed i Process Owner) a tener conto delle regole sopra illustrate. Questo è il motivo per cui chi, in azienda, svolge il ruolo di Compliance Manager, deve poter disporre di autonomia gestionale reale, e di autorevolezza di primo livello;

2. il Risk Management che svolge il lavoro di analisi approfondita della conoscenza dei processi, per trovarne i punti deboli, e l'individuazione dei controlli operativi;

3. l'Internal Audit che garantisce, in modo del tutto indipendente, che tutto ciò funzioni correttamente; ed anche che la governance (come sopra indicata) sia fatta funzionare.

"Compliance" è una faccia di una medaglia. La seconda faccia si chiama cultura dell'integrità. Ed il risultato di questo processo, sono la fiducia e la reputazione.

Accredia *è l'Ente unico nazionale di accreditamento designato dal Governo italiano. Il suo compito è attestare la competenza dei laboratori e degli organismi che verificano la conformità di prodotti, servizi e professionisti agli standard di riferimento, facilitandone la circolazione a livello internazionale.*

Accredia è un'associazione privata senza scopo di lucro che opera sotto la vigilanza del Ministero delle Imprese e del Made in Italy e svolge un'attività di interesse pubblico, a garanzia delle istituzioni, delle imprese e dei consumatori.

Accredia ha 69 soci che rappresentano tutte le parti interessate alle attività di accreditamento e certificazione, tra cui 9 Ministeri (Imprese e Made in Italy, Ambiente e Sicurezza Energetica, Difesa, Interno, Infrastrutture e Trasporti, Università e Ricerca, Lavoro e Politiche Sociali, Agricoltura, Sovranità Alimentare e Foreste, Salute), 7 Enti pubblici di rilievo nazionale, i 2 Enti di normazione nazionali, UNI e CEI, 13 organizzazioni imprenditoriali e del lavoro, le associazioni degli organismi di certificazione e ispezione e dei laboratori di prova e taratura accreditati, le associazioni dei consulenti e dei consumatori e le imprese fornitrici di servizi di pubblica utilità come Ferrovie dello Stato ed Enel.

L'Ente è membro dei network comunitari e internazionali di accreditamento ed è firmatario dei relativi Accordi di mutuo riconoscimento, in virtù dei quali le prove di laboratorio e le certificazioni degli organismi accreditati da Accredia sono riconosciute e accettate in Europa e nel mondo.

L'articolo "Compliance e conformità: la sfida delle organizzazioni" di Emanuele Riva è stato pubblicato sulla rivista Qualità di Aicq (Ed. 5/2023 – pagg. 42-45).