

DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

ISO 37301 e compliance integrata

Governance, controlli e creazione di valore

Novembre 2026

Antonio Di Giorgio, Partner, Annunziata&Conso
Leonardo Limiti, Responsabile Compliance&Anticorruption, Mooney Group





Antonio Di Giorgio, Partner, Annunziata&Conso

Leonardo Limiti, Responsabile Compliance&Anticorruption, Mooney Group*

Antonio Di Giorgio

Antonio Di Giorgio è avvocato dal 2014 ed è tirocinante revisore legale dei conti. Le principali aree di specializzazione riguardano la consulenza legale e regolamentare in materia di diritto societario, bancario, assicurativo e dei mercati finanziari, con particolare riferimento al settore dei servizi di pagamento, all'emissione di moneta elettronica e all'ambito fintech.

* Le opinioni espresse in questo articolo sono strettamente personali e non riflettono necessariamente il punto di vista dell'organizzazione/azienda di appartenenza.

1. Premessa

Negli ultimi anni, la crescente complessità del quadro normativo e regolamentare, unitamente all'evoluzione dei modelli di business e delle strutture organizzative, ha progressivamente rafforzato il ruolo della compliance nei sistemi di governo e controllo delle organizzazioni (i.e. imprese, enti, etc.). Da funzione tradizionalmente orientata alla verifica del rispetto delle disposizioni applicabili, la compliance ha assunto una rilevanza sempre maggiore nei processi decisionali e nella definizione delle strategie aziendali, contribuendo alla prevenzione dei rischi e alla creazione di valore nel lungo periodo.

In tale contesto si inserisce la norma UNI ISO 37301[1], che definisce i requisiti per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo di un sistema di gestione per la compliance (di seguito anche l'"SGC"). La norma, applicabile – per scelta dell'organizzazione - a operatori di qualsiasi natura e dimensione (i.e. al settore industriale e finanziario[2]), introduce un modello organizzativo, fondato sull'integrazione degli obblighi di compliance nei processi aziendali, sulla responsabilizzazione degli Organi aziendali e del *management* (alta direzione) e sulla valutazione continua dell'efficacia dei presidi adottati.

Il presente contributo esamina il ruolo della ISO 37301 nell'evoluzione della compliance da presidio di conformità a componente della governance, per la creazione di valore, soffermandosi sui principi dell'integrazione, sulle responsabilità degli Organi aziendali, sulle modalità di gestione e valutazione dei rischi. L'analisi considera, inoltre, le possibili sinergie con i modelli organizzativi sviluppati nel settore finanziario e le opportunità di applicazione dello *standard* ISO anche alle imprese non vigilate.

2. La ISO 37301: un sistema di gestione integrato della compliance per le organizzazioni

La ISO 37301 è uno *standard* internazionale per l'SGC, applicabile a organizzazioni di diversa dimensione e natura. Il suo oggetto è il sistema attraverso cui l'organizzazione governa la conformità. La norma

1 Si tratta della norma UNI ISO 37301:2021+A1 di ottobre 2024. L'aggiornamento del 2024 è relativo alla considerazione del cambiamento climatico nell'analisi del contesto e delle parti interessate.

2 L'organizzazione è intesa come società, gruppi, aziende, imprese e singoli operatori, cfr. par. 3.1, norma UNI ISO 37301:2021.

vedi l'articolo online

offre una base comune per strutturare e migliorare tale sistema e, a differenza della precedente ISO 19600[3], contiene requisiti verificabili per ottenere una certificazione[4].

La norma ISO introduce una nozione ampia di "conformità": il SGC considera sia gli obblighi normativi direttamente applicabili, sia gli impegni a cui la stessa organizzazione sceglie di aderire. In questa prospettiva, quindi, anche la coerenza tra codici di condotta adottati e comportamenti effettivi dell'organizzazione entra nella valutazione della qualità del governo aziendale (cfr. il par. 4 per approfondire).

Inoltre, secondo le FAQ del comitato ISO[5], il sistema di gestione della compliance comprende l'identificazione degli obblighi e la valutazione dei rischi, le responsabilità della *leadership*, gli obiettivi, la formazione, il monitoraggio, le verifiche e le azioni correttive. Il SGC deve essere mantenuto e migliorato attraverso la valutazione periodica della sua efficacia e il riesame da parte degli Organi aziendali.

Aderendo alla norma ISO, pertanto, l'organizzazione è chiamata a rendere verificabili da un certificatore accreditato le proprie scelte organizzative ed a garantire nel tempo il funzionamento dell'SGC. La certificazione ISO, tuttavia, non attribuisce lo status di "intermediario vigilato" all'organizzazione, non sostituisce gli adempimenti di settore e non attesta l'osservanza di tutte le prescrizioni prudenziali o di condotta. Occorre inoltre considerare il perimetro certificato: il SGC può riguardare l'intera organizzazione oppure soltanto determinate attività della stessa.

La scelta di adottare la ISO 37301 è normalmente volontaria per l'organizzazione, salvo specifici obblighi applicabili, anche contrattuali (es. la richiesta di un cliente o della controparte). Una volta intrapreso il percorso, ottenere e mantenere la certificazione richiede di dimostrare la conformità del sistema ai requisiti dichiarati. Per un'impresa già dotata di presidi specialistici, il percorso dovrebbe quindi partire dall'analisi di ciò che esiste: responsabilità, controlli, sistemi di gestione e informazioni disponibili; su questa base, poi, è possibile individuare le lacune e costruire i raccordi necessari rispetto ai requisiti della ISO.

3. La compliance diventa una componente del governo aziendale

Ogni organizzazione prende decisioni entro un insieme di regole che ne condiziona prodotti, rapporti commerciali, organizzazione e possibilità di sviluppo. La capacità di comprendere queste regole e di incorporarle nei processi incide sulla qualità della gestione dell'organizzazione. Una strategia aziendale fondata su pratiche commerciali scorrette, controlli inadeguati o impegni non sostenibili può generare risultati economici immediati, ma può esporre l'organizzazione a costi futuri che ne potrebbero compromettere la stabilità.

In questa prospettiva, attribuire alla compliance un ruolo nella governance dell'organizzazione può migliorare la qualità e la durata del valore prodotto o del servizio offerto.

La ISO 37301 non identifica, tuttavia, la compliance esclusivamente con una funzione aziendale, ma con un sistema di responsabilità distribuite nell'intera organizzazione. Gli Organi aziendali devono poter conoscere le esposizioni a rischi rilevanti dell'organizzazione, comprendere le conseguenze delle alternative disponibili e verificare che le misure deliberate siano attuate e rese effettive. In tale ambito, la funzione di compliance, istituita a livello di organizzazione, può contribuire a rendere disponibili tali informazioni, interpretare le implicazioni delle norme e segnalare le condizioni necessarie per operare nel rispetto della normativa applicabile (interna ed esterna all'organizzazione). La responsabilità delle scelte e dell'esecuzione, comunque, resta in capo agli organi competenti[6].

3 La ISO 37301:2021 ha sostituito la precedente ISO 19600:2014, segnando il passaggio da uno *standard* contenente linee guida a una norma che stabilisce requisiti verificabili per i sistemi di gestione della compliance. Tale evoluzione consente di sottoporre il SGC a una valutazione di conformità da parte di un organismo di certificazione, ferma restando la natura volontaria dell'adozione dello standard, salvo specifici obblighi applicabili.

4 Accredia è l'Ente Italiano di Accreditamento ed è l'unico organismo nazionale designato dallo Stato per attestare la competenza, l'imparzialità e l'indipendenza degli organismi di valutazione della conformità. Tale Ente ha aperto nell'ottobre 2021 i processi per concedere l'accreditamento agli Organismi di Certificazione interessati a rilasciare certificazioni ufficiali a fronte della norma UNI ISO 37301 (cfr. anche Accredia, Compliance con la nuova ISO 37301 parte la certificazione sotto accreditamento, 20 ottobre 2021).

5 Si vedano al seguente link le FAQs qui richiamate: https://committee.iso.org/files/live/sites/tc309/files/FAQ%2037301/ISO%2037301%20FAQs%2C%20May%202022.pdf.

6 Cfr. UNI ISO 37301:2021+A1:2024, punti 5.1.3 e 5.3.1. La norma attribuisce specifica rilevanza alla governance della compliance, richiedendo che siano assicurati l'indipendenza della funzione, il suo accesso diretto all'organismo di governo e l'attribuzione di autorità e competenze appropriate. Lo standard distingue inoltre le responsabilità dell'organismo di governo e dell'alta direzione, valorizzando il ruolo di supervisione del primo e quello di attuazione e gestione operativa della seconda.

vedi l'articolo online

La compliance come un sistema di responsabilità distribuite nell'organizzazione trova ulteriore espressione nel principio della cultura della compliance, cui la ISO 37301 attribuisce autonoma rilevanza (cfr. punto 5.1.2 della norma ISO). L'efficacia dell'SGC non dipende, infatti, soltanto dalla istituzione della funzione di compliance e dalla definizione di regole e controlli, ma anche dalla loro effettiva incorporazione nei comportamenti delle persone, in tutte le aree di business e nelle decisioni aziendali dell'Alta direzione. In questa prospettiva, il coinvolgimento degli Organi aziendali e dell'alta dirigenza assume un ruolo determinante nella promozione di valori condivisi, nella diffusione della consapevolezza dei rischi e nell'adozione di comportamenti coerenti con gli obblighi di compliance[7].

4. Cosa significa integrare gli obblighi di compliance nell'organizzazione

Un elemento qualificante della ISO 37301, a cui si è fatto cenno, è rappresentato dall'ampiezza della nozione di obblighi di compliance, che comprende non soltanto le disposizioni legislative e regolamentari applicabili, ma anche gli impegni ai quali l'organizzazione abbia scelto volontariamente di conformarsi: i codici di condotta, *standard* di settore, specifici impegni contrattuali, etc..

La norma richiede che l'organizzazione sia in grado di identificare, documentare e aggiornare tali obblighi, valutandone l'impatto sulle attività, sui prodotti e sui servizi. Il SGC assume così una funzione di raccordo tra fonti eterogenee di obblighi e responsabilità aziendali, favorendo una visione unitaria dei rischi di non conformità[8] [9].

7 È significativo che la Banca di Italia, in un intervento del novembre 2025 sull'evoluzione della funzione di compliance, abbia richiamato il contributo della conformità alla competitività e alla creazione di valore nel lungo periodo, sottolineandone il coinvolgimento preventivo nelle decisioni e la necessità di un governo unitario dei rischi (cfr. Giuseppe Siani, L'attività di compliance. Evoluzione della funzione e appunti di vigilanza, intervento AICOM, Banca d'Italia, Roma, 27 novembre 2025). Si tratta di un'indicazione di prospettiva, da distinguere dalle singole prescrizioni di vigilanza, che aiuta a collocare la compliance all'interno della conduzione dell'impresa.

8 Cfr. UNI ISO 37301:2021+A1:2024, punti 4.5 e 4.6. Lo standard distingue l'identificazione degli obblighi di compliance dal processo di valutazione dei relativi rischi. Quest'ultimo deve porre in relazione gli obblighi con le attività, i prodotti e i servizi dell'organizzazione, considerando anche i processi affidati all'esterno e i rapporti con soggetti terzi. La valutazione deve essere effettuata periodicamente e in occasione di cambiamenti sostanziali delle condizioni o del contesto organizzativo.

9 Un ambito di convergenza è rappresentato dal sistema di prevenzione della responsabilità degli enti disciplinato dal D.Lgs. 8 giugno 2001, n. 231. Il Modello di organizzazione, gestione e controllo previsto dagli artt. 6 e 7 del Decreto presenta elementi di complementarità con il SGC delineato dalla ISO 37301, in particolare con riferimento all'identificazione e valutazione dei rischi, alla definizione di protocolli e presidi organizzativi, all'attribuzione delle responsabilità, alla formazione e al monitoraggio dell'efficacia delle misure adottate. L'integrazione tra i due sistemi può favorire il coordinamento dei processi di valutazione dei rischi e dei controlli aziendali, evitando duplicazioni e valorizzando i flussi informativi tra le funzioni competenti e l'Organismo di Vigilanza. Resta ferma, tuttavia, la diversa finalità dei due strumenti: il Modello 231 è specificamente diretto alla prevenzione dei reati presupposto e assume rilevanza ai fini del regime di responsabilità dell'ente, mentre la ISO 37301 disciplina un sistema di gestione della compliance di portata più ampia.

Alla luce di ciò, il SGC richiede che ad ogni processo dell'organizzazione siano applicati tutti gli obblighi di compliance pertinenti. Si tratta di collegare regole specialistiche che spesso operano secondo logiche separate allo stesso processo. In particolare, protezione dei dati, correttezza nella relazione commerciale, prevenzione della corruzione, sicurezza del lavoro e tutela ambientale possono incidere sul medesimo processo, pur rispondendo a discipline e responsabilità differenti.

Inoltre, un modello integrato di compliance costruisce una relazione riconoscibile tra processi, obblighi, rischi, responsabili dell'attività e controlli. Pertanto, per ogni processo rilevante dell'organizzazione dovrebbero individuarsi - oltre alle citate regole applicabili - chi ne assicura il rispetto, come viene verificata l'efficacia dei presidi ed a quale livello devono essere portate le criticità.

Si consideri, ad esempio, il processo di selezione e gestione dei fornitori, nel quale possono concorrere obblighi di compliance di diversa natura, relativi alla prevenzione della corruzione, alla protezione dei dati personali, alla sicurezza delle informazioni, alla tutela dei lavoratori e al rispetto degli impegni contrattuali. Un approccio integrato consente di ricondurre tali obblighi a un unico processo aziendale, individuando le responsabilità delle diverse funzioni coinvolte, i rischi di non conformità e i relativi presidi di controllo. In questo modo, le verifiche specialistiche non rimangono attività isolate, ma concorrono alla valutazione complessiva del fornitore, alla definizione delle condizioni contrattuali e al successivo monitoraggio del rapporto.

5. L'esperienza del settore finanziario e la sua trasferibilità ad altri settori

Il settore finanziario ha sviluppato un'esperienza particolarmente significativa su metodologie, compiti e attività della compliance. Per le banche, i principi del Comitato di Basilea richiamano la responsabilità del consiglio di amministrazione nella supervisione del rischio di non conformità, quella dell'alta dire-

vedi l'articolo online

zione (organo di gestione) nella sua gestione, l'indipendenza della funzione, l'adeguatezza delle risorse e la verifica periodica della funzione di *internal audit* sulla struttura di controllo di secondo livello. La collaborazione tra l'area di compliance e l'area di business è compatibile con l'indipendenza quando sono assicurati autorevolezza, accesso alle informazioni e possibilità di riferire agli organi sociali e/o all'organo di gestione. Inoltre, la BCE ha evidenziato, nelle proprie analisi sugli operatori bancari, che la qualità della compliance dipende dalla governance, dalle risorse e dall'effettiva attuazione di politiche e processi[10].

Il confronto tra norma ISO e principi organizzativi e di compliance sviluppati nel settore finanziario fa emergere una parziale sovrapposizione: ad esempio, responsabilizzazione dei vertici, valutazione dei rischi, attribuzione dei compiti, controlli, flussi informativi e miglioramento delle misure adottate. Si tratta di una convergenza funzionale, ma non di un'equivalenza normativa[11].

Questa lettura comparativa suggerisce che la ISO 37301 possa aiutare anche un'impresa non finanziaria a rendere più sistematica la propria governance della conformità[12] [13].

Inoltre, l'esperienza del settore finanziario è trasferibile ad altre organizzazioni (non finanziarie) soprattutto per quanto riguarda la struttura organizzativa: attribuire responsabilità, sostenere i controlli con risorse adeguate, individuare anomalie/criticità e trasformarle in decisioni correttive.

Non esiste, tuttavia, un unico modello finanziario da replicare indistintamente in altre organizzazioni. Ad esempio, Banche, assicurazioni, istituti di pagamento e istituti di moneta elettronica sono soggetti a discipline specifiche; poi, all'interno della stessa categoria di ente (es banche), dimensioni, complessità e caratteristiche operative incidono sulle soluzioni organizzative. Quindi, il confronto o l'esperienza del settore finanziario deve riguardare principi e meccanismi di funzionamento, senza presumere identità di obblighi o automatica trasferibilità del modello.

Una struttura organizzativa di compliance pertanto è utile quindi anche per settori diversi da quello finanziario. Senza che ciò dipenda soltanto dalla presenza di un'Autorità di vigilanza prudenziale. Un'impresa del settore industriale può dover coordinare obblighi ambientali, sicurezza dei lavoratori e rapporti con distributori internazionali; un operatore commerciale può dover presidiare comunicazioni, condizioni contrattuali e trattamento dei dati; e un'impresa caratterizzata da innovazione e tecnologia può dover considerare l'impatto dei servizi offerti e delle dipendenze dai propri fornitori.

In questi contesti, una struttura organizzativa di compliance offre un metodo per intercettare anomalie e discontinuità e portarle all'attenzione del competente responsabile o alta direzione. Riducendo, così, i passaggi tra funzioni: ad esempio, un contratto modificato senza aggiornare le procedure, una nuova attività avviata senza adeguata formazione, una criticità del fornitore conosciuta dagli acquisti ma non valutata da chi governa il servizio.

L'istituzione del presidio di compliance deve però sempre guardare al principio di proporzionalità, che resta decisivo per non ingessare la struttura organizzativa. Una piccola organizzazione non ha necessariamente bisogno dell'apparato organizzativo di un grande gruppo; ha però bisogno di sapere quali obblighi la riguardano, quali rischi richiedono attenzione e chi è responsabile dell'intervento.

6. L'SGC e la creazione di valore

Il contributo "economico" della compliance all'organizzazione - sotto diversi profili - va letto attraverso il presidio dei rischi, la riduzione degli eventi avversi, etc.. Senza collegamenti diretti con il rendimento[14].

10 Cfr. BCE, Strengthening banks' compliance frameworks, Supervisory Newsletter, febbraio 2020.

11 Per gli intermediari bancari, il confronto deve essere condotto anche con la disciplina nazionale in materia di sistema dei controlli interni, ad esempio con riferimento alla Circolare della Banca d'Italia n. 285 del 17 dicembre 2013, Parte Prima, Titolo IV, Capitolo 3, e successive modifiche. Tale disciplina prevede specifici requisiti organizzativi e di controllo che conservano piena autonomia rispetto agli standard volontari di certificazione. La ISO 37301 può pertanto rappresentare un riferimento metodologico complementare, senza sostituire né modificare gli obblighi prudenziali e di governance applicabili.

12 Comitato di Basilea per la vigilanza bancaria, Compliance functions, Basel Consolidated Guidelines, modulo IAC 20, in particolare principi su responsabilità degli organi, indipendenza, risorse e revisione interna.

13 ISO/TC 309, ISO 37301 FAQs, maggio 2022, in particolare quesiti 6, 10–12 e 14–20.

14 Cfr. UNI ISO 37301:2021+A1:2024, punti 6.2 e 9.1. La norma richiede la definizione di obiettivi di compliance e il monitoraggio, la misurazione, l'analisi e la valutazione delle prestazioni del sistema. In tale prospettiva, gli indicatori possono riguardare, ad esempio, l'attuazione delle misure correttive, l'andamento delle non conformità e l'efficacia dei controlli. L'eventuale contributo dell'SGC alla creazione di valore economico costituisce una valutazione ulteriore, che non può essere automaticamente desunta dal conseguimento della certificazione.

vedi l'articolo online

Un primo profilo è la protezione e la custodia del valore esistente: prevenire errori e condotte scorrette può contenere perdite, costi di *remediation* e interruzioni operative.

Un secondo profilo riguarda la qualità dell'attività. Coinvolgere o integrare la compliance nell'organizzazione può ridurre nuove lavorazioni dei processi o dei servizi/prodotti offerti e ripensamenti, perché i requisiti entrano nei processi e nella progettazione dei servizi/prodotti.

Un terzo profilo riguarda l'affidabilità dell'organizzazione sul mercato. La capacità di documentare responsabilità e controlli può rendere più trasparente il confronto con clienti professionali, partner e investitori. Nelle verifiche su una controparte, un sistema ordinato facilita la comprensione di come la citata controparte governa i propri rischi. Ciò può favorire le relazioni commerciali, aggiudicazione di contratti o migliori condizioni economiche.

Un quarto profilo riguarda il valore nel rapporto con il cliente. Un processo commerciale comprensibile, coerente con le caratteristiche del prodotto/servizio e accompagnato da assistenza efficace può prevenire incomprensioni e controversie. Reclami e anomalie diventano informazioni utili per correggere il servizio/prodotto offerto.

7. Osservazioni conclusive: valutare la qualità dell'SGC nel tempo

Il SGC crea le condizioni per un'organizzazione più consapevole delle conseguenze delle proprie decisioni. La ISO 37301 può consolidare questo percorso attraverso un riferimento riconoscibile e verificabile, utile sia agli operatori finanziari, sia alle organizzazioni di altri settori.

La certificazione non costituisce il momento conclusivo del processo[15], ma si inserisce in un sistema che deve essere continuamente valutato e migliorato dagli Organi aziendali. Il risultato dipende dalla capacità di trasformare il sistema di gestione in una pratica quotidiana di governo: rendere visibili i rischi, attribuire responsabilità e utilizzare le evidenze per migliorare le scelte da cui nasce il valore dell'impresa.

Per banche e altri intermediari vigilati, un sistema di gestione della compliance coerente con lo *standard* ISO può costituire un riferimento per verificare la connessione tra presidi già esistenti, rafforzare il coordinamento tra funzioni/aree della società e rendere più sistematico il miglioramento della compliance, evitando duplicazioni rispetto agli assetti richiesti dalla Autorità di vigilanza. L'eventuale certificazione aggiunge una valutazione esterna e indipendente dell'SGC.

La certificazione ISO assume particolare rilievo negli ecosistemi in cui il servizio al cliente nasce dall'interazione tra intermediari, operatori fintech, piattaforme digitali, fornitori tecnologici e reti distributive: nei servizi c.d. *open banking*, nella finanza incorporata in servizi non finanziari e nelle catene di esternalizzazione, la qualità del risultato dipende anche dai raccordi tra organizzazioni diverse. In tali contesti, lo *standard* ISO può offrire un linguaggio comune per definire responsabilità, condividere criteri di valutazione dei rischi e organizzare flussi informativi, segnalazioni di anomalie e interventi correttivi lungo la filiera. L'adozione della normativa ISO da parte delle organizzazioni dell'ecosistema, anche non vigilate, e l'eventuale certificazione possono quindi rappresentare elementi utili nella selezione e nel monitoraggio delle controparti, da valutare in funzione delle attività effettivamente coperte e insieme alle evidenze sul funzionamento dei controlli. Il beneficio atteso è una maggiore capacità di riconoscere e governare i rischi che si propagano attraverso le relazioni tra imprese, compresi quelli derivanti da dipendenze comuni e da passaggi operativi non adeguatamente presidiati.

15 Cfr. UNI ISO 37301:2021+A1:2024, punti 9.2, 9.3 e 10. La norma prevede un sistema di verifica articolato in audit interni, riesame periodico da parte dell'organismo di governo e dell'alta direzione e gestione delle non conformità e delle azioni correttive. Il riesame deve considerare, tra l'altro, i risultati dei controlli, l'adeguatezza delle risorse, l'efficacia della valutazione dei rischi e il raggiungimento degli obiettivi di compliance, traducendosi in decisioni documentate sulle opportunità di miglioramento e sulle modifiche necessarie al sistema.

vedi l'articolo online



DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it