Corso di laurea in Strategic Management
Cattedra di Risk e Compliance Management

ISO 37301 PER LA GESTIONE INTEGRATA DELLA *COMPLIANCE*: ANALISI DELLA NORMA E IMPLEMENTAZIONE IN UN CONTESTO AZIENDALE

Prof. Sante Ricci
RELATORE

Prof. Massimo Ferrari
CORRELATORE

Gaetano Mazzù 780051
CANDIDATO

ANNO ACCADEMICO 2024/2025

INDICE

INTRODUZIONE

La gestione della *compliance* aziendale ha subito un'evoluzione significativa negli ultimi anni, passando da un mero adempimento legale a un approccio strategico integrato con le dinamiche di governo societario e di gestione del rischio.

In quest'ottica, gli *standard* internazionali e le *best practice* consigliano di adottare una prospettiva GRC (*Governance, Risk & Compliance*), dove l'acronimo rappresenta la gestione dei processi aziendali, l'analisi dei rischi e le attività di conformità normativa.

A ciò si aggiunge il collegamento strutturale con i sistemi di controllo interno. In Italia, ad esempio, il Sistema di Controllo Interno e Gestione dei Rischi (SCIGR) è concepito come un processo dei vertici aziendali volto a garantire, tra gli altri, il raggiungimento degli obiettivi di conformità a leggi e regolamenti.

L'importanza di tale approccio integrato è confermata dalla letteratura specialistica: le scelte di *governance* devono essere influenzate dall'analisi dei rischi e viceversa, in modo da evitare duplicazioni di ruoli e controlli ridondanti. In tale contesto, la *compliance* non è un'attività isolata, ma uno dei pilastri del modello di *governance* in quanto assicura che l'impresa operi nel rispetto delle normative, salvaguardando la reputazione e supportando la sostenibilità del *business*.

L'adozione di processi formalizzati e l'impegno del vertice aziendale nella cultura della *compliance* sono condizioni necessarie per un sistema di gestione efficace.

Nell'ambito degli *standard* internazionali, la norma ISO 37301:2021 (*Compliance Management Systems – Requirements with guidance for use*) si inserisce come punto di riferimento per i sistemi di gestione della *compliance*. Essa sostituisce formalmente la precedente ISO 19600:2014 e ne specifica i requisiti, fornendo le linee guida, e rappresentando pertanto un vero e proprio *standard* di certificazione.

La ISO 37301 codifica principi quali buona *governance*, integrità, trasparenza, *accountability* e sostenibilità e definisce un efficace sistema integrato di gestione della *compliance*.

Particolare importanza assume l'istituzione di una funzione di *compliance* autonoma, dotata dei requisiti di indipendenza, accesso diretto al vertice aziendale e risorse adeguate.

In questo contesto, l'obiettivo della tesi è duplice: da un lato analizzare in profondità la norma ISO 37301 nei suoi principi fondamentali, nella struttura e nei requisiti chiave; dall'altro, indagare l'applicazione pratica dello *standard* in un grande Gruppo industriale. Si valuterà come il Gruppo abbia implementato il sistema di gestione della *compliance* in conformità alla ISO 37301, verificando l'efficacia delle procedure adottate, i risultati ottenuti e le eventuali criticità riscontrate.

Lo studio coniuga, dunque, un'analisi teorica con un approfondimento empirico sul campo.

Il lavoro di tesi è articolato in tre capitoli principali. Il primo capitolo inquadra il tema nel contesto teorico di riferimento: vengono presentati i principali concetti di *compliance* e i modelli normativi e organizzativi più rilevanti, nonché le connessioni tra *compliance*, *governance* aziendale e sistema di controllo interno (SCIGR).

Il secondo capitolo è dedicato interamente alla norma ISO 37301: se ne descrivono la genesi, l'architettura basata sull'*High Level Structure* (HLS), i principi cardine e i requisiti chiave, evidenziando come lo *standard* possa essere integrato nei processi aziendali esistenti.

Infine, il terzo capitolo presenta il *business case*: qui si analizza il percorso di implementazione della ISO 37301 in un grande Gruppo industriale, illustrando la metodologia adottata, i risultati conseguiti e le principali sfide affrontate.

Tale struttura garantisce un'esposizione coerente e lineare, dai fondamenti teorici all'applicazione pratica dello *standard*.

CAPITOLO 1 - IL CONCETTO DI *COMPLIANCE* NELLA *GOVERNANCE* AZIENDALE

1.1 L'evoluzione della *compliance* nelle aziende

Per poter affrontare la questione della *governance* aziendale è fondamentale partire dall'analisi primordiale del concetto stesso di *compliance* e, per farlo, urge tenere in debita considerazione quelle che sono le evoluzioni dei bisogni e dei valori all'interno delle aziende e delle società nel corso del tempo. Le leggi che nei decenni si sono susseguite di certo riflettono la necessità di assecondare esigenze nuove; pertanto, la regolamentazione è stata da sempre un punto di partenza, non potendo certo pensare di poter sempre e comunque anticipare nuove dinamiche e problematiche.

Il termine "*compliance*" intanto va inteso sotto una duplice veste: da una parte tiene conto dell'ambito di applicazione, ovvero dei vari soggetti che ad essa si conformano e quali motivazioni attengono a quella determinata regolamentazione; dall'altro lato, con questo termine si vuole ampliare il punto di osservazione, tenendo in considerazione quelli che sono gli enti regolatori e qual è la portata delle strategie adottate in risposta alla normativa in essere.

In questa seconda accezione il termine *compliance* permette di considerare un suo significato più specialistico che mira a disciplinare l'aspetto regolatore a differenza del primo aspetto che invece punta a regolamentare la cooperazione e la persuasione dei soggetti coinvolti. In tal modo si evita la mera applicazione di sanzioni e pene, optando invece per una visione fondata sul deterrente e coinvolgendo gli interessi aziendali da perseguire. Puntando ad una tale valutazione probabilmente l'intento verrà massimizzato poiché ogni azienda propenderà inevitabilmente a soddisfare i propri intenti e per farlo proverà a soddisfare a pieno il novero delle regole da rispettare considerando la *compliance* come una congeniale misura da adottare per i benefici da ricavare al fine di evitare sanzioni particolarmente gravose.

Proprio la Banca d'Italia, nel documento di consultazione sulla *compliance* afferma la necessità di "*Promuovere una cultura aziendale (...) orientata al rispetto, non solo della*

lettera, ma anche dello spirito delle norme(...)"[1], a riprova del fatto di quanto sia davvero importante far acquisire in capo ad ogni azienda quel senso di responsabilità indispensabile per prevenire e gestire il rischio di non conformità, quel rischio che soggiace al mancato rispetto delle regole che porta ad incorrere in sanzioni penali e/o amministrative con conseguenti perdite finanziarie spesso rilevanti ed inevitabili danni all'immagine e alla reputazione per aver trasgredito a leggi, regolamenti o codici deontologici.

Per comprendere l'evoluzione della *governance* aziendale, è importante innanzitutto definire il significato stesso del termine.

Come già accennato in precedenza, il concetto di *corporate governance* intende delineare, più nello specifico, l'insieme delle regole e dei meccanismi attraverso cui le aziende operano, nel rispetto di normative ben precise che ne disciplinano la gestione e la direzione.

L'obiettivo principale è garantire l'efficacia delle strategie adottate dall'impresa.

In sostanza, attraverso la *governance* è possibile stabilire le modalità con cui vengono prese le decisioni aziendali, definendo anche gli strumenti e i metodi da utilizzare per raggiungere gli obiettivi prefissati.

Il governo d'impresa, quindi, attua quelle regole che consentono di esercitare e controllare l'autorità fiduciaria dell'impresa, regole che, chiaramente, rimandano anche a tutte le leggi dello Stato in cui opera l'azienda includendo le più varie relazioni che si innescano nel mondo societario quali: la proprietà, i manager, gli amministratori, i dipendenti, etc.

C'è da aggiungere, inoltre che, nel concetto di *governance* non può essere estromesso il meccanismo che riguarda la delega dell'autorità né tantomeno quell'insieme di aspetti che definiscono la *performance* come pure la sicurezza e la contabilità.

C'è da dire che in Italia dal 2004 è possibile scegliere tra diversi modelli di *governance* societaria: quello tradizionale, quello monistico e quello dualistico.

Più nello specifico, il modello tradizionale, detto anche ordinario, in quanto molto diffuso, prevede la presenza di un consiglio di amministrazione, che può essere composto da un amministratore unico oppure da un consiglio.

[1] Banca d'Italia (2006)

A questo si affianca un collegio sindacale, i cui organi hanno compiti e attività ben distinte e separate tra loro laddove il consiglio di amministrazione opera con funzione prettamente amministrativa mentre il collegio supervisiona l'attività dell'organo amministrativo.
Nel sistema monistico invece, c'è la presenza di un unico organo amministrativo che opera in veste di amministratore ma anche in qualità di organo di controllo.
Questo implica che, all'interno del consiglio di amministrazione, sia presente un comitato che esercita attività di controllo, comitato composto da amministratori che hanno requisiti ben precisi tra cui l'indipendenza e la professionalità; la parte contabile invece, in questo tipo di *governance*, viene affidata ad un revisore o ad un ente esterno.
Nel sistema dualistico si osserva una netta distinzione rispetto agli altri due modelli, in quanto l'amministrazione della società è suddivisa tra il consiglio di gestione e il consiglio di sorveglianza. Proprio al consiglio di sorveglianza vengono affidati compiti che, nel sistema ordinario vengono assegnati all'assemblea dei soci.
Altro incarico affidato al consiglio di sorveglianza è quello di nominare il consiglio di gestione dell'impresa mentre, anche qui, del controllo contabile viene investito un organo esterno.

1.2 L'integrazione tra *compliance*, gestione dei rischi e SCIGR

Laddove si ha a che fare con situazioni particolarmente complesse dal punto di vista operativo e regolamentare, la gestione dei rischi e dei diversi comparti di controllo assume un'importanza centrale.
In tali contesti, risultano fondamentali gli aspetti legati ai processi decisionali, con l'obiettivo di progettare benefici duraturi e di ampio respiro, in grado di generare valore non solo per gli azionisti, ma anche a favore di tutti gli *stakeholder* più rilevanti all'interno della società.
Quello a cui un'azienda punta è, principalmente, la realizzazione di obiettivi che possano definirsi di sviluppo sostenibile secondo quelli che sono i paletti imposti anche dall'Agenda 2030 delle Nazioni Unite (si parla dei cosiddetti "*Sustainable Devolopment Goals*" – SDGs). Tale assunto implica che, nelle grandi aziende, oltre al classico Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR), risulta fondamentale integrare

quest'ultimo sia sotto il profilo organizzativo, sia sotto quello amministrativo e contabile. Ciò presuppone, alla base, una netta interdipendenza tra i vari elementi che compongono il sistema, al fine di garantirne l'efficacia complessiva.

È chiaro che, una tale combinazione di fattori necessita una netta separazione tra il sistema interno di controllo e quello integrativo, sia dal punto di vista patrimoniale, contabile e organizzativo tant'è che, i sistemi di controllo di secondo livello vanno a definire i modelli di gestione del rischio, effettuando attività di monitoraggio garantendo una completa integrazione ai fini del funzionamento globale e complessivo del Sistema di Controllo Interno e Gestione dei Rischi.

Grandi aziende nel tempo hanno maturato sistemi integrati di controllo che, oltre a quello interno, presuppongono una convergenza della suddetta attività su più piani proprio per assicurare un governo unitario come gruppo tramite l'adozione di un meccanismo a processi.

In questo modo, ogni singolo processo permette una visione integrata e d'insieme dei diversi presidi di gestione dei rischi. Basti pensare alla corsa di molte società strutturate per aggiornare i propri sistemi in vista non solo della sostenibilità decantata poc'anzi ma anche in ragione delle novità poste in essere dalle più importanti *leading practice*, senza mai perdere di vista le fisiologiche mutazioni intervenute all'interno del gruppo stesso in termini di innovazioni ed evoluzioni e, quindi, conformemente alle norme vigenti sia a livello statale che regolamentare interno.

Ad oggi, le principali società, si soffermano molto alle strategie di sostenibilità definendo ruoli e responsabilità specifiche in ambito ESG *(Environmental, Social and Governance*) in modo che vi sia una chiara proiezione delle informazioni tra i diversi attori coinvolti entro il Sistema di Controllo Interno e, di conseguenza, nei confronti di tutti quelli che sono gli organi aziendali per meglio calibrare e definire la gestione dei relativi rischi.

Per poter attuare una programmazione così capillare e definita è importante garantire un'ottima interlocuzione tra i vari *stakeholder* affinché si possa ottimizzare il costante confronto sulle strategie d'impresa e il loro perseguimento.

A tal proposito c'è chi ha pensato di rafforzare il SCIGR consentendo alle società coinvolte di attuare di fatto i valori e i principi di integrità, trasparenza e legalità ai vari livelli del *business*, nel pieno rispetto delle norme e dei codici di condotta interni ed esterni limitando i conflitti tra i vari interessi aziendali e personali. Non si può non

ricordare quanto le varie componenti del SCIGR siano interdipendenti tra loro e strettamente collegate così come il sistema, nella sua totalità, sia ben integrato con il complesso assetto organizzativo, contabile e amministrativo.

Il SCIGR punta ad una massimizzazione sia dell'efficacia che dell'efficienza mediante un coordinamento tra i ruoli definiti dallo stesso e degli elementi che lo compongono affinché i compiti da svolgere da parte dell'organo di controllo siano funzionali ad un'ottima efficacia.

Importante è stata l'adozione di un programma di *compliance* finalizzato a tutelare la concorrenza e lo stesso consumatore, focalizzando l'attenzione su tutti quei valori essenziali destinati al rispetto di regole e principi basilari in materia.

Alcuni grossi gruppi societari hanno ampliato il sistema di controllo grazie anche a strumenti informatici che permettono di procedere all'analisi e alla gestione dei rischi operativi ma anche quelli di frode, di sicurezza IT, strategici fiscali, ESG e reputazionali, estesi a quelli di *compliance*.

Questo ha permesso di attuare la piena integrazione del processo di *risk management* di gruppo, garantendo così una condivisione massima tra le diverse metodologie di analisi dei rischi operando una migliore comunicazione anche tra i vertici aziendali e gli organi della stessa.

È evidente che, il sistema di controllo e di gestione dei rischi costituisce quell'insieme di regole e procedure proprie di un'azienda che offrono un valido supporto per garantire un'efficacie funzionamento dell'organizzazione permettendole di identificare, valutare, misurare e gestire i principali fattori di rischio a cui possa essere esposta.

Preme inoltre rammentare che, nell'ambito del SCIGR, i soggetti coinvolti sono individuati secondo un modello articolato su tre livelli di controllo ovvero le tre "linee di difesa", più precisamente: i controlli di primo livello (o prima linea) implicano tutte quelle attività di controllo poste in essere svolte dalle singole strutture organizzative del gruppo nell'ambito dei propri processi di modo che si garantisca la regolare esecuzione delle attività.

Il principale responsabile di queste operazioni viene demandata in capo al *management* e sono parte di ogni processo aziendale. Coloro che figurano quali responsabili delle diverse aree organizzative hanno, pertanto, il pieno compito di controllare il processo in ogni sua fase e gestirne i rischi dovendo, quotidianamente, acclarare la presenza di

possibili rischi che vanno identificati, monitorati, misurati e gestire onde consentire il giusto intervento per far rientrare il rischio e l'attività aziendale entro la sua ordinarietà conformemente con le norme vigenti, le procedure e i regolamenti interni.

Per quanto concerne i controlli di secondo livello questi vengono rimessi a strutture *ad hoc* preposte a tale scopo con propria autonomia e indipendenza funzionale e gerarchica rispetto alle strutture organizzative di primo livello. I loro compiti sono ben specificati e hanno un controllo su determinate aree e/o tipologie di rischio, in tale circostanza i referenti responsabili vanno a monitorare i rischi aziendali di propria competenza adducendo linee guida sui sistemi di controllo, dopo averne accertato la conformità rispetto all'efficienza che si vuole prediligere.

In ultimo abbiamo i controlli di terzo livello che vengono espletati dalla struttura organizzativa *internal audit*, offrendo consulenza obiettiva ed indipendente sull'adeguatezza dei controlli sia di primo che di secondo livello e, di conseguenza sul SCIGR nella sua globalità.

L'intento dell'*internal audit* è quello di analizzare struttura e funzionalità del SCIGR anche attraverso quel complesso monitoraggio operato mediante i controlli degli altri due livelli poc'anzi citati.

Alla base della gestione del rischio ovviamente esiste una specifica normativa che possiamo rintracciare nel Codice di *Corporate Governance*, rivolto a tutte le società con azioni quotate sul Mercato Telematico Azionario (MTA) che viene gestito da Borsa Italiana.

Il Codice suindicato ha un'adesione volontaria e, al suo interno, troviamo ben sei sezioni, ciascuna delle quali, a sua volta, è suddivisa in principi generali e in raccomandazioni che vanno a stabilire gli obiettivi per realizzare una buona *governance* con l'intento di orientare le condotte di modo che si adeguino alle finalità e alle basi proprie di buon "governo" aziendale.

Il nocciolo duro del Codice rivisitato è costituito da tre elementi: la semplificazione, la flessibilità e la proporzionalità; la prima si fonda sul fatto che ad oggi la raccolta normativa è molto più concisa rispetto al passato, si parla di flessibilità perché la sua applicazione prescinde dal sistema di amministrazione e dal tipo di controllo adottato,

mentre si parla di proporzionalità in quanto tiene conto di due differenti categorie: le società grandi[2] e le società a proprietà concentrate.

Come si accennava precedentemente un altro aspetto fondamentale è rappresentato, dal 2020, dalla necessità di garantire anche un'adeguata sostenibilità, ciò implica che, gli amministratori devono appunto mirare a perseguire questo ulteriore intento dovendo tenere in considerazione anche le finalità proprie di altri portatori di interesse (i cosiddetti *stakeholders).*

Ad oggi il tema della gestione dei rischi e del sistema di controllo interno assume un rilievo ancora maggiore, soprattutto alla luce degli effetti generati dalla pandemia da COVID-19. Quest'ultima ha evidenziato l'emergere di nuovi rischi globali che, in determinate condizioni, possono compromettere la stabilità delle aziende.

Secondo studi condotti dal *World Economic Forum*[3] i principali fattori di allerta a livello globale, strettamente legati a questioni ambientali ma con significative ricadute anche sul piano finanziario ed economico, sono principalmente cinque: la recessione economica, i fallimenti aziendali, le difficoltà legate all'approvvigionamento, gli attacchi informatici (*cybersecurity*) e le frodi[4]. La ragione di questi nuovi rischi è dipeso senza dubbio dall'uso dello *smart working* che ha determinato uno spostamento in digitale di tutta una serie di dati importanti e documenti sui quali è possibile operare e quindi accedere fuori dal tipico contesto lavorativo con inevitabili conseguenze in termini di sicurezza, aspetti questi, che necessitano di una marcata attenzione da parte dell'intero sistema di gestione dei rischi allo scopo di ridurre al minimo i danni che ne potrebbero derivare a carico soprattutto delle società più grandi e quotate sul mercato.

A riguardo è bene ricordare che, nello specifico, il Codice di Autodisciplina individua tre principi cardine ai quali il SCIGR deve attenersi. Tali principi sono essenzialmente quelli enunciati nell'art. 6: "**XVIII**. *Il sistema di controllo interno e di gestione dei rischi è orientato all'identificazione, misurazione, gestione e monitoraggio dei rischi cui il business è prevalentemente esposto, col fine ultimo di mitigarli e/o neutralizzarli effettivamente, grazie all'efficacia e all'efficienza dello stesso;* **XIX**. *L'organo*

[2] Si intendono "grandi" quelle società che hanno avuto una capitalizzazione superiore ad un miliardo di Euro alla fine dei tre precedenti esercizi

[3] The Global Risks Report 2021 – XVI edizione – gennaio 2021

[4] Si veda, per ulteriori approfondimenti, l'articolo di Quintavalle, M. (2020) "*La crisi COVID-19 aumenta il rischio frodi per le imprese. I sistemi di controllo "intelligenti" permettono di non abbassare la guardia durante una crisi: il caso AST*" pubblicato su Marsh.com.

amministrativo valuta e definisce l'orientamento di tale sistema in coerenza con le strategie societarie e con il risk appetite della proprietà, valutandone annualmente sia l'adeguatezza sia l'efficacia; **XX**. *Il coordinamento e i flussi informativi sono sempre definiti dall'organo amministrativo e sono volti a massimizzare l'efficienza del sistema, a ridurre le duplicazioni di attività e ad agevolare l'efficace svolgimento dei compiti dell'organo di controllo*[5]*".*

Lo stesso Codice, per quanto concerne le raccomandazioni, offre un ventaglio di indicazioni abbastanza complesse e ricche di informazioni dettagliate offrendo spunti interessanti che, se pienamente acquisite dalle aziende, possono fare la differenza in termini di gestione dei rischi assicurando quell'insieme di equilibri ritenuti essenziali per poter realizzare obiettivi di salvaguardia in linea con la sostenibilità che possano durare nel tempo.

Nel dettaglio sempre all'art. 6 del sopra citato Codice troviamo la Raccomandazione n. 32 che elenca l'insieme delle specifiche da attuare ,tenendo in debita considerazione i ruoli di ciascun organo all'interno della società stabilendo che: "*L'organizzazione del sistema di controllo interno e di gestione dei rischi coinvolge, ciascuno per le proprie competenze*[6]*"*, dove troviamo nel dettaglio i compiti propri di ognuno, quale l'organo di amministrazione, il *chief executive officer*[7], il comitato controllo e rischi, il responsabile della funzione di *internal audit*, l'organo di controllo e tutte le altre funzioni aziendali coinvolte nei controlli e maggiormente esposte ai rischi.

[5] Il Comitato per la Corporate Governance è stato costituito, nell'attuale configurazione, nel giugno del 2011 ad opera delle Associazioni di impresa (ABI, ANIA, Assonime, Confindustria), Borsa Italiana S.p.A. e l'Associazione degli investitori professionali (Assogestioni). Il Comitato ha quale scopo istituzionale la promozione del buon governo societario delle società italiane quotate. A tal fine il Comitato approva il Codice di Corporate Governance delle Società Quotate e ne assicura il costante allineamento alle best practice internazionali. Il Comitato garantisce anche un monitoraggio con cadenza annuale dello stato di attuazione del Codice da parte delle società aderenti, indicando le modalità più efficaci per favorire una applicazione sostanziale delle sue raccomandazioni. Per un'integrale lettura del documento si rimanda al sito: https://www.borsaitaliana.it/comitato-corporate-governance/codice/2020.pdf.

[6] https://www.borsaitaliana.it/comitato-corporate-governance/codice/2020.pdf

[7] Il "*chief executive officer*" che è l'incaricato dell'istituzione e del mantenimento del sistema di controllo interno e di gestione dei rischi

1.3 La *compliance* come strumento di *governance* e tutela dei rischi

Per poter affrontare la complessità dei rischi all'interno di un'azienda è fondamentale avvalersi di un sistema di *Governance, Risk and Compliance Management* (GRC) che possa fornire in tempi brevi tutte le informazioni relative all'ambiente esterno e che possa permettere di trovare soluzioni rapide e sostenibili alle diverse criticità presenti.

È ancora frequente che le aziende, cerchino di affrontare la *compliance* normativa in modo destrutturato e solo in presenza di situazioni più complesse da affrontare si procede con l'implementazione di un sistema di *governance* e *compliance* cercando di contenere costi e arginare le problematiche affrontate in ragione delle proprie necessità.

È chiaro che una visione del genere non consente di avere una lettura unitaria e lungimirante di quelle che sono le problematiche aziendali con il rischio di non riuscire a prevenire le situazioni critiche soprattutto nel lungo periodo.

Ovviamente, vista l'importanza del sistema di sicurezza all'interno di un'azienda, affidare a dei gestori esterni questo tipo di servizio è diventato un fenomeno necessario e sempre più diffuso, comportando l'acquisto di piattaforme specializzate potendo così operare su sistemi applicativi che riducono in qualche misura il carico dell'onere in capo alle imprese, compresi quelli inerenti agli aggiornamenti dei software e del quadro normativo di riferimento.

La maggior parte dei sistemi utilizzati fa affidamento ad una gestione conforme con gli *standard* ISO e, sul mercato, possiamo trovare principalmente due modelli: uno di tipo verticale che si occupa di ambiti specifici o del settore *industry* e poi c'è il sistema integrale che opera invece su più aree tematiche in maniera dettagliata e approfondita.

Il primo tipo di piattaforma chiaramente fa venir meno l'obiettivo inerente al raggiungimento di benefit collegati ad una visione globale, portando spesso a dover investire ulteriormente in altri moduli che, singolarmente, vadano a gestire e curare settori scoperti dal sistema di controllo principale.

Da ciò si evince che la soluzione più oculata pare essere quella di un sistema integrale che andrebbe a beneficiare su tutte e tre le aree: quella di *governance*, di *risk* e di *compliance management*.

Nell'ambito della *governance* poter contare su un sistema unico permette di evitare che si abbiano delle inutili duplicazioni sia nelle risorse che nei processi, inoltre, un sistema

così completo offre la possibilità di capitalizzare a pieno le conoscenze aziendali adottando una *governance* che sia efficace ed efficiente.
Bisogna anche aggiungere che i sistemi GRC consentirebbero anche di avere una visione lungimirante rispetto all'identificazione dei rischi, anche quelli meno evidenti, potendo così attuare le strategie più congeniali capaci di attenuare gli effetti negativi e migliorando i benefici nel tempo garantendo una continuità di *business* con conseguente ridotta perdita di capitali.
A tal riguardo dobbiamo da subito dire che i sistemi più all'avanguardia sono basati sullo *standard* ISO 31000:2009.
Logicamente operare grazie ad un sistema integrato di *compliance management* garantisce la possibilità di rispettare non solo le norme imposte ma anche quelle proprie dell'azienda offrendo così un continuo controllo che automaticamente mette l'azienda nella condizione di attenersi al quadro normativo vigente limitando i danni derivanti da possibili violazioni e sanzioni che, inevitabilmente andrebbero ad intaccare anche l'immagine della stessa. Chiaramente, avere una visione unitaria nella gestione del rischio, come si accennava poc'anzi, abbatte anche i costi per un'azienda, costi derivanti dalla *compliance,* soprattutto laddove parliamo di imprese che presentano un quadro notevolmente complesso al suo interno così come quando, al loro interno, presentano forti differenze in termini di settore comportando anche una grande dinamicità sul mercato.

1.4 Il ruolo dei sistemi di gestione certificati nella strategia aziendale

È importante stabilire intanto l'importanza dei sistemi di controllo che hanno soprattutto una funzione di prevenzione e per poter legittimare una tutela dei rischi di *business* è fondamentale definire il cosiddetto "rischio accettabile". Il rischio si definisce accettabile laddove i controlli ulteriori implicano una spesa di costo più alta rispetto alla risorsa da tutelare ma i soli costi non rappresentano l'unico riferimento a cui fare riferimento per valutare il rischio accettabile, in quanto entrano in gioco anche variabili quali la probabilità di accadimento dell'evento rischioso, l'impatto reputazionale sull'organizzazione, le possibili conseguenze legali e regolamentari, nonché la tolleranza al rischio definita dalla *governance* aziendale.

Perché un'azienda possa mettersi al riparo da situazioni di rischio è fondamentale affidarsi a sistemi di controllo che siano certificati per migliorare l'immagine e la visibilità delle stesse e ottenere così maggiore consenso anche fra clienti e investitori sul mercato. Questo suggerisce come, tali sistemi, abbiano una funzione ben diversa rispetto ai modelli organizzativi e di gestione previsti dal decreto legislativo n. 231/2001 che mirano a prevenire eventuali reati nelle attività dell'ente.

Certificare i sistemi di gestione significa ottenere degli *standard* di qualità che siano certi e ben definiti poiché attraverso tali strumenti è possibile assicurare una specifica capacità dell'azienda di riuscire ad organizzarsi sul mercato per gestire le risorse e ottimizzarle nei vari processi produttivi in modo da renderli efficaci. Gli *standard* di questi sistemi vengono definiti dall'*International Organization for Standardization* (ISO). Si tratta di un'organizzazione operativa a livello mondiale che uniforma le norme nelle diverse materie del settore. La sede è a Ginevra e i membri sono costituiti dai vari organismi internazionali di standardizzazione che sono dislocati in 164 Paesi.

Le norme ISO sono identificate mediante un titolo, un numero e l'anno di pubblicazione o revisione, nel titolo si descrive brevemente la norma stessa.

Gli *standard* ISO sono concepiti per garantire un miglioramento continuo dei sistemi di gestione, affinché questi risultino sempre coerenti, efficaci e sostenibili e il modello impiegato è denominato PDCA (*Plan-Do-Check-Act*).

Esistono diverse certificazioni relative ai sistemi di gestione, tra cui la ISO 9001, che definisce i requisiti per i sistemi di gestione della qualità, e la ISO 14001, che riguarda la gestione ambientale, con l'obiettivo di monitorare e ridurre gli impatti ambientali derivanti dalle attività delle organizzazioni.

Altrettanto importante è la ISO 45001 (ormai nota come UNI EN ISO 45001:2023 in quanto recepita a livello europeo dal CEN[8] mediante un aggiornamento che la norma internazionale ha subito il 28 settembre del 2023) che va a dettagliare i requisiti per avere un sistema di gestione per la salute e la sicurezza sul lavoro (SSL).

Lo scopo della ISO 45001 è principalmente quello di consentire alle organizzazioni di poter realizzare luoghi di lavoro che siano sempre più sicuri e salubri, prevenendo, laddove possibile, malattie e lesioni strettamente correlate all'attività lavorativa.

[8] Il Comitato europeo di normazione, meglio noto con l'acronimo CEN, è un ente normativo che ha lo scopo di armonizzare e produrre norme tecniche europee in collaborazione con enti normativi nazionali e sovranazionali quali per esempio l'ISO.

Questa ISO è estendibile ad ogni tipo di azienda a prescindere dalle sue dimensioni e dall'attività e anche per questa norma ci si è avvalsi della struttura ad alto livello (HLS) comune ad altre norme ISO sui sistemi di gestione facilitandone così l'integrazione tra le stesse.

La norma inoltre contiene un'appendice informativa nazionale che al suo interno ha delle note sulla corretta collocazione di essa entro il sistema legislativo vigente, qual è appunto il Testo Unico per la sicurezza nei luoghi di lavoro[9].

Il sistema di cui ci si occuperà più nello specifico nel corso di questo elaborato è però l'ISO 37301 sistema operativo dall'aprile 2021 che riguarda la "*Compliance Management System – Requirements with for use*" e mira a soddisfare tanto le organizzazioni private quanto quelle pubbliche, allo scopo di favorire un sistema di gestione della *compliance* per il controllo dei rischi. Lo scopo principale di ISO 37301 è quello di realizzare obiettivi di sviluppo sostenibile puntando alla *compliance obligations*, alla *compliance culture* che tiene conto dei valori, dei comportamenti e dell'etica che sono alla base dell'organizzazione, nonché del *conduct*, ovvero dello specifico comportamento che può determinare conseguenze sui soggetti coinvolti sia interni che esterni ma che può avere anche conseguenze sull'ambiente.

Alla base della nuova ISO 37301 vi sono, come in tutti i sistemi di certificazione, alcuni principi fondamentali quali la trasparenza, la gestione del rischio e la *leadership*. La norma si propone di consolidare e rafforzare tali aspetti, aggiornando e sostituendo la precedente ISO 19600 per allinearsi ai più recenti *standard* richiesti dal sistema normativo e dalle esigenze del mercato.

Uno degli aspetti più interessanti è che la ISO 37301 rispetto alla ISO 19600 presenta l'elemento della certificabilità del nuovo *standard* in quanto la ISO 19600 essendo una norma *type* B si limitava a fissare le linee guida e i criteri generali mentre, la ISO 37301 è "verificabile" nel senso che implica la presenza di requisiti che sono compatibili con una vera e propria certificazione dello *standard* ISO, aspetto questo che si collega alle norme definite *type* A.

[9] Il Testo Unico per sicurezza sul lavoro è stato introdotto con il Decreto legislativo n.81 del 9 aprile 2008, successivamente modificato dal D.L. 202/2024, convertito con modifiche mediante la L. 15/2025. Per una lettura integrale del documento si rimanda al seguente link: https://www.altalex.com/documents/codici-altalex/2013/10/16/testo-unico-in-materia-di-sicurezza-sul-lavoro

Lo scopo del Comitato Tecnico internazionale è stato quello di spingere la suddetta norma al di là del *management* coinvolgendo le posizioni apicali delle organizzazioni, così introducendo il concetto di cultura della *compliance* aziendale che mira a sostenere valori e principi aziendali condivisi anche mediante una loro concreta adozione da parte dei vertici; da qui l'istituzione della funzione di *compliance* con le seguenti caratteristiche: l'indipendenza della struttura organizzativa, l'accesso diretto all'organismo di governo e all'alta direzione, l'autorità e la competenza adeguati alla funzione rilevante che si prefigge.

Le regole prescrittive descritte nella norma, difatti, si basano sui principi di una buona *governance,* proporzionalità, integrità, trasparenza, *accountability*, e sostenibilità, descrivendo le componenti, i requisiti e i processi chiave di un adeguato *Compliance Management System* (CMS).

Per quanto concerne l'implementazione dello *standard*, dalla lettura della ISO 37301 è evidente che si parte sempre dagli obiettivi (integrità, cultura, conformità, valori etici e reputazione) e dai correlati principi dell'organizzazione (sopra citati), prevedendo il consolidato ciclo: *Plan – Do – Check – Act*.

Focalizzandoci sui requisiti per l'adeguamento alla ISO 37301, si trova una chiara evidenziazione del collegamento tra la certificazione e la prova dell'effettivo impegno societario a una corretta gestione integrata della *compliance*.

Al vertice aziendale, difatti, viene richiesto un riesame periodico sull'adeguatezza ed efficacia del sistema di gestione per raggiungere i propri obiettivi e conseguire il miglioramento continuo.

Altro elemento distintivo della ISO 37301 è l'assegnazione a una funzione/ struttura di *compliance* di specifiche competenze e dei poteri necessari per:

- supervisionare e assicurare la conformità del sistema di controllo (come funzione di controllo di secondo livello, raffrontandolo al *framework* delle 3 Linee di controllo);
- relazionare al vertice aziendale e *top management* sull'attuazione del sistema;
- effettuare una valutazione dei rischi di *compliance*;
- definire controlli e procedure, promuovendo l'approvazione di una *compliance policy* (comprensiva di un sistema di *whistleblowing*);

- verificare sull'attuazione del sistema procedurale e organizzativo, attraverso *compliance audit* (e correlati *follow up*) e monitoraggi periodici sull'attuazione del sistema e dei piani di azione di miglioramento dello stesso.

CAPITOLO 2 - LA NORMA ISO 37301: STRUTTURA, FINALITÀ E PROCESSO DI CERTIFICAZIONE

2.1 Origini della ISO 37301

I criteri che stanno a fondamento di questo sistema di gestione rappresentano un importante punto di riferimento per realizzare sistemi aziendali idonei che si conformino ad un modello di organizzazione, gestione e controllo in stretta connessione con il D.Lgs 231/2001 che stabilisce la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della L. n.300 del 2000".*

Per introdurre quindi questo nuovo sistema di certificazione è bene soffermarsi sul dettaglio della normativa vigente e summenzionata, partendo proprio dal D. Lgs. 231/2001 che, per la prima volta, ha disciplinato la responsabilità penale degli enti, responsabilità che si affianca a quella propria della singola persona fisica che ha commesso l'illecito al solo scopo di favorire l'organizzazione stessa per la quale opera anche in assenza di un vantaggio concreto purché si accerti un mero interesse dell'ente. Tale circostanza è perseguibile sia nell'ipotesi in cui l'evento venga commesso da chi ha un ruolo di vertice sia da soggetti sottoposti ma anche da coloro che agiscono in qualità di procacciatori o consulenti.

Nonostante il dato di responsabilità che emerge dal dettato normativo di cui sopra, c'è però da aggiungere che lo stesso legislatore ha introdotto talune modalità che consentono agli enti di andare esenti da questo tipo di responsabilità e lo specifica negli artt. 6 e 7 del D. Lgs 231/2001 laddove sono indicate quelle caratteristiche che il modello di gestione e controllo deve a tal fine possedere.

Più propriamente l'art 6, comma 1, del D. Lgs 231/2001 statuisce che *"(...) l'ente non risponde se prova che: a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, i modelli di organizzazione e di gestione idonei a prevenire i reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e*

l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (...)"[10].

Altrettanto significativo è quanto riporta lo stesso articolo ma al comma 2 dove si prevede che *"(...) a) individuare le attività nel cui ambito possono essere commessi reati; b)prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire; c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati; d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli; e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello (...)"*[11].

In sostanza, dalla lettura combinata di queste norme si evince l'importanza di analizzare il contesto aziendale per prevenire e identificare eventuali rischi evidenziando settori o aree di attività dalle quali possano derivare maggiori situazioni pregiudizievoli, inoltre pare ovvia la rilevanza di una progettazione di un sistema di controllo nonché l'istituzione di un organismo di vigilanza che vada realmente a monitorare l'efficacia del sistema di controllo. È chiaro che, un modello, così come descritto per funzionare necessita di un processo continuo di verifica e adeguamento soprattutto per far fronte alle situazioni di cambiamento che possono interessare l'organizzazione aziendale in determinati momenti storici.

Sulla scorta di quanto descritto fino ad ora possiamo cercare di delineare le origini del sistema ISO 37301 ricordando che la norma è stata pubblicata il 14 aprile del 2021 introducendo la "*Compliance Management Systems*" che ha determinato un cambio di passo importante nei sistemi di controllo e gestione del rischio aziendale.

La suddetta norma è poi di fatto entrata in vigore il 1° luglio del 2021 andando determinare una evoluzione della precedente UNI ISO 19600:2016. La portata applicativa

---

[10] Decreto legislativo 8 giugno 2001, n. 231 Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300 (G.U. n. 140 del 19 giugno 2001), artt. 6 co. 1 lettere a) e b); per il testo integrale https://www.bosettiegatti.eu/info/norme/statali/2001_0231.htm.

[11] Decreto legislativo 8 giugno 2001, n. 231 Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300 (G.U. n. 140 del 19 giugno 2001), art. 6 co. 2; per una integrale lettura https://www.bosettiegatti.eu/info/norme/statali/2001_0231.htm.

della ISO 37301 si estende alle piccole, medie e grandi aziende operanti nei vari settori, tanto nel pubblico quanto nel privato, comprese le organizzazioni no-*profit*.

Un dato rilevante è che con questa norma è andata ad innovarsi la certificabilità del nuovo *standard*. Gli aspetti di successo su cui si basa il nuovo CMS (*Compliance Management System*) sono costituiti dalla presenza di una buona *governance*, dal rispetto di principi quali la proporzionalità, l'integrità, la trasparenza e la sostenibilità. Ciò determina una serie di obblighi in capo all'organizzazione aziendale, come l'adeguamento a leggi, regolamenti, convenzioni, licenze ma anche ad accordi di carattere volontario quali i regolamenti interni, i codici etici e i codici di condotta di categoria.

Un dato essenziale che emerge dalla norma ISO 37301 è che, per la prima volta, si parla di "cultura" della *compliance* aziendale, la quale guarda ad ampio raggio a tutta una serie di regole e principi, ma anche valori e comportamenti a cui ci si debba necessariamente uniformare per valutare il rischio e scegliere le risorse più idonee.

Uno dei requisiti della ISO 37301 è la presenza di una specifica funzione aziendale dedicata alla *compliance* che vada a dirigere la *Compliance Obligations* e i relativi rischi (si parla, infatti, di *Compliance Risk*). Lo scopo è quello di dare alla suddetta *compliance* una certa indipendenza rispetto alle strutture decisionali ed esecutive così come deve avere un accesso diretto all'alta direzione di modo che possa esercitare un certo grado di autorità che sia proporzionata al contesto.

Per poter realmente attuare quanto sin qui detto è fondamentale che ci sia una chiara attribuzione dei ruoli e delle responsabilità all'interno dell'azienda, devono essere ben inquadrati i controlli con adeguata programmazione delle procedure, di modo che emergano, al bisogno, le criticità da correggere e su cui intervenire con prontezza.

È chiaro che la norma ISO 37301 non va attuata da sola ma richiede un costante allineamento anche ad altri precedenti riferimenti come la ISO 37002 ad esempio, affinché si garantisca anonimato e riservatezza al soggetto che si espone nel riferire possibili irregolarità e violazioni, e questo per impedire che possano esserci eventuali ripercussioni sullo stesso.

È bene ricordare che la ISO 37002 nasce dopo un anno dall'entrata in vigore del cosiddetto Decreto *Whistleblowing*[12], a seguito della direttiva UE 1937/2019, che

[12] *Tofacchi F., LA DISCIPLINA DEL WHISTLEBLOWING;* Giuffrè, 2024. Il Whistleblowing viene per la prima volta introdotto in Italia nel 2012 con la Legge 6 novembre 2012 n. 190 rubricata "*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione*",

regolamentava la protezione delle persone che segnalano violazioni del diritto dell'Unione. In Italia la suddetta direttiva è stata recepita con il D. Lgs. 24/2023.

In ragione di quanto sopra indicato, *l'International Organization for Standardization* (ISO) ha provveduto a pubblicare, nel 2021 la norma 37002 contemplando le Linee Guida al fine di ampliare e conservare un sistema di gestione sul *Whistleblowing*, basato sui principi di fiducia, imparzialità e tutela dei soggetti coinvolti. Anche se la ISO 37002 è stata introdotta prima dell'avvento del D. Lgs. n. 24/2023, ha consentito alle imprese di acquisire, con largo anticipo, pratici suggerimenti operativi a sostegno delle garanzie prescritte. In sostanza, con la ISO 37002, si è cercato di sostenere la difesa e la protezione dei dati e delle informazioni connesse ad una segnalazione, tutelando l'anonimato di un possibile segnalante e/o dei soggetti individuati mediante la segnalazione stessa. L'obiettivo dello *standard* è stato quello di processare in maniera più dettagliata il sistema di segnalazione individuando quattro fasi specifiche: ricezione del rapporto di illeciti, valutazione del rapporto di illeciti, trattamento del rapporto di illeciti e chiusura del caso di *whistleblowing*[13].

Aderire alla ISO 37002 significa quindi facilitare le segnalazioni di azioni *contra legem,* migliorando l'efficacia dei sistemi di gestione e favorendo le regole di trasparenza e legalità, da qui l'importanza di raccordare questa ISO con la ISO 37301 in quanto, in stretta sinergia, le due norme contribuiscono a potenziare la cultura aziendale: la ISO 37002, integrandosi con la ISO 37301, fornisce alle aziende strumenti per affrontare eventuali violazioni in modo più rapido ed efficace.

Questo quindi ci fa comprendere che l'intento è proprio quello di realizzare una sinergia e una corretta integrazione tra le varie norme suesposte al fine di ottimizzare i risultati. Del resto, quanto asserito trova conferma nel fatto che la ISO 37002 può ben soddisfare i requisiti della ISO 37301 in quanto gli ambiti di applicazione sono complementari tra loro

---

meglio nota come "Legge Severino". La disciplina aveva l'obiettivo di promuovere uno strumento di lotta alla corruzione che consentisse al dipendente pubblico di denunciare gli illeciti di cui fosse venuto a conoscenza nell'ambito della propria attività lavorativa, senza temere eventuali azioni ritorsive a suo carico. Tale normativa, tuttavia, non ebbe il seguito sperato, anche a causa della mancata adozione di un apparato di norme volte a tutelare il segnalante in modo effettivo e concreto.

[13] Per un approfondimento della ISO 37002:2021 si rimanda al sito dell'UNI (Ente Italiano di Normazione) al seguente link: https://www.uni.com/sistemi-di-gestione-per-il-whistleblowing/.

ed entrambi si fondano sull'Annex SL[14] che ha lo scopo di armonizzare la struttura di tutti gli *standard* ISO.

Ovviamente, nonostante le correlazioni tra le diverse norme, non mancano delle varianti importanti, ad esempio: la ISO 37301 mira ad una buona *governance* garantendo l'integrità, la conformità, la cultura, la reputazione, i valori e l'etica, e per farlo impone degli obblighi di conformità dell'azienda per poter ampiamente soddisfare i vincoli prescritti.

2.2 Struttura della norma: sezioni, principi e linguaggio di alto livello (HLS)

Dopo aver introdotto la norma ISO 37301 partendo dall'esegesi della stessa, nel presente paragrafo si cercherà, più nel dettaglio, di descrivere e comprendere gli aspetti essenziali di tale certificazione. Premessa da fare è che la ISO 37301 è stata elaborata dal Comitato Tecnico ISO/TC 309 sotto la stretta competenza della Commissione Tecnica UNI - l'Ente italiano di normazione - che ha salvaguardato le esigenze nazionali dal punto di vista tecnico sottoponendo alla Commissione Centrale Tecnica dell'UNI l'adozione della norma nella versione in lingua italiana, approvazione giunta come si è già detto in precedenza il 24 giugno 2021 con successiva ratifica da parte del Presidente dell'UNI fino alla sua concreta entrata in vigore l'1 luglio 2021.

È necessario ricordare che tutte le norme UNI sono redatte in maniera tale che vengano presi in considerazione tutti gli interessi delle parti coinvolte nell'intento di far convogliare in esse le varie richieste puntando a conciliare possibili conflitti, tutto ciò allo scopo di concretizzare il consenso opportunamente richiesto.

Per favorire la suddetta progettazione normativa viene infatti data l'opportunità ai soggetti coinvolti di proporre suggerimenti e miglioramenti che vanno trasmessi nei tempi opportuni all'UNI.

[14] L'Annex SL è quella struttura di alto livello dell'ISO (Organizzazione Internazionale per la Normazione) e serve per assicurare coerenza e uniformità tra gli standard dei sistemi di gestione. Sostituisce la ISO Guide 83 e stabilisce una comune struttura, con termini e definizioni uguali per tutti i nuovi standard ISO riguardanti i sistemi di gestione.; https://www.sicurezzaegiustizia.com/.

Le norme UNI sono soggette a revisione con la pubblicazione delle nuove versioni alle quali gli utilizzatori sono tenuti ad uniformarsi accertandosi di possedere le ultime edizioni.

Abbiamo già visto a chi si rivolge la ISO 37301, ora urge capire qual è la sua struttura partendo dal presupposto che la norma si basa sull'HLS dell'ISO, di recente aggiornamento che oggi si definisce semplicemente HS (*Harmonized Structure*), facilitando l'integrazione con le altre norme che si applicano ai sistemi di gestione (v. *infra*).

Possiamo quindi distinguere una parte che concerne il vero e proprio contenuto normativo e i suoi requisiti, vale a dire i criteri prescritti a cui rifarsi obbligatoriamente nel rispetto della conformità agli *standard* e poi c'è la cosiddetta "Appendice A" che è la guida all'utilizzo della norma: in essa vengono contemplate le indicazioni o le linee guida per l'applicazione corretta della ISO. Ribadiamo che, i principi su cui essenzialmente si deve fondare il sistema di gestione sono: la buona *governance*, la proporzionalità, l'integrità, la trasparenza, l'*accountability* e la sostenibilità.

Gli enti che vogliono ottenere buoni risultati nel lungo periodo devono ovviamente puntare sulla *compliance* quale vero e proprio stile operativo affinché si tenga conto dei vari interessi coinvolti e delle diverse aspettative; quindi, *compliance* significa dare una concreta opportunità di successo guardando alla sostenibilità.

Soltanto un sistema di gestione fondato sulla *compliance* permette di dimostrare l'impegno di un'organizzazione al rispetto delle leggi, dei codici di settore ma anche nel rispetto delle regole per una buona *governance*. Tutto questo, secondo la ISO 37301, offre gli strumenti per migliorare il profilo ESG dell'impresa nel rispetto del territorio e dell'ambiente ma sempre con occhio attento alla società e agli aspetti interni propri dell'azienda e alla sua amministrazione.

Più nel dettaglio vediamo gli obiettivi che la norma ISO 37301 persegue per uno Sviluppo Sostenibile dell'Agenda 2030 (SDGs) sono:

- Obiettivo 8: Lavoro dignitoso e crescita economica;
- Obiettivo 9: Imprese, innovazione e infrastrutture;
- Obiettivo 11: Città e comunità sostenibili;
- Obiettivo 12: Consumo e produzione sostenibile;
- Obiettivo 16: Pace, giustizia e istituzioni solide.

Ma quali sono gli obblighi di *compliance* a cui bisogna attenersi per realizzare i summenzionati obiettivi? Ad esempio, nel caso dell'obiettivo 8 si deve puntare agli obblighi inerenti alla sicurezza nei luoghi di lavoro, affrontati dalla norma ISO 45001, poi abbiamo quelli relativi alla parità di genere a cui fa riferimenti la UNI/PdR 125:2022, e le organizzazioni se certificate potranno avvalersi di benefici fiscali che stabiliscono le norme in materia in quanto gli unici riconosciuti a livello nazionale mediante il Decreto del Presidente del Consiglio dei Ministri del 29 aprile 2022.

Nel caso invece dell'obiettivo 9, dovendo le imprese tenere conto della proprietà intellettuale, della ricerca e sviluppo, della collaborazione uomo-macchina e ulteriori aspetti di carattere tecnologico, per poter cristallizzare questi aspetti dovranno tenere conto, ad esempio, della norma ISO 56005 che fa riferimento alla proprietà intellettuale o alla norma di gestione dell'innovazione ISO 56002 in tema di intelligenza artificiale che ormai è entrata prepotentemente in tutti i settori.

Quanto citato sono solo alcuni esempi che però ci consentono di comprendere l'importanza della regolamentazione e della integrazione tra le norme per realizzare una corretta gestione della *compliance*, affinando la crescita dell'impresa sul piano della durata e della sostenibilità.

Alla base delle norme ISO c'è un linguaggio di alto livello noto come HLS, acronimo di *High Level Structure* ed è appunto un elemento comune a tutti i nuovi *standard* ISO affinché si realizzi un'adeguata interazione tra i sistemi di gestione integrati tra loro. Questo indica il fatto che tali *standard* sono conformi ad una struttura identica fondata sulla medesima terminologia, stessi testi, definizioni, titoli e sequenze.

Questa struttura di alto livello è stata introdotta dall'Organizzazione internazionale per la standardizzazione (ISO) proprio con l'intento di offrire ai sistemi di gestione una struttura univoca per migliorare l'integrazione e l'allineamento delle differenti norme ISO grazie ad una struttura di portata trasversale. Si può asserire che l'HLS funge da guida per l'emanazione anche di norme future stabilendo regole precise a cui uniformarsi nel tempo nel rispetto di requisiti specifici e definizioni di carattere comune.

Affinché si attui a pieno l'applicazione della norma ISO 37301 bisogna tenere in considerazione i punti essenziali, di seguito indicati, che la stessa dispone:

- Punto 5.3: Ruoli, responsabilità e autorità management. Il management deve essere il responsabile di riferimento alla *compliance* nelle aree di sua competenza e deve

cooperare e supportare la funzione di *compliance* e stimolare il personale a fare altrettanto; deve garantire che i propri sottoposti rispettino gli obblighi, le politiche, i processi e le procedure di *compliance*; deve identificare e comunicare i rischi di *compliance* nell'ambito delle proprie attività operative; deve integrare gli obblighi di *compliance* nella prassi e in tutte le procedure di *business* in cui esso opera; deve partecipare e supportare alla formazione in materia di *compliance*; deve sviluppare consapevolezza nel personale e fare in modo che tutti soddisfino i requisiti di formazione e competenza; deve indurre il proprio personale a trasmettere i flussi informativi ed eventuali segnalazioni impedendo forme di ritorsione; deve partecipare attivamente alla risoluzione di problematiche attinenti alla *compliance*; deve assicurare l'attuazione di eventuali azioni correttive laddove siano state raccomandate.

- Punto 4.5: Obblighi di *compliance*. L'organizzazione deve individuare gli obblighi di *compliance* che sono strettamente connesse alla propria attività e valutare da subito l'impatto sulla propria operatività. Per fare questo bisogna non solo identificare questi obblighi ma anche integrarli di volta in volta per garantire una *compliance* continuativa, deve valutare l'impatto dei cambiamenti e apportare, ove necessario, le modifiche negli obblighi di *compliance* dettagliando le informazioni che vanno debitamente documentate.
- Punto 4.6: Processo di valutazione dei rischi di *compliance*. L'azienda deve provvedere ad identificare e analizzare i propri rischi, ponderandoli sulla scorta del processo di valutazione dei rischi di *compliance*, mettendo in relazione i propri obblighi con le proprie attività operative. Bisogna però anche tenere conto dei rischi in ragione di quelli che sono i processi affidati all'esterno a soggetti terzi e il tutto va valutato periodicamente.
- Punto 8.1: Pianificazione e controlli operativi. L'organizzazione deve pianificare, attuare e tenere sotto controllo i requisiti richiesti per la *compliance*.
- Punto 8.2: Definizione di controlli e procedure. Fondamentali sono i controlli, come ben si accennava in precedenza, per gestire i propri obblighi di *compliance* e rischi correlati. I controlli vanno eseguiti costantemente e riesaminati sempre in maniera periodica e sottoposti a prova per garantirne l'efficacia.

- Punto 8.3: Far emergere le preoccupazioni. Questo implica che tutti i soggetti operanti entro l'organizzazione devono essere in grado di riportare eventuali violazioni, che siano meramente tentate, sospette o effettive. Per permettere ciò si dovrà comunque garantire la riservatezza, la visibilità e l'accessibilità del processo a tutti, accettare segnalazioni anche in forma anonima, proteggere chi "denuncia" la violazione da possibili ritorsioni e consentire al personale di ricevere la dovuta assistenza. Chiaramente per legittimare una tale prassi è sostanziale che l'azienda informi tutti delle modalità di *reporting* e dei diritti di tutela riconosciuti loro.
- Punto 9.1: Monitoraggio, misurazione, analisi e valutazione. L'organizzazione deve assicurare il monitoraggio continuo del sistema di gestione per la *compliance* al fine di garantire il perseguimento degli obiettivi, per farlo è indispensabile sviluppare e attuare degli indicatori appropriati che fungano da supporto. Vanno anche fissate delle precise regole per il *reporting* stabilendo delle scadenze entro le quali presentarli, fissare le modalità per permettere che i *reporting* siano accurati e completi di tutte le informazioni necessarie.
- Punto 5.1.2: Cultura della *compliance*. L'organizzazione deve sviluppare, mantenere e promuovere la cultura alla *compliance* a tutti i suoi livelli, in questo gioca un ruolo essenziale la *leadership* che deve attuare con impegno attivo e coerente uno *standard* di comportamento comune richiesto a tale scopo. L'alta direzione deve incoraggiare ogni tipo di condotta orientata a creare la *compliance* prevenendo e non tollerando azioni che invece possano mettere a repentaglio questa precisa finalità aziendale e organizzativa del sistema.

Alla base della norma c'è l'esistenza di un linguaggio di alto livello che impone ai sistemi di gestione sottoposti agli *standard* certificabili di essere dotati di una struttura fissata in dieci punti con contenuti e paragrafi comuni tra loro.

Pertanto, laddove ci sarà una condivisione della stessa HLS si avrà un documento strutturato in maniera identica che offrirà i seguenti titoli:

- Scopo e campo di applicazione;
- Riferimenti normativi;
- Termini e definizioni;
- Contesto dell'organizzazione;
- *Leadership*;

- Pianificazione;
- Supporto;
- Attività operative;
- Valutazione delle prestazioni;
- Miglioramento.

Bisogna ricordare che le regole su cui si fonda l'HLS sono state pubblicate per la prima volta nel 2012 tramite l'Allegato SL denominato "Approccio armonizzato alle norme di sistema di gestione", allegato relativo alle Direttive ISO/IEC; successivamente nel 2021 l'ISO ha pubblicato la revisione dell'Annex SL apportando all'HLS chiarimenti, integrazioni ma anche eliminando aspetti e contenuti ritenuti desueti.

Adottare una struttura organizzativa avanzata offre numerosi vantaggi evidenti.

Come discusso in precedenza, permette di implementare un sistema integrato di gestione con una maggiore qualità e sicurezza delle informazioni. Tuttavia, per ottenere questi benefici, è essenziale rispettare rigorosamente le regole.

In particolare, ciò implica: creare una struttura uniforme che faciliti la comprensione dello *standard* da parte di tutti gli utenti; standardizzare le procedure per materia, migliorando così l'integrazione e l'aggiornamento in modo efficiente e veloce; infine, avere un sistema integrato di gestione che semplifica notevolmente la conduzione di *audit*, sia interni che esterni all'organizzazione.

Si può quindi concludere sottolineando che le aziende che adottano un sistema di gestione integrato, basato su una struttura di alto livello, evitano problemi di duplicazione e interfaccia. Inoltre, riescono a ottenere una visione più ampia e sostenibile dei vari processi operativi.

Questo accade perché la combinazione della certificazione all'interno di un sistema integrato migliora l'approccio inter-tematico, individuando eventuali contraddizioni tra le diverse aree e permettendo di individuare tempestivamente le migliorie da implementare. Ciò consente ai modelli di *compliance* di fare riferimento ad una norma di portata internazionale, grazie alla quale è possibile ottenere la certificazione rilasciata da un organismo terzo.

Tra i contenuti fondamentali della norma, oltre alla *Leadership*, un ruolo fondamentale è svolto dalla pianificazione, che mira a individuare i rischi e le opportunità, affrontandoli

attraverso uno schema organizzativo che integra gli obiettivi di miglioramento in un programma unico, approvato dal *top management*.
Altro aspetto peculiare della ISO 37301 è dato dai processi di monitoraggio relativi all'avanzamento degli obiettivi di *compliance* e delle *performance*, tenendo conto dei *feedback* sulle prestazioni, riservando ampio spazio anche al processo di *auditing* interno che vede coinvolti sia l'organismo di governo che l'alta direzione.

2.3 Requisiti fondamentali per l'implementazione

Uno degli aspetti fondamentali della ISO 37301 è costituito dal successo nell'implementazione della certificazione nonostante i diversi fattori di rischio ad essa annessa quale ad esempio le difficoltà ad accogliere adeguatamente i cambiamenti o l'incapacità della *leadership* ad ottimizzare l'impegno.
Si ritiene infatti che allo stato attuale diverse aziende abbiano difficoltà nel gestire il pieno coinvolgimento della *leadership* durante il processo di implementazione e questo costituisce uno scoglio decisivo nell'attuare la politica fondata sulla conformità.
Inoltre, di solito, l'iter per ottenere la certificazione ISO 37301 si estende fino agli otto mesi, sempre che le risorse e il coinvolgimento dei soggetti interessati siano ottimali e alla base deve esserci anche un solido programma di conformità che funge da indirizzo per l'intera attività di certificazione.
Per poter attuare concretamente il piano di implementazione, è fondamentale l'impegno attivo delle aziende, che devono operare nel pieno rispetto della normativa vigente. Questo aspetto è particolarmente importante per i vertici dell'organizzazione, che devono non solo partecipare attivamente, ma anche supportare ogni iniziativa in questa direzione. Ciò implica l'attivazione di programmi di formazione adeguati e la messa a disposizione delle risorse necessarie per sostenere i dipendenti.
È importante sottolineare che i *feedback* più positivi provengono proprio da quegli enti che registrano i livelli di formazione più elevati e costanti.
Oltre a quanto sin qui detto è oltremodo fondamentale migliorare i sistemi di comunicazione di modo che ci siano costanti interlocuzioni tra le parti, onde facilitare la

risoluzione di eventuali problemi o la capacità di arginarne l'insorgenza, allineandosi agli obiettivi organizzativi.

Si ritiene che, in un prossimo futuro, la gestione della conformità ISO 37301 dovrà passare anche per altri canali come le nuove tecnologie, maggiore attenzione alla *privacy* dei dati e il rispetto verso la sostenibilità.

Questo induce a pensare oggi con maggiore attenzione e riguardo alla cura del processo di implementazione che deve operare a 360 gradi per non far trovare impreparate le aziende, e questo implica che le organizzazioni devono essere sempre pronte e informate.

Basti pensare che proprio la ISO 37301 mira a realizzare una cultura dell'integrità e un miglioramento della *governance*, tutto finalizzato a garantire una solida reputazione dell'ente sul mercato e una conseguente ottima reputazione.

Per la sua implementazione la ISO 37301 prevede principalmente quattro fasi di miglioramento: *Plan, Do, Check e Act*[15] (cosiddetto ciclo PDCA che implica la pianificazione, l'attuazione, il controllo e il miglioramento continuo del sistema di gestione) ma anche tutta una serie di requisiti che riguardano l'intera attività e, come si accennava precedentemente, le funzioni di responsabilità della *leadership*.

Infatti i programmi per questo processo prevedono sette principali punti segnalati e descritti dalla *U.S. Federal Sentencing Guidelines* (USSG), essi sono: *standards and procedures; governance, oversight and authority; due diligence in delegation of authority; communication and training; monitoring, auditing and reporting systems; incentives and enforcement; response to wrongdoing*[16].

Analizzare i summenzionati elementi è la base per comprendere la *compliance risk management* allo scopo di allineare i sistemi di gestione mediante una corretta analisi del

[15] Le tipiche attività di sviluppo del modello dovrebbero riguardare la pianificazione delle azioni di risposta ai rischi emersi a seguito dell'assessment e l'individuazione degli obiettivi e delle modalità per integrare i processi esistenti e la loro efficacia. A tale attività dovrebbe poi far seguito l'attuazione dei controlli sulle azioni di risposta (es. politiche operative, la previsione di un impianto sanzionatorio, la segregation of duty, l'attività di audit sui processi, l'attività di reporting tra le strutture di compliance, il management ed il board, un'attività di due diligence su terze parti in caso di affidamenti all'esterno), l'attività di monitoraggio (es: metodologie, periodicità, analisi dei risultati, flussi per l'invio di informazioni di ritorno da parte di tutti gli stakeholders e la loro classificazione etc.), l'attuazione dei controlli sulle azioni di risposta (es. politiche operative, la previsione di un impianto sanzionatorio, la segregation of duty, l'attività di audit sui processi, l'attività di reporting tra le strutture di compliance, il management ed il board, un'attività di due diligence su terze parti in caso di affidamenti all'esterno) e l'individuazione di azioni correttive appropriate agli effetti prodotti dalle non conformità e la previsione delle necessarie azioni di escalation successive al verificarsi dell'evento.

[16] Per approfondire, Compliance risk management: applying the COSO ERM framework.

contesto sia interno che esterno all'ente prima di procedere nella valutazione del rischio stesso.
Per favorire l'implementazione è decisivo fornire le linee guida e comprenderne bene il contenuto di modo che nell'organizzazione vengano individuate le persone più competenti a cui assegnare le responsabilità operative attinenti con un conseguente dimensionamento delle risorse disponibili.
Sostanzialmente per la sua implementazione la ISO 37301 deve poter fare riferimento ad una serie di regole precise, vediamo insieme quali sono:

1) Definizione degli obiettivi di conformità;
2) Analisi e valutazione dei rischi;
3) Implementazioni di controlli e procedure;
4) Coinvolgimento della *leadership*;
5) Formazione e sensibilizzazione del personale;
6) Monitoraggio e miglioramento costante;
7) Gestione dei cambiamenti.

Questa la sintesi di quanto si è descritto in precedenza partendo dal fatto che sia di vitale importanza prima di tutto inquadrare il sistema normativo a cui uniformarsi fissando obiettivi da realizzare per attuare concretamente quel ventaglio di obblighi a cui attenersi.
Non si può prescindere, inoltre, da un'analisi dei potenziali rischi di non conformità, da cui è necessario proteggersi attraverso lo sviluppo di strategie adeguate.
A ciò deve seguire l'attivazione di controlli rigorosi, supportati da procedure documentate, volte a garantire il rispetto dei requisiti normativi.
Fondamentale è il coinvolgimento attivo dei livelli più alti della direzione aziendale, che deve fornire risorse adeguate, promuovere la formazione del personale e assumersi le responsabilità necessarie per diffondere una vera e propria cultura della conformità all'interno dell'organizzazione.
Si è anche parlato della necessità di incentivare la formazione continua del personale affinché sia operativo e pienamente responsabile nell'esercitare le proprie funzioni all'interno dell'azienda ed infine indispensabile è anche guardare con occhio vigile ai costanti cambiamenti che intervengono sul mercato e nel settore di azione, comprese le

innovazioni normative, al fine di adeguare i sistemi di gestione ad ogni piccola peculiare novità.

2.4 Il processo di certificazione: attori, fasi e *output*

Il processo di certificazione prevede un *audit* di verifica da una parte terza, offrendo la possibilità alle aziende interessate di ottimizzare il controllo dei rischi di *compliance*.
Ad introduzione del presente paragrafo è bene comprendere il perché sia fondamentale ottenere la certificazione della ISO 37301:2021 e la risposta al quesito è data dal fatto che, mediante la suddetta certificazione, le aziende possono dotarsi di uno strumento altamente idoneo a minimizzare il rischio di commettere infrazioni con conseguenti danni reputazionali e di costi ulteriori da sostenere in conseguenza delle possibili sanzioni ex D. Lgs. 231/2001.
Il sistema di gestione oggetto di questa trattazione vuole migliorare, come più volte sottolineato, quelle che sono le opportunità di sostenibilità e di *business* delle organizzazioni che se ne avvalgono. Pertanto, ottenere la certificazione del sistema di gestione della *compliance* da parte di un organismo terzo rappresenta una sorta di "garanzia" per gli *stakeholders* in relazione alla gestione dei rischi mantenendo alti i livelli di fiducia e anche le aspettative.
Vediamo ora, più nel dettaglio, qual è l'iter di certificazione della norma ISO 37301, partendo proprio dal cosiddetto "*Audit* di certificazione".
Intanto dobbiamo precisare che, la norma in questione, mira ad utilizzare un sistema "progressivo" che tiene conto degli obblighi di *compliance* applicabili all'ente e questo porta a ragionare sul fatto che, inizialmente, la certificazione possa essere limitata ai soli processi aziendali che in qualche modo sono interessati nella gestione dei rischi di *compliance* in modo più rilevante.
Questi processi e questi rischi verranno selezionati ed evidenziati dall'organizzazione mediante il "*Compliance Risk Assessment*" [17] andando a indicare i seguenti punti di rilievo:

[17] Rif. UNI ISO 37031 par. 4.6; nello specifico il paragrafo 4.6 della norma UNI ISO 37301 riguarda il "Ruolo della leadership" e definisce i requisiti per la leadership e l'impegno dell'alta direzione nell'ambito

1) Individuando i rischi e le minacce legati alla mancata *compliance* e i processi aziendali più coinvolti;
2) Analizzando in che misura potranno verificarsi e quali effetti potranno avere sui processi aziendali i rischi intercettati;
3) Stabilendo per ogni tipo di rischio individuato la rilevanza dello stesso e nel contempo fissando i processi maggiormente coinvolti;
4) Definendo la portata applicativa della certificazione.

Sulla base di quanto emerge dal *compliance risk assessment* si potrà decidere, eventualmente, di procedere ad una progressiva certificazione. In questa ipotesi si presenterà al competente organo di controllo un programma di estensione dello scopo di certificazione ai diversi processi aziendali coinvolti, di modo che si raggiunga una copertura totale dei settori di *compliance*.
Nel momento in cui si individuano gli ambiti del o dei processi interessati da sottoporre a certificazione l'azienda dovrà, obbligatoriamente, provvedere a includere ogni aspetto relativo a quell'ambito (es. privacy, protezione dati, antiriciclaggio, security, etc.). Inoltre, il programma estensivo dovrà ovviamente essere validato dall'organo di controllo andando di volta in volta ad avviare una fitta rete di comunicazione qualora si proceda ad un progressivo ampliamento della portata della certificazione.
I soggetti coinvolti in questa fase sono tutti coloro che operano nei processi di *governance*/*legal* quali:

- addetti alla *governance* aziendale (CDA, ufficio legale, uffici che si occupano delle attività di *compliance*);
- soggetti coinvolti nel processo a cui si applica il sistema di gestione da certificare o già certificato;
- altri individui operanti in uffici o aree di produzione e aree di servizi aziendali.

In ultimo vanno ricordati in questa fase anche tutti gli addetti che offrono servizi di consulenza e collaborazione nell'azienda in modalità *outsourcing*.

---

del sistema di gestione della conformità. In sostanza, questo paragrafo sottolinea l'importanza che la direzione dimostri un forte impegno nel promuovere e sostenere la conformità all'interno dell'organizzazione.

Tutto ha inizio dapprima con una vera e propria richiesta di certificazione che l'azienda fa all'ente riconosciuto e che generalmente si conclude con la firma di un contratto, dopo aver esperito e chiarito gli aspetti economici del caso.

A questo momento segue un *audit* preliminare non obbligatorio ma utile ad esaminare il livello di preparazione del sistema di gestione che dev'essere certificato; trattandosi di una fase puramente volontaria non ne derivano obblighi per l'azienda ma semplici raccomandazioni che non vengono notificate in via ufficiale sul rapporto di *audit*.

Successivamente inizia il primo *audit* di certificazione, detto spesso *Stage 1* che si svolge nella sede aziendale. In questa fase viene esaminata la documentazione che riguarda le politiche e le procedure adottate dall'azienda, i documenti organizzativi e ogni altro dato previsto obbligatoriamente dalla legge.

Queste informazioni vengono raccolte insieme ai dati che riguardano il contesto operativo e servono principalmente ad evidenziare alcuni aspetti essenziali: l'esistenza di un sistema di gestione ISO 37301; la presenza di un sistema di monitoraggio interno e gestione delle azioni correttive; il rispetto delle leggi e dei regolamenti; l'avvio di un riesame da parte della Direzione.

L'organizzazione che richiede la certificazione all'organismo accreditato deve inoltre sottoporre all'esame di quest'ultimo tutta una serie di documenti che riguardano nello specifico: le politiche, le procedure ed eventuale manuale di gestione ISO 37301; l'organigramma funzionale e nominativo con la specifica della funzione di *compliance*; il documento di valutazione del rischio "*Compliance Risk Assessment*"; il raggio d'azione del sistema di gestione per la *compliance* indicando nel dettaglio siti, uffici e processi interessati; il programma di estensione della certificazione ad ogni altro ambito aziendale se applicabile; l'elenco dei documenti relativi al sistema ISO 37301.

L'importanza di questi documenti sta nel fatto che da essi è possibile stabilire se ci sono o meno le condizioni per il rispetto dei requisiti che sono la *condicio sine qua non* per proseguire nelle attività di certificazione.

Bisogna inoltre precisare che, una volta ottenuta la certificazione, questa dovrà necessariamente estendersi a tutti i siti, le filiali, le sedi secondarie del processo aziendale interessato dalla gestione dei rischi di *compliance* oggetto di certificazione non potendone quindi ridurre la portata applicativa.

Questo implica che, qualora l'organizzazione opti per una certificazione progressiva, il programma di estensione definito in sede iniziale dovrà essere seguito fedelmente, senza deviazioni rispetto a quanto approvato e validato dall'ente di certificazione prima del rilascio della certificazione stessa.

Segue l'*audit* di certificazione detto *Stage 2* durante il quale l'*auditor* verificherà che il sistema di gestione venga di fatto adottato dall'azienda.

Questo momento di monitoraggio servirà per stilare una relazione ove l'*auditor* eventualmente segnalerà tutto, principalmente il rispetto di tutte le regole prescritte al fine di poter presentare all'organo deliberante la richiesta ufficiale per l'emissione della certificazione ISO 37301.

È chiaro che, al contrario, se emergessero durante l'*audit* di certificazione delle carenze o negligenze, si procederà a richiedere tempestivamente l'intervento da parte degli organi addetti all'interno dell'azienda per implementare azioni correttive indispensabili per risolvere le criticità.

Ad ogni modo, conclusosi favorevolmente questo iter, si raggiungerà la tanto attesa delibera di certificazione emessa dall'ente accreditato che rilascerà la certificazione ISO valida tre anni.

La durata della certificazione non esime l'azienda dall'esecuzione dei controlli, l'azienda, tramite un sistema di gestione conforme, sarà infatti sottoposta annualmente a vigilanza e osservazione prevedendo *audit* di sorveglianza con cadenza puntuale. Il fatto che ci siano controlli periodici nei tre anni successivi alla certificazione sottolinea la volontà di attivare un sistema che persegue il miglioramento continuo.

In pratica, le verifiche annuali non servono solo a confermare la conformità alla norma ISO 37301, ma anche a verificare che il sistema di gestione della *compliance* continui a prevenire i rischi di illecito previsti dal D. Lgs. 231/2001, aggiornandosi in base alle nuove esigenze normative e operative.

Questo approccio permette di intervenire tempestivamente in caso di criticità, rafforzando la capacità dell'organizzazione di gestire i rischi di *non-compliance* e mantenendo elevati livelli di fiducia da parte degli *stakeholder*.

In ultimo si deve ricordare che, qualora si accerti una non-*compliance*, ovvero una non conformità[18], l'azienda dovrà prendere provvedimenti necessari per trattare la stessa, affrontandone le conseguenze e valutando la necessità di agire per eliminare prontamente le cause di non conformità acclarate mettendo in pratica tutte le misure idonee: riesaminando l'intero sistema, determinando le cause che l'hanno generata, applicando strategie *ad hoc,* esaminando l'eventuale efficacia di azioni correttive adottate.

2.5 Vantaggi e impatti concreti della certificazione per le aziende

"*La funzione di conformità svolge un ruolo di rilievo nella creazione di valore aziendale, attraverso il rafforzamento e la preservazione del buon nome (...) e della fiducia del pubblico nella sua correttezza operativa e gestionale (...). Il rischio di non conformità alle norme è il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazioni di norme imperative (di legge o di regolamenti) ovvero di autoregolamentazione (es. statuti, codici di condotta, codici di autodisciplina). Detto rischio è diffuso a tutti i livelli dell'organizzazione aziendale, soprattutto nell'ambito delle linee operative; l'attività di prevenzione deve svolgersi in primo luogo dove il rischio viene generato; è pertanto necessaria un'adeguata responsabilizzazione di tutto il personale* (…)[19]".

Con questo *incipit* si vuole introdurre quest'ultimo paragrafo dedicato all'importanza concreta per le aziende di ottenere la certificazione ISO 37301 e si può già chiaramente dedurre il senso di quanto fino ad ora descritto leggendo parte del comunicato di Banca d'Italia riguardo proprio alla conformità, comunicato pubblicato in Gazzetta Ufficiale nel luglio 2007. Dalla lettura del testo sopra riportato si evince che il *compliance risk* è esteso a tutti i livelli organizzativi dell'azienda, principalmente nell'ambito delle linee operative,

[18] Non conformità (*non conformity*): Mancato soddisfacimento di un requisito. Una non conformità non è necessariamente una non compliance. Non compliance (*non compliance*): non soddisfacimento di obblighi di compliance

[19] Disposizioni di vigilanza in materia di conformità compliance (GU Serie Generale n.172 del 26-07 2007); Banca d'Italia; https://www.gazzettaufficiale.it/eli/id/2007/07/26/07A06762/sg.

ciò implica che la prevenzione deve svolgersi intanto laddove il rischio si genera quindi è fondamentale prima di ogni altra cosa una massiccia responsabilizzazione del personale. Per comprendere il valore della conformità e della certificazione bisogna partire dai danni che invece l'ente potrebbe subire in assenza di tutto questo, considerando che la non conformità andrebbe a incidere negativamente non solo sull'esercizio dell'attività caratteristica dell'impresa (ad esempio l'attività di intermediazione), ma anche su aspetti trasversali di rilievo come la gestione dei conflitti di interesse e la trasparenza nei confronti della clientela.

Gestire il rischio in modo efficace ed efficiente prevede che i ruoli e le responsabilità vengano ben distinti e individuati in maniera chiara e formale, ci deve essere chi svolge nello specifico il compito di gestire il rischio di non conformità, così come all'interno dell'azienda deve essere individuato colui che assolve alla funzione di responsabile della conformità. Va anche predisposto un documento dove i compiti, le responsabilità, le modalità operative, i flussi informativi, la programmazione e i risultati dell'attività svolta dalla funzione di conformità vengano ben descritti e specificati.

Ottenere la certificazione alla norma ISO 37301 quindi, rappresenta per le aziende un importante traguardo perché le organizzazioni possano beneficiare di un insieme di vantaggi che sono:

1) gestione migliore dei rischi, in quanto si può facilitare l'identificazione del rischio di non conformità in maniera proattiva limitando il potenziale effetto negativo sulle operazioni aziendali;

2) concorrenza e reputazione, perché la certificazione rende più "credibile" l'azienda rafforzando la sua reputazione sul mercato e quindi agli occhi di partner commerciali, clienti e autorità di regolamentazione;

3) accesso e opportunità di mercato, in quanto la ISO 37301 offre la possibilità alle organizzazioni di prendere parte a gare d'appalto e ad ulteriori opportunità per le quali il mercato richiede una gestione ben solida della *compliance*;

4) efficienza operativa, favorendo l'ottimizzazione dei processi interni con conseguente riduzione dei costi di gestione collegati alla non conformità e accrescendo l'efficienza operativa complessiva;

5) responsabilità aziendale, poiché si incentiva l'impegno dell'azienda a mantenere una condotta aziendale in linea con i principi etici e di responsabilità.

Per un'azienda, avere un sistema di gestione per la *compliance* che sia solido e certificato è dunque un biglietto da visita molto importante perché permette di poter dimostrare la profusa attenzione verso le leggi, i regolamenti, i codici etici e codici di settore che, chiaramente, vanno a rafforzare quella efficienza sul mercato nei confronti di tutti gli operatori con i quali si interfaccia.

Un dato su cui fa molto leva l'intero sistema di *compliance* è rappresentato dalla *leadership*: un'organizzazione che vanta una solida direzione ha sicuramente un valore aggiunto perché è la *leadership* a dettare misure per promuovere un comportamento conforme e lo impone a tutti i livelli dell'ente di modo che il rischio di non-*compliance* si riduca al minimo.

Ormai per le aziende operare nel rispetto di una norma ISO 37301 debitamente certificata da un ente terzo rappresenta un *quid* indispensabile in quanto l'applicazione di valori vincolanti e avere una gestione appropriata della *compliance* favorisce l'integrità e porta ad una condotta socialmente responsabile di tutti gli operatori.

La certificazione ISO 37301 è un solido strumento che permette di prevenire e contrastare il riciclaggio di denaro ma anche la corruzione all'interno dell'azienda ad ogni livello, implementare la portata della norma inoltre porta a ridurre anche un maggior vantaggio competitivo.

Nella parte introduttiva della norma ISO 37301, al capitolo 1 si legge testualmente:

"*Un sistema di gestione per la compliance efficace, esteso a tutta l'organizzazione, permette di dimostrare il proprio impegno a conformarsi a leggi, requisiti regolamentari, codici di settore e specifiche organizzative (…) il presente documento specifica i requisiti e fornisce linee guida per istituire, sviluppare, attuare, mantenere e migliorare un efficace sistema di gestione per la compliance all'interno di un'organizzazione*"; quanto espresso nella norma in questione fa comprendere che la certificazione permette di evidenziare come l'azienda abbia operato, mettendo in atto tutte le procedure richieste, le istruzioni operative indispensabili per la *compliance*.

Ottenere la certificazione ISO 37301 significa quindi che il modello organizzativo impiegato dall'azienda non è solo un insieme astratto di procedure e di istruzioni ma è,

concretamente, uno strumento efficace e operativo nelle attività quotidiane dell'organizzazione esprimendo prova di solidità aziendale.

Riuscire ad ottenere la certificazione ISO 37301, per un'azienda, rappresenta un aspetto cruciale in quanto non basta aver predisposto un sistema di gestione ben organizzato ma è indispensabile essere appunto supportati da un organismo terzo di certificazione che, mediante l'*audit* e l'analisi dei singoli processi coinvolti, riesce a dimostrare che il modello organizzativo e il sistema di gestione è centrato, in linea con quanto prescritto, quindi concretamente funzionale.

Non dimentichiamo che ormai, sempre più spesso anche per le gare di pubblici appalti avere una certificazione delle norme ISO costituisce un elemento essenziale e anche se ancora non è un obbligo rimane di certo un elemento di prestigio e sicurezza. Basti ricordare che dall'Allegato II. 13 del nuovo codice degli appalti (D.lgs. 36/2023)[20] si evince come il possesso della certificazione ISO 37301:2021 consenta di ridurre l'importo della fidejussione di garanzia.

È bene infine ricordare che puntando alla certificazione si ha modo di intervenire a favore di tutte le organizzazioni, soprattutto quelle più complesse che vogliono realizzare una *compliance* come obiettivo a cui devono propendere tutti gli addetti ai lavori e non solo l'alta direzione poiché, come più volte detto: la *compliance* deve diventare una vera e propria "cultura" aziendale.

[20]Per una lettura completa, si rimanda al codice degli appalti, al seguente link: https://www.codiceappalti.it/DLGS_36_2023/Allegato_II_13_Certificazioni_o_marchi_rilevanti_ai_fini_della_riduzione_della_garanzia_/12903

CAPITOLO 3 - I RISVOLTI DELLA CERTIFICAZIONE ISO 37301 ALL'INTERNO DELLE ORGANIZZAZIONI

3.1 Inquadramento generale dell'azienda

Il caso oggetto di analisi riguarda una delle realtà più rilevanti e articolate del panorama economico italiano che opera da oltre 160 anni nei settori dei servizi postali, della logistica integrata, dei servizi finanziari, assicurativi e digitali, rappresentando una delle più grandi imprese multiservizio per fatturato, diffusione territoriale e numero di dipendenti.

L'ente in questione è un fornitore storico del servizio postale universale che ha gradualmente ampliato la sua missione istituzionale e commerciale e si è sviluppato in un gruppo industriale quotato in borsa, soggetto a *standard* di trasparenza, supervisione e governance simili a quelli applicati agli operatori sistemici.

L'attuale struttura legale può essere fatta risalire alla fine degli anni '90, quando ha subito il processo di trasformazione da ente economico pubblico a società per azioni (S.p.A.), come parte dei processi di riforma del servizio postale italiano e dei servizi pubblici. Ha progredito nel tempo, espandendosi in nuovi mercati e rafforzando i suoi segmenti di *business*, fino ad entrare nel segmento principale della Borsa Italiana nel 2015.

Lo sviluppo è stato di tale portata che la società è a maggioranza di proprietà del Ministero dell'Economia e delle Finanze, e vi è una partecipazione di minoranza negoziata al pubblico. Per quanto riguarda la sua organizzazione, il gruppo è articolato in diverse aree operative, corrispondenti ai principali settori di attività.

In particolare, il modello di *business* è strutturato attorno a quattro macro-divisioni: Servizi Corrispondenza, Pacchi e Distribuzione, che comprende la rete logistica e la gestione dei recapiti; Servizi Finanziari, che integra i servizi bancari, di investimento e gestione del risparmio; Servizi Assicurativi, con offerta di prodotti previdenziali, vita, infortuni e altri rami danni; e Servizi Pagamento e Mobile, dedicati a servizi digitali, carte, pagamenti elettronici e telefonia mobile. Tale struttura consente all'organizzazione di

coprire sinergicamente un intero spettro di mercati, promuovendo innovazione, inclusione e sostenibilità.

Sul piano dimensionale, la società rappresenta uno dei maggiori gruppi economici in Italia. I dati consolidati più recenti mostrano ricavi complessivi superiori ai 12,6 miliardi di euro, un utile netto in crescita e una redditività sostenuta in tutti i settori di riferimento. Al 2024, l'azienda conta oltre 120.000 dipendenti, confermandosi come uno dei maggiori datori di lavoro privati in Italia.

Altrettanto importante è la presenza territoriale: le 12.800 filiali della banca rappresentano una rete di prossimità fisica senza pari nell'ambiente italiano. Questa infrastruttura territorialmente intrecciata consente al gruppo di connettere quotidianamente milioni di cittadini, famiglie, aziende e amministrazioni pubbliche, oltre a svolgere un ruolo sociale e istituzionale chiave.

Sul piano patrimoniale e finanziario, il gruppo gestisce complessivamente circa 590 miliardi di euro in attività finanziarie per conto dei clienti (risparmi amministrati e gestiti) in prodotti bancari, di risparmio postale e assicurativi.

L'attuale portafoglio clienti ammonta a circa 45 milioni di clienti, cifra che conferma la centralità del gruppo nel sistema economico nazionale e la sua capacità di operare come infrastruttura strategica per l'erogazione di servizi essenziali.

Inoltre, l'azienda ha un ruolo chiave nel quadro ESG (*Environmental, Social, Governance*), come uno dei principali attori italiani nell'emissione di green bond e sponsor di progetti per la sostenibilità ambientale, l'inclusione sociale e la trasformazione digitale del Paese.

L'esistenza di un'organizzazione sistemica, con una diffusione capillare nel tessuto sociale nazionale e produttivo, con una natura settoriale diversificata (inclusi Banca d'Italia, IVASS, AGCOM, ARERA, AGCM, MEF, Consob e Garante per la *Privacy*) rende l'adozione di un modello di gestione della *compliance* integrata non solo auspicabile, ma necessaria.

In questo contesto, il gruppo ha investito negli ultimi anni nello sviluppo di un sistema di *compliance* moderno, conforme ai più elevati *standard* internazionali, con l'obiettivo di rafforzare i presidi di legalità e di integrità, garantire il rispetto delle normative applicabili e contribuire alla fiducia del mercato e degli *stakeholder*.

Va detto inoltre che, se da un lato l'organizzazione dell'azienda costituisce un punto fermo, è altrettanto vero che risulta fondamentale approfondire la struttura interna attraverso cui l'impresa presidia la correttezza, la trasparenza e l'efficacia della propria gestione. In tale ambito, il Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR) costituisce un elemento essenziale della *governance* aziendale, in quanto consente al Consiglio di Amministrazione di esercitare un'efficace direzione strategica, perseguendo la creazione di valore nel lungo termine e definendo la natura e il livello di rischio ritenuti compatibili con gli obiettivi strategici. Si può affermare che nell'ottica di un successo sostenibile, le valutazioni compiute da tale organo costituiscono elementi essenziali.

Il SCIGR è l'orchestrazione di regole, procedure, strumenti, sistemi informativi e schemi organizzativi progettati per rendere possibile la gestione delle attività secondo i principi di solidità, trasparenza e conformità al quadro legale vigente.

Esso garantisce una chiara attribuzione di ruoli, compiti e responsabilità tra i vari soggetti coinvolti, promuovendo un processo continuo di identificazione, valutazione, gestione e monitoraggio dei rischi, supportato da flussi informativi efficaci e tempestivi, indispensabili per una *governance* consapevole.

Particolare attenzione è riservata all'integrazione dei principi ESG *(Environmental, Social and Governance*) nelle strategie aziendali, nella gestione dei rischi e nelle politiche di incentivazione, in coerenza con le principali *leading practice* internazionali.

Il sistema mira, pertanto, al raggiungimento del successo sostenibile dell'organizzazione, anche attraverso la definizione di responsabilità specifiche in ambito ESG, la strutturazione dei flussi informativi interni ed esterni, e l'adozione di modalità strutturate di gestione dei rischi correlati.

Per sostenere tale approccio, l'impresa promuove anche un dialogo attivo con gli *stakeholder* rilevanti, volto a garantire un confronto trasparente e costante sulle strategie aziendali e sul loro grado di attuazione.

In conformità alla normativa di settore e alle *best practice* di riferimento, il SCIGR si articola su tre livelli di controllo, ognuno dei quali presidia specifici aspetti del sistema e contribuisce, in maniera coordinata, alla sua efficacia complessiva.

- Il primo livello di controllo è rappresentato dalle funzioni operative e di linea, le quali sono direttamente responsabili dell'identificazione, valutazione, gestione e monitoraggio dei rischi connessi alle attività di competenza. Tali funzioni attuano

interventi di mitigazione volti ad assicurare il corretto svolgimento delle operazioni aziendali.

- Il secondo livello di controllo comprende le funzioni preposte al controllo dei rischi e alla conformità normativa, le quali definiscono i modelli di gestione del rischio, svolgono attività di monitoraggio continuo e verificano l'efficienza e l'efficacia del sistema di controllo. Esse operano in modo autonomo rispetto alle funzioni operative, contribuendo all'integrazione del sistema e garantendo la coerenza con leggi, regolamenti e disposizioni interne.
- Il terzo livello di controllo è affidato alla funzione di *audit* interno, la quale svolge una valutazione indipendente sull'adeguatezza, sull'effettiva operatività e sull'affidabilità dei primi due livelli, nonché dell'intero SCIGR. Tale presidio ha il compito di fornire *assurance* al vertice aziendale, individuando eventuali criticità, violazioni o aree di miglioramento, e contribuendo in modo significativo al rafforzamento del sistema di controllo interno e alla promozione di una cultura del rischio diffusa e consapevole.

All'interno della struttura di *governance*, il Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR) si sviluppa attraverso l'azione coordinata di diversi organi e funzioni, ciascuno con compiti specifici.

Il Consiglio di Amministrazione ha un ruolo di indirizzo strategico in quanto definisce le linee guida del sistema, verificandone periodicamente l'efficacia e l'adeguatezza, e approvando il piano di audit annuale. Identifica, monitora e gestisce tutti i rischi significativi, inclusi i rischi di sostenibilità, promuove un dialogo con gli *stakeholder* e assicura l'interazione tra le funzioni di controllo.

A supporto del Consiglio di Amministrazione opera il Comitato Controllo e Rischi, che svolge funzioni istruttorie, propositive e consultive.

Tale organo valuta l'adeguatezza complessiva del sistema, esamina le informative periodiche e fornisce pareri sulle nomine delle figure preposte alla gestione del rischio e alla revisione interna. Collabora inoltre alla definizione della propensione al rischio, anche con riferimento ai rischi climatici, attraverso l'impostazione del *Risk Appetite Framework*.

Accanto al Comitato Controllo e Rischi si trova il Comitato Sostenibilità che supporta il Consiglio di Amministrazione nella definizione delle strategie relative a fattori

ambientali, sociali e di *governance*. Incoraggia anche l'integrazione delle best practice di sostenibilità con il modello di *business*, valuta il rischio ESG, supporta la strategia ambientale, analizza il bilancio integrato per verificarne coerenza e completezza e lavora con il Comitato Controllo e Rischi in relazione al rischio climatico.

L'Amministratore Delegato è responsabile dell'attuazione operativa del SCIGR, garantendone l'allineamento alle direttive del Consiglio di Amministrazione e intervenendo per individuare, monitorare e gestire i principali rischi. Può disporre verifiche mirate e propone la nomina di figure chiave per le funzioni di controllo, contabilità e antiriciclaggio.

A supportarlo vi è il Direttore Generale, che coordina le strutture operative e assicura l'integrazione tra gli aspetti legali, societari, fiscali, di *governance* e sostenibilità, rafforzando i processi di *Risk Management* e *Compliance*.

Il Collegio Sindacale vigila sul rispetto di leggi, regolamenti e statuto, verificando la correttezza dell'assetto organizzativo e contabile, nonché l'efficacia del SCIGR e dei flussi informativi tra gli organi coinvolti. Formula pareri su nomine strategiche e segnala eventuali irregolarità alle autorità competenti.

Infine, l'Organismo di Vigilanza garantisce l'efficace applicazione del Modello 231, monitorando le attività a rischio e proponendo eventuali aggiornamenti. Assicura l'allineamento dei modelli adottati dalle società controllate con le linee guida della Capogruppo, e riferisce periodicamente ai vertici aziendali, e può essere anche convocato in situazioni specifiche.

Nell'ottica dell'attuazione di uno schema di *governance* coerente e funzionale al presidio del rischio, il Sistema di Controllo Interno e di Gestione dei Rischi si struttura secondo tre distinti livelli di controllo, noti nella letteratura di settore come il modello delle 'tre linee di difesa'.

Il primo livello di controllo è affidato ai *risk owner*, ovvero ai responsabili delle unità operative e gestionali che, nello svolgimento delle proprie attività, hanno la diretta titolarità dei rischi. Questi sono responsabili dell'identificazione, valutazione, monitoraggio e gestione dei rischi in linea con gli obiettivi aziendali, le politiche di gestione del rischio e le procedure interne applicabili. Il loro compito è fondamentale poiché garantiscono che i rischi siano presidiati sin dalla fase operativa, integrando la cultura del controllo nel *day-by-day* aziendale.

Una particolare articolazione di questa linea è rappresentata da una funzione incaricata della gestione di un patrimonio separato, il cui responsabile opera con poteri delegati dal vertice aziendale. Tale figura, in qualità di *risk owner* nell'ambito delle attività di sua competenza, assicura l'attuazione delle politiche di governo del rischio definite dagli organi societari, monitora l'efficacia del sistema di controllo interno e propone eventuali interventi correttivi in caso di scostamenti rispetto al profilo di rischio atteso.

Inoltre, il primo livello di controllo assicura un flusso costante di informazioni verso le funzioni di controllo di secondo e terzo livello, garantendo la trasparenza nella gestione dei fattori di rischio e la tracciabilità dei processi. In coordinamento con le funzioni aziendali competenti, i *risk owner* collaborano all'adeguamento dei presidi di controllo in risposta a evoluzioni normative, organizzative o operative, contribuendo così alla resilienza complessiva del sistema.

Il secondo livello di controllo è composto da quelle funzioni aziendali che, pur non svolgendo attività operative dirette, hanno il compito di monitorare l'adeguatezza dei controlli posti in essere dalla prima linea e di assicurare che i principali rischi aziendali siano correttamente identificati, valutati e gestiti. Queste funzioni forniscono le linee guida per i sistemi di controllo e vigilano sulla loro efficacia, contribuendo così all'efficienza operativa, alla prudenza nella conduzione del *business* e alla conformità normativa dell'intera organizzazione. Esse sostengono il vertice aziendale nella definizione e attuazione dei processi di gestione dei rischi e di *compliance*, nonché nella definizione degli obiettivi di sostenibilità, garantendo un governo unitario su tematiche trasversali di natura legale, fiscale, societaria e di *corporate governance*.

Tra queste funzioni, la funzione *Risk & Compliance* di Gruppo ricopre una posizione di particolare rilievo. Essa rappresenta il presidio centrale per il governo e la gestione dei rischi, non solo in termini finanziari, ma anche sotto il profilo della *compliance* normativa e della sostenibilità.

Questa funzione coordina l'intero sistema di controllo di secondo livello, servendosi di unità specialistiche di rischio e *compliance* poste sotto la propria responsabilità diretta, così come dei presidi di rischio indiretti presenti nelle società del Gruppo. Si occupa della definizione delle politiche, degli strumenti e delle metodologie *standard* per ciascuna categoria di rischio, assicurando così un approccio integrato e coerente su tutto il perimetro aziendale.

La funzione *Risk & Compliance* assume un ruolo attivo anche nella definizione della propensione al rischio da parte del vertice aziendale e nella valutazione della compatibilità tra i rischi assunti e gli obiettivi strategici. Inoltre, grazie ad un costante flusso informativo, garantisce che gli organi societari abbiano piena visibilità sul profilo di rischio del Gruppo e sull'efficacia dei presidi implementati.

Questa funzione è supportata da numerose unità specialistiche dedicate alla gestione di rischi specifici, quali i rischi operativi, reputazionali, ESG, di frode, di controparte e di conformità alla normativa 231, nonché dai presidi dedicati alla gestione dei sistemi di controllo integrati. Coopera anche con la funzione dedicata allo sviluppo sostenibile, al fine di integrare i rischi ESG nel processo di doppia materialità e garantire un approccio olistico alla gestione del rischio. Tale funzione è efficace perché garantita anche da un assetto organizzativo che ne tutela l'indipendenza e l'autorevolezza, con riporto diretto al vertice aziendale e relazioni funzionali con il Consiglio di Amministrazione.

Accanto alla funzione *Risk & Compliance*, operano altri presidi di secondo livello che si occupano di ambiti specifici.

La funzione dedicata allo sviluppo sostenibile coordina l'elaborazione della strategia ESG, garantendo la coerenza dei processi e degli strumenti di sostenibilità e supportando la rendicontazione non finanziaria.

Il responsabile di questa funzione ricopre anche il ruolo formale di Dirigente Preposto alla redazione della rendicontazione di sostenibilità, attestandone la conformità agli *standard* europei. La funzione antiriciclaggio assicura che tutte le società del Gruppo rispettino la normativa in materia di prevenzione del riciclaggio e del finanziamento del terrorismo, attraverso un presidio centrale e una rete di referenti nelle singole entità. Essa è supportata da un esponente del Consiglio di Amministrazione con responsabilità specifiche in materia, a conferma dell'importanza strategica di questo ambito.

La conformità alle normative in materia di concorrenza e tutela del consumatore è invece affidata a un responsabile del relativo programma di *compliance*, che organizza le attività delle diverse società del Gruppo e fornisce supporto specialistico, operando in sinergia con la funzione *Risk & Compliance*. La sicurezza informatica è presidiata da una funzione specifica che, in collaborazione con il CERT aziendale, presidia la *cybersecurity*, la protezione delle informazioni e la gestione della *business continuity*, assicurando la resilienza dell'infrastruttura digitale e la conformità alle normative di settore. La funzione

Privacy garantisce l'osservanza della normativa in materia di protezione dei dati personali e monitora l'attuazione delle misure previste dal GDPR.

La rendicontazione finanziaria è invece presidiata dal Dirigente Preposto che ha la responsabilità di attestare la correttezza e l'affidabilità dei dati contabili e finanziari, svolgendo un ruolo di controllo sui processi amministrativo-contabili.

Infine, la funzione fiscale garantisce la corretta gestione dei rischi fiscali, attraverso la definizione di procedure interne, l'adozione di modelli di valutazione del rischio e la predisposizione di una relazione annuale sul rischio fiscale da sottoporre sia al Consiglio di Amministrazione che all'Agenzia delle Entrate, nell'ambito del regime di adempimento collaborativo. Tutti questi ambiti interagiscono e condividono le informazioni con la funzione *Risk & Compliance* per assicurare una visione integrata, omogenea e coordinata dei rischi a livello consolidato.

La terza linea di controllo del sistema di controllo interno e gestione dei rischi dell'organizzazione è costituita dalle funzioni di *internal auditing* indipendenti. Esse sono incaricate di fornire un'*assurance* imparziale sull'adeguatezza e sull'effettiva operatività dei controlli di primo e secondo livello, nonché sul complessivo funzionamento dello SCIGR. In particolare, questo livello di controllo è affidato a due strutture distinte ma coordinate: la Funzione di Controllo Interno della capogruppo (*Internal Audit*) e la funzione di Revisione Interna dedicata al settore bancario della società. Entrambe agiscono in modo indipendente rispetto al *management* aziendale, assicurando in tal modo obiettività di giudizio e autonomia di azione nel processo di verifica.

A livello di Gruppo la Funzione di Controllo Interno svolge verifiche estese su processi e attività di tutte le aree aziendali, con l'obiettivo di valutare periodicamente l'adeguatezza del disegno dei controlli e la loro effettiva applicazione. In virtù di tali *audit*, vengono individuati eventuali carenze o aree di miglioramento nei presidi esistenti e vengono formulate raccomandazioni per le opportune azioni correttive. L'attività di *audit* viene pianificata mediante un programma (piano di *audit* annuale o pluriennale) predisposto dal Responsabile della Funzione di Controllo Interno e approvato dal Consiglio di Amministrazione almeno una volta all'anno. Inoltre, la funzione predispone relazioni periodiche sullo stato di adeguatezza del sistema dei controlli interni, le quali sono esaminate dagli organi apicali in modo da permettere al vertice di monitorare costantemente la robustezza complessiva del SCIGR.

La funzione di Revisione Interna dedicata al comparto bancario dell'azienda svolge compiti analoghi, ma con focalizzazione sulle attività finanziarie e sui servizi sottoposti a vigilanza regolamentare.

Essa elabora un proprio piano di *audit* per l'ambito bancario, che viene esaminato e approvato dal Consiglio di Amministrazione con il supporto del Comitato Controllo e Rischi, in parallelo al piano dell'*audit* di Gruppo.

La Revisione Interna del settore bancario verifica in maniera indipendente l'adeguatezza dei presidi di rischio e di conformità relativi alle operazioni finanziarie, assicurando che i processi chiave rispettino gli *standard* normativi e le politiche di gestione dei rischi dell'ente.

Ad esempio, il rapporto annuale sul processo interno di valutazione dell'adeguatezza patrimoniale (ICAAP) e la relativa relazione di *audit* predisposta su tale processo vengono sottoposti a un esame dedicato da parte del Comitato Controllo e Rischi prima della presentazione al Consiglio di Amministrazione. I risultati di tali verifiche svolte in questo perimetro vengono poi riportate agli organi di governo competenti, offrendo al Consiglio una visione chiara del livello di affidabilità ed efficacia del sistema di controlli interni anche per il settore bancario.

Vi è una stretta interazione tra le funzioni di *audit* del terzo livello, sulla base di un chiaro assetto di competenze che evita sovrapposizioni e sfrutta possibili sinergie nei controlli.

La normativa interna, in linea con le disposizioni delle Autorità di Vigilanza, prevede infatti la definizione puntuale dei compiti e delle responsabilità di ciascun organo e funzione di controllo, nonché dei flussi informativi reciproci. Sono altresì stabilite le modalità di coordinamento e collaborazione tra le diverse funzioni di controllo qualora vi siano ambiti di potenziale sovrapposizione, così da garantire un'azione di controllo integrata ed efficiente. In sostanza, la Funzione di Controllo Interno e la Revisione Interna del comparto bancario condividono metodologie e risultati rilevanti delle rispettive attività di verifica, assicurando una copertura completa di tutti i rischi aziendali senza duplicazioni inutili.

La *governance* societaria rafforza l'indipendenza e l'efficacia di queste funzioni di controllo di terzo livello attraverso una supervisione diretta da parte degli organi di vertice. In particolare, il Comitato Controllo e Rischi (CCR) svolge un ruolo di monitoraggio attivo: verifica l'autonomia, l'adeguatezza, l'efficacia e l'efficienza della

Funzione di Controllo Interno, esaminandone le relazioni periodiche sulla valutazione del sistema dei controlli, e riferisce al Consiglio di Amministrazione, con cadenza almeno semestrale, in merito all'attività svolta e allo stato di adeguatezza del SCIGR.

Inoltre, il CCR può richiedere alla Funzione di Controllo Interno di effettuare *audit* mirati su specifiche aree operative o su determinati processi aziendali, qualora emergano esigenze di approfondimento indipendente su potenziali criticità.

In merito alle funzioni di controllo del settore bancario, il Comitato rilascia un parere preventivo obbligatorio sulla nomina (o l'eventuale revoca) dei rispettivi responsabili (incluso il responsabile della Revisione Interna della divisione bancaria) e si esprime sull'adeguatezza delle risorse loro assegnate per lo svolgimento dei compiti.

Attraverso tali prerogative, il CCR garantisce che le strutture di *audit* dispongano di professionalità e mezzi adeguati e che la loro azione rimanga imparziale rispetto al *management* operativo.

Anche il Consiglio di Amministrazione interviene direttamente sulla gestione delle funzioni di *audit* interno, tutelando la loro autonomia. Su proposta del CCR e con il parere favorevole del Collegio Sindacale, il Consiglio di Amministrazione approva almeno annualmente il piano di *audit* predisposto dalla Funzione di Controllo Interno e delibera in merito alla nomina o all'eventuale revoca del relativo Responsabile.

Nell'ambito di tali decisioni, il Consiglio di Amministrazione valuta attentamente anche l'adeguatezza delle risorse e dei mezzi assegnati alla funzione, così da assicurarne l'efficacia operativa e la piena indipendenza di giudizio. Meccanismi analoghi di nomina, valutazione e garanzia dell'indipendenza sono applicati anche alla funzione di Revisione Interna operante sul perimetro bancario, in modo da assicurare un pari livello di rigore e autonomia organizzativa in entrambe le articolazioni del terzo livello di controllo.

Grazie a questa struttura duale del controllo di terzo livello, l'organizzazione sviluppa un monitoraggio indipendente e capillare del proprio sistema di controllo e gestione dei rischi, sia nelle attività ordinarie sia nelle operazioni bancarie specializzate.

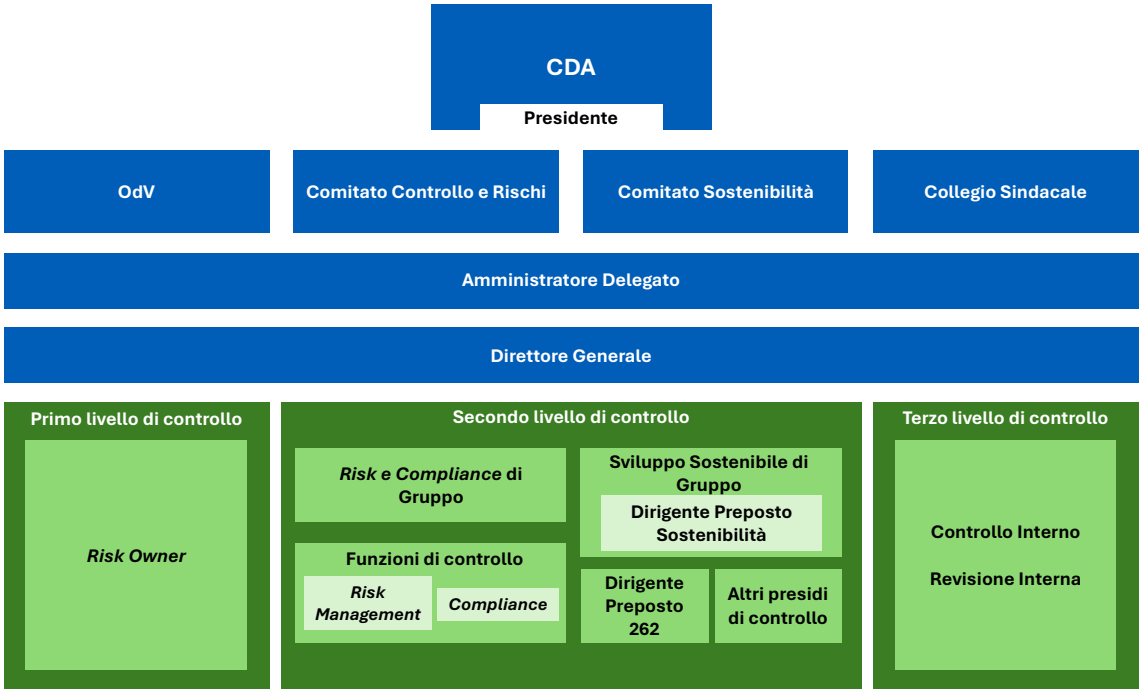
Le verifiche svolte dalle funzioni di *audit* interno permettono di far emergere tempestivamente eventuali punti di debolezza nei processi aziendali o violazioni di normative e procedure, portandoli all'attenzione degli organi di governo insieme a raccomandazioni su possibili azioni correttive.

Questo flusso informativo risulta fondamentale per la continua evoluzione e il rafforzamento del SCIGR, poiché consente al vertice di intervenire in maniera mirata sulle criticità identificate e di promuovere un miglioramento sistematico dei presidi di controllo.

Di conseguenza, le due funzioni svolgono un ruolo indispensabili nel garantire l'efficacia complessiva del sistema di controllo, complementando i controlli operativi di primo livello e le attività di monitoraggio specialistico di secondo livello.

Nella figura 1 si riporta la vista di sintesi degli attori del SCIGR.

Figura 1 – Struttura del SCIGR



Fonte: rielaborazione personale dell'autore, anno 2025

3.2 Il Modello di *Compliance* Integrata: struttura, ruoli e responsabilità

L'evoluzione del quadro normativo e la crescente complessità delle attività aziendali, distribuite in molteplici settori di *business*, hanno spinto il Gruppo ad adottare progressivamente un insieme di presidi specialistici per ciascun ambito di conformità.

Già prima dell'introduzione di un modello unitario, l'organizzazione disponeva di controlli consolidati in aree quali la responsabilità amministrativa degli enti, la prevenzione della corruzione, la salute e sicurezza sul lavoro, la protezione dei dati personali, la tutela del consumatore, la conformità in materia di *import-export* e la gestione della *compliance*.

Lo sviluppo nel tempo di questi strumenti ha garantito controlli efficaci, coerenti e trasparenti nel rispetto delle norme lungo l'intera catena del valore.

Volendo rafforzare ulteriormente il Sistema di Controllo Interno e di Gestione dei Rischi e di rendere più efficienti i presidi di *governance*, l'azienda ha avviato un processo di *compliance* integrata a livello di gruppo che si fonda sulla combinazione di due direttrici fondamentali.

La prima è l'approccio misto, che prevede l'esistenza di un presidio centrale e di presidi specialistici per ciascun ambito normativo, con una chiara definizione di ruoli e responsabilità all'interno del contesto professionale della *compliance*.

Questa impostazione permette di rafforzare il coordinamento e la collaborazione tra i diversi attori coinvolti nella gestione dei rischi di non conformità.

La seconda direttrice è l'approccio *multicompliance*, ideato per affrontare in modo unitario e integrato la crescente complessità degli adempimenti legislativi e regolamentari.

Attraverso tale approccio, si promuovono sinergie tra i presidi degli specifici ambiti normativi riducendo al tempo stesso le ridondanze operative tra i vari modelli di gestione dei rischi e i programmi di *compliance* settoriali, quali, ad esempio, il programma per la tutela della concorrenza e del consumatore, il sistema di gestione integrato comprensivo del presidio anticorruzione, il sistema di gestione e controllo del rischio fiscale nel regime di adempimento collaborativo, il sistema di controllo interno sull'informativa finanziaria e il modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001.

Il modello di *compliance* integrata è stato definito a seguito di un approfondito *assessment* dei presidi e dei modelli di *compliance* già presenti nel Gruppo, con l'obiettivo di unirli in un unico quadro di riferimento strutturato e coerente.

Questa impostazione ha permesso di superare la frammentazione a *silos* e di adottare una visione unitaria della conformità normativa, ponendo le basi per l'ottenimento della

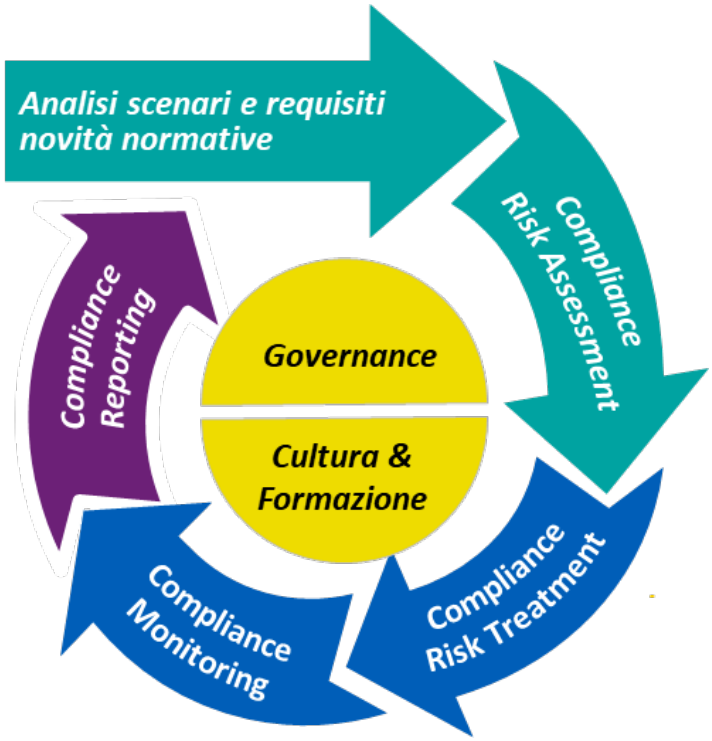
certificazione ISO 37301, che dimostra l'adesione dell'organizzazione ai principi internazionali di integrità, trasparenza e gestione efficace dei rischi di non conformità.

Dopo aver delineato i principi e la struttura del modello di *compliance* integrata, è opportuno soffermarsi sulle fasi operative, che costituiscono un ciclo costante attraverso il quale l'organizzazione assicura la conformità normativa e una gestione efficace dei rischi di non conformità.

Questo processo, sostenuto in maniera trasversale dai pilastri della *Governance*, della Cultura e della Formazione, si articola in una sequenza logica di passaggi interconnessi che assicurano un approccio proattivo e integrato alla *compliance*, in linea con l'evoluzione dello scenario normativo e operativo.

Nella Figura 2 riportata di seguito è possibile osservare le principali fasi del processo di *compliance* integrata dell'azienda.

Figura 2 – Processo di *compliance* integrata



Fonte: rielaborazione personale dell'autore, anno 2025

In primo luogo, viene condotta un'attenta analisi degli scenari evolutivi sul piano normativo e regolamentare.

La Società monitora costantemente il contesto esterno, seguendo l'agenda legislativa nazionale e internazionale, le iniziative dei regolatori e le novità normative in itinere, così da individuare tempestivamente eventuali nuovi obblighi in via di introduzione (proposte di legge, schemi di decreti, direttive europee, documenti di consultazione, etc.) e intercettare anche provvedimenti immediatamente vincolanti emanati d'urgenza (come decreti-legge) ancor prima della loro eventuale conversione o attuazione.

Questo monitoraggio proattivo consente all'Organizzazione di valutare il potenziale impatto dei cambiamenti normativi sul proprio *business* e definire la posizione aziendale da assumere: vengono analizzati gli interessi del Gruppo rispetto alle nuove regole proposte e, quando opportuno, si elaborano osservazioni o richieste di modifica da sottoporre agli organi legislativi o alle autorità (anche attraverso *benchmark,* studi di settore e altri documenti che evidenzino le esigenze strategiche dell'azienda).

Una volta che le nuove norme vengono emanate in forma definitiva ed entrano in vigore, si passa a esaminare nel dettaglio i requisiti normativi: per ogni nuova disposizione viene verificata l'applicabilità alle attività e ai processi aziendali, valutandone l'impatto secondo una metodologia predefinita.

Contestualmente, le funzioni competenti avviano un'istruttoria interna per recepire i nuovi requisiti, predisponendo piani di adeguamento e intervento affinché la Società si conformi alle norme sopravvenute.

Questi piani vengono attuati tempestivamente e ne viene monitorato l'avanzamento, in modo da garantire che ogni prescrizione sia effettivamente integrata nelle procedure operative aziendali nei tempi fissati.

Una volta recepite le novità esterne, si passa alla fase di *Compliance Risk Assessment*, nella quale vengono identificati, valutati e analizzati i rischi di non conformità rilevanti per l'organizzazione.

Il processo di valutazione del rischio di *compliance* si svolge sia contestualmente all'entrata in vigore di nuove normative (come parte dell'analisi di impatto sopra descritta), sia attraverso verifiche periodiche pianificate o attivate ad evento in caso di cambiamenti significativi nel contesto operativo. L'azienda inizia a mappare tutti i potenziali eventi di non conformità nei vari ambiti normativi applicabili e, per ciascuno,

ne stima la gravità e la probabilità in assenza di controlli (il *rischio inerente*). Successivamente vengono analizzati i presidi di controllo esistenti e la loro capacità di mitigare quei rischi: confrontando il rischio inerente con l'efficacia delle misure di controllo che sono state introdotte, si determina pertanto il *rischio residuo*, ovvero il livello di rischio che permane per la Società dopo l'applicazione dei controlli esistenti. Sulla base di questa analisi, i rischi di non conformità vengono classificati in base alla loro rilevanza, evidenziando quelli più elevati che richiedono interventi correttivi o una sorveglianza più intensa.

Il *Compliance Risk Assessment* consente infatti di individuare eventuali carenze o aree di miglioramento nel sistema di controllo: ad esempio, in presenza di rischi residui non del tutto accettabili, si potranno progettare nuovi controlli o potenziare quelli esistenti, ottimizzando il complessivo assetto di *governance* del rischio di *compliance*.

L'intero processo avviene secondo un rigoroso approccio *risk-based*, allocando le risorse e gli sforzi in misura proporzionale alla criticità dei rischi individuati. Ciò consente di focalizzare l'attenzione sugli ambiti più esposti e prevenire in maniera prioritaria le violazioni più gravi o probabili.

Sulla base dei risultati emersi dal *risk assessment*, il modello passa al trattamento dei rischi di non conformità.

In questa fase si definiscono e implementano le misure di presidio necessarie per mitigare i rischi identificati. Per ciascun rischio rilevante vengono stabilite delle azioni correttive e controlli specifici *ad hoc*, secondo *standard* metodologici uniformi a livello di Gruppo, in modo da garantire un presidio omogeneo su tutte le aree aziendali. L'attuazione concreta di questi presidi spetta ai *Process Owner*, ossia ai responsabili di processo e delle unità operative di primo livello, i quali sono tenuti a integrare le misure di controllo nei processi di loro competenza e a gestirle operativamente, assicurando il rispetto delle normative nel lavoro quotidiano.

La funzione centrale di *Compliance* integrata, insieme ai vari *Compliance Specialist* (figure di secondo livello specializzate sui diversi ambiti normativi), svolge un ruolo di coordinamento e supporto in questa fase: essa fornisce linee guida, metodologie e strumenti per l'attuazione dei controlli, e garantisce una congiunzione tra le diverse funzioni coinvolte affinché le soluzioni adottate siano coerenti con la strategia di *compliance* aziendale. Inoltre, la funzione di *compliance*, grazie al suo punto di vista

trasversale, monitora l'efficacia del trattamento del rischio e interviene in caso di criticità: se emergono controlli non efficaci, vulnerabilità o nuove problematiche, i *Compliance Specialist* affiancano i responsabili operativi nell'individuare le cause del problema e nel definire ulteriori interventi correttivi.

La finalità principale del trattamento dei rischi è di ridurre il livello di esposizione a ciascun rischio di non conformità entro soglie accettabili per l'organizzazione, assicurando che per ogni rischio significativo esistano adeguati controlli o misure mitigative effettivamente funzionanti.

Un elemento fondamentale del modello è il monitoraggio continuo dei rischi di *compliance* e dei controlli attuati. Dopo (e durante) l'implementazione delle misure di trattamento, la Società inizia una serie di attività di controllo di secondo livello volte a verificare nel tempo l'evoluzione del profilo di rischio e l'adeguatezza dei presidi posti a tutela della conformità.

Questo monitoraggio si basa su indicatori chiave predisposti *ad hoc* e alimentati dai flussi informativi interni: vengono raccolti dati e segnali provenienti dalle diverse funzioni aziendali, dai sistemi di segnalazione e dalle verifiche periodiche, in modo da far emergere tempestivamente eventuali fattori di criticità.

Attraverso specifici *Key Risk Indicator* (KRI) sul manifestarsi dei rischi e *Key Control Indicator* (KCI) sul funzionamento dei controlli, il *team* di *compliance* può rilevare anomalie, violazioni o *trend* sfavorevoli prima che si traducano in problemi maggiori. Ad esempio, un aumento di segnalazioni di non conformità in un certo ambito, oppure il ripetersi di incidenti operativi nonostante i controlli esistenti, rappresentano allarmi che il monitoraggio è in grado di cogliere.

Questo monitoraggio, oltre a fotografare lo stato di salute del sistema di controllo, verifica anche l'attuazione delle misure correttive pianificate: controlla che gli interventi decisi nella fase di trattamento (come nuovi controlli o attività formative) siano stati effettivamente eseguiti nei tempi previsti e che abbiano risolto le criticità iniziali.

Ne consegue che, grazie a un monitoraggio strutturato e continuo, il modello di *compliance* integrata mantiene una sorveglianza attiva sull'aderenza dell'azienda alle norme, garantendo una rapida risposta di fronte a cambiamenti o incidenti e alimentando il flusso informativo necessario per le decisioni correttive.

L'attività di *reporting* rappresenta la fase apicale e di raccordo dell'intero ciclo di *compliance* integrata. In questa fase finale, tutti gli esiti e le informazioni raccolte nelle fasi precedenti vengono radicati e rappresentati in maniera organica, così da fornire una visione d'insieme sia all'interno della funzione *compliance* sia nei confronti del *top management*.

Il *reporting* di *compliance* consiste nella predisposizione di relazioni periodiche e di indicatori sintetici sullo stato della conformità aziendale: esso include gli esiti del *Compliance Risk Assessment* (con i livelli di rischio residuo rilevati e le aree di maggiore esposizione), lo stato di implementazione dei piani di adeguamento alle nuove normative, i risultati emersi dall'attività di monitoraggio (ad esempio numero di controlli effettuati, indicatori fuori soglia, anomalie riscontrate), nonché l'evidenza di eventuali violazioni significative verificatesi e delle azioni intraprese per gestirle.

Queste informazioni vengono dapprima raccolte "dal basso verso l'alto", ossia convogliate dai *Compliance Specialist* e dalle unità operative verso la funzione centrale di *Compliance* integrata, che le aggrega a livello di Gruppo. Successivamente, attraverso appositi flussi informativi, i risultati consolidati vengono riportati verso l'alto agli organi aziendali competenti come il vertice esecutivo e i Consigli o Comitati di controllo (ad esempio il Consiglio di Amministrazione, il Comitato Controllo e Rischi, l'Organismo di Vigilanza ex D.Lgs. 231/01, etc.).

Questo *reporting* integrato garantisce piena trasparenza e tracciabilità al processo di *compliance*: la direzione aziendale viene messa nelle condizioni di conoscere in modo chiaro e tempestivo il livello di rischio di non conformità a cui l'azienda è esposta, l'efficacia dei presidi posti a sua tutela e le eventuali criticità residue. Sulla base di tali *report*, il *top management* può così esercitare un ruolo attivo di indirizzo e controllo, valutando se siano necessarie ulteriori misure di rafforzamento e assicurando che la gestione della *compliance* rimanga allineata agli obiettivi strategici e ai principi di integrità, trasparenza e legalità propri della cultura aziendale.

Tutte queste fasi (dall'analisi degli scenari fino al *reporting* finale) sono strettamente collegate tra loro in un percorso ciclico di miglioramento continuo.

L'esito del *reporting*, ben lontano dal costituire una conclusione statica, diviene input prezioso per riavviare nuovamente il ciclo: le evidenze raccolte e le lezioni apprese

alimentano la successiva analisi degli scenari e il periodico aggiornamento del *Compliance Risk Assessment*.

Ad esempio, le criticità emerse nel monitoraggio e formalizzate nei *report* direzionali possono suggerire nuove priorità di intervento o la necessità di rivedere alcune procedure, influenzando la pianificazione delle attività future di *compliance*.

Parallelamente, il costante mutamento del contesto esterno (rilevato nella fase di analisi degli scenari evolutivi) richiede continue verifiche e adeguamenti nelle fasi di valutazione e trattamento del rischio. Si genera in tal modo un meccanismo virtuoso: ogni fase fornisce informazioni e stimoli che confluiscono nella fase successiva, e al termine del ciclo queste informazioni ritornano all'inizio per essere rielaborate alla luce di nuove conoscenze.

Il modello di *compliance* integrata adottato dalla Società opera, dunque, come un processo dinamico e reiterativo, in cui il *feedback* derivante dal monitoraggio e dal *reporting* permette di affinare progressivamente l'intero sistema. Con questo approccio ciclico, l'organizzazione è in grado di mantenere la propria conformità normativa sempre sotto controllo, rispondendo in modo agile ai cambiamenti e riducendo nel tempo il rischio di non conformità attraverso un percorso di miglioramento continuo.

3.3 Strumenti operativi: *Legal Inventory*, *Compliance Dashboard*, piattaforma GRC

L'approccio teorico del modello di *compliance* integrata, trattato nel precedente paragrafo, vede delineate le diverse fasi chiave in linea con la Linea Guida aziendale: si parte dall'analisi degli scenari evolutivi e delle novità normative, per passare alla valutazione e al trattamento dei rischi di non conformità (*risk assessment* e *risk treatment*), quindi all'implementazione di meccanismi strutturati di monitoraggio e *reporting*, fino ad abbracciare una solida impostazione di *governance* della *compliance* e a promuovere una diffusa cultura aziendale della conformità supportata da mirati programmi di formazione.

A questo approccio metodologico teorico corrisponde una fase operativa in cui il modello viene concretamente attuato attraverso procedure e strumenti dedicati. Questo passaggio

dalla teoria alla pratica è guidato da un'apposita "Istruzione Operativa interna", che disciplina nel dettaglio le attività da svolgere e gli strumenti da impiegare per implementare i sottoprocessi fondamentali del modello integrato.

In sostanza, per assicurare coerenza con le fasi metodologiche previste e con gli *standard* internazionali di riferimento (come la ISO 37301:2021), l'organizzazione ha tradotto i principi della *compliance* integrata in un processo operativo strutturato.

Ciò consente di passare dalla mera progettazione del modello alla sua esecuzione quotidiana, garantendo che i requisiti normativi vengano gestiti in modo sistematico ed efficace in tutta l'azienda.

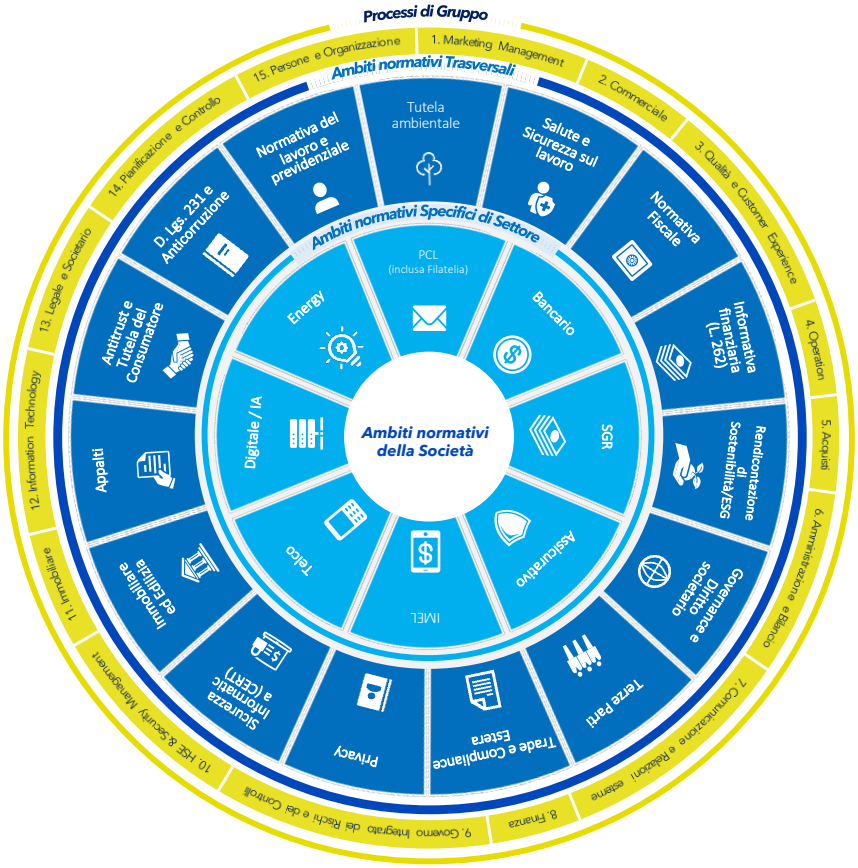
La Mappatura dei Presidi di *Compliance* rappresenta un passaggio preliminare fondamentale per l'attuazione operativa del modello.

Tale attività è volta a identificare in modo sistematico tutti gli ambiti normativi rilevanti per l'organizzazione e le funzioni aziendali incaricate di presidiarli.

È proprio in questo contesto che l'ente ha individuato quindici ambiti di *compliance* specialistici, ciascuno affidato a funzioni dotate di competenze specifiche nella relativa materia.

Nella figura 3 riportata di seguito sono riportati i quindici ambiti di *compliance* specialistici.

Figura 3 – *Tableau* degli ambiti normativi del Gruppo



Fonte: rielaborazione personale dell'autore, anno 2025

Oltre a questi presidi specifici, operano anche presidi di Gruppo, con compiti trasversali di coordinamento e supervisione delle politiche di conformità.

Questo sistema garantisce che per ogni area normativa critica vi siano delle risorse con un'elevata competenza specialistica, e allo stesso tempo promuove un raccordo orizzontale tra le varie funzioni di presidio, così da evitare sovrapposizioni o lacune nei controlli.

Questa mappatura permette di integrare le informazioni e i flussi di lavoro dei vari presidi in un sistema unitario e sinergico.

Uno degli strumenti cardine per l'implementazione operativa è il *Compliance Dashboard*, un cruscotto di monitoraggio concepito per valutare e tracciare i rischi di non conformità derivanti dalle nuove tendenze normative.

Grazie a questo *dashboard* l'azienda riesce ad individuare tempestivamente i nuovi requisiti legislativi o regolamentari. Essendo quest'ultimo basato su una piattaforma informatica integrata, che consente il monitoraggio in tempo reale sia delle normative in fase di elaborazione sia quelle già in vigore, l'organizzazione riesce ad adottare le misure correttive necessarie.

Il *Compliance Dashboard* in particolare aiuta a monitorare l'evoluzione normativa attraverso due fasi complementari: la Fase A, dedicata all'analisi degli scenari normativi e regolamentari (ad esempio disegni di legge, provvedimenti regolamentari in itinere), e la Fase B, focalizzata sull'esame dettagliato dei requisiti introdotti da nuove norme una volta che queste siano entrate in vigore.

Attraverso questo strumento, la funzione *Compliance* integrata, con il supporto dei *Compliance Specialist* delle varie aree, intercetta le novità normative più rilevanti e ne valuta in maniera sistematica il potenziale impatto sul *business* aziendale.

Gli esiti di tali analisi vengono sintetizzati in schede informative e confluiscono in una reportistica periodica verso i vertici aziendali e gli organi di controllo, specialmente nei casi in cui una nuova disposizione sia stata valutata di impatto "alto" per l'organizzazione.

Grazie al flusso costante di informazioni sulle evoluzioni del quadro normativo di riferimento assicurato dal *Compliance Dashboard*, l'azienda riesce ad anticipare i cambiamenti e di pianificare in tempo utile gli interventi appropriati per mantenere la conformità.

Parallelamente, un secondo pilastro operativo del modello è rappresentato dalla *Legal Inventory*, il quale costituisce il repertorio unico e completo di tutti gli obblighi normativi a cui l'organizzazione è soggetta. Esso si presenta come un catalogo onnicomprensivo delle *Compliance Obligations*: vi sono censite sia le normative esterne (leggi, regolamenti, direttive europee, provvedimenti di Autorità, ecc.), sia le fonti normative interne (policies, procedure, codici di condotta, modelli organizzativi), includendo obblighi di natura sia vincolante sia volontaria cui l'azienda ha deciso di aderire.

La *Legal* Inventory, oltre ad essere organizzata per Ambiti di *Compliance* e per Settori normativi, viene gestita in primo luogo dai *Compliance Specialist* competenti per materia,

secondo criteri uniformi definiti centralmente dalla funzione *Compliance* di Gruppo. Ogni obbligo normativo censito viene inoltre collegato ai processi aziendali specifici su cui esso impatta, grazie a un collegamento con la mappatura dei processi organizzativi di gruppo.

Questo strumento svolge diverse funzioni operative cruciali: da un lato guida i *Compliance Specialist* nell'individuazione e nell'aggiornamento dei requisiti normativi pertinenti alle loro attività di *compliance*, garantendo che nulla venga trascurato; dall'altro è fondamentale per il monitoraggio dell'evoluzione normativa, poiché mantenendo aggiornata la lista delle fonti applicabili permette di verificare in ogni momento la conformità dell'azienda.

Questo a sua volta consente di ridurre il rischio di sanzioni o danni reputazionali dovuti a inadempienze. Inoltre, la *Legal Inventory* costituisce il riferimento centrale per il *Compliance Risk Assessment*: la valutazione dei rischi di non conformità viene infatti svolta prendendo in considerazione ciascuna normativa censita in questo archivio, determinando così il profilo di rischio inerente e residuo associato a ogni obbligo di *compliance* identificato.

La gestione operativa della *Legal Inventory* segue un processo strutturato di "censimento e aggiornamento continuo" delle norme rilevanti. Ciascun *Compliance Specialist*, per l'ambito normativo di propria competenza, è tenuto a identificare le nuove fonti normative (o le modifiche a quelle esistenti) da cui possano derivare obblighi di *compliance* per l'azienda, inserendole tempestivamente nell'Inventario.

La funzione *Compliance* Integrata centrale (funzione CIG) supervisiona questo processo da una prospettiva integrata multi-tematica, coordinando l'attività dei vari specialisti e verificando che siano censite tempestivamente tutte le normative rilevanti (ossia considerate rilevanti in quanto di preminente interesse o comunque aventi alto impatto per il Gruppo) così da poter informare adeguatamente il *Top Management* sugli sviluppi normativi e sui piani di interventi eventualmente necessari.

Per ogni obbligo normativo inserito nella *Legal Inventory* vengono registrate una serie di informazioni chiave che possono essere utilizzate per quantificare il suo rischio di non conformità.

Queste informazioni comprendono, ad esempio, la natura e la fonte della disposizione (distinguendo tra normativa esterna e interna), il titolo o riferimento normativo (es.

numero di legge, decreto, norma interna), l'indicazione se si tratti di una prescrizione obbligatoria oppure volontaria, nonché i processi aziendali impattati dalle *Compliance Obligations*.

Questa anagrafica strutturata permette di collegare ogni requisito normativo al contesto operativo aziendale garantendo delle analisi di rischio rigorose e mirate.

È importante sottolineare che la *Legal Inventory* viene gestita in modo unitario e armonizzato per evitare duplicazioni: la stessa fonte normativa non viene censita più volte in ambiti diversi, ma è registrata una sola volta dall'unità di *compliance* più competente per materia, mentre gli altri ambiti eventualmente interessati vi fanno riferimento senza replicarla.

L'inventario include anche i principali *strumenti normativi interni* adottati dall'azienda (quali, ad esempio, Codice Etico, Politica Integrata, Linea Guida SCIGR, Modello Organizzativo ex D.Lgs. 231/2001, etc.), i quali, avendo applicabilità trasversale, vengono censiti in tutti gli ambiti di *compliance* e valutati anch'essi in termini di rischio secondo una metodologia "di alto livello".

Nella tabella 1 di seguito riportata viene illustrata la struttura interna della *Legal Inventory*.

Tabella 1 – *Legal Inventory*

Anagrafica Compliance Obligations				Processo/i di Riferimento														
Riferimento normativa esterno/ interno (Specialistico / Trasversale)	Riferimento normativo	Prescrizione normativa	Prescrizione Obbligatoria / Volontaria	Processo														
Tipologia di prescrizione, distinzione tra normativa esterna / interna (menù a tendina)	*Riferimento al "numero" della Legge, Decreto, Norma interna*	*Riferimento al "titolo" del Requisito Normativo*	*Tipologia di prescrizione, distinzione tra normativa obbligatoria / volontaria (menù a tendina)*	*Marketing Management*	*Commerciale*	*Qualità e Customer*	*Operation*	*Acquisti*	*Amministrazione e Bilancio*	*Comunicazione e Relazioni*	*Finanza*	*Governo Integrato del HSE & Security Management*	*Immobiliare*	*Information Technology*	*Legale e Societario*	*Pianificazione e Controllo*	*Persone e Organizzazione*

Fonte: rielaborazione personale dell'autore, anno 2025

Dal punto di vista tecnologico e metodologico, l'intero processo di *compliance* integrata è supportato da una piattaforma GRC (*Governance, Risk & Compliance*) centralizzata, che funge da infrastruttura unificata per gli strumenti sopra descritti.

Questa piattaforma informatica, implementata in modo armonizzato a livello di Gruppo, permette alla funzione di *Compliance* centrale e ai vari presìdi specialistici di cooperare efficacemente mediante flussi informativi standardizzati e operazioni uniformi sui dati.

In pratica, attraverso il sistema GRC l'azienda ha digitalizzato e integrato i diversi moduli del proprio modello di *compliance*: il *Compliance Dashboard* e la *Legal Inventory* risiedono su questo ambiente condiviso, così che l'intercettazione di una nuova norma, la sua analisi, il suo censimento nell'Inventario e la successiva valutazione del rischio avvengano come passaggi consequenziali di un unico flusso di lavoro tracciato.

La piattaforma GRC garantisce dunque che ogni aggiornamento normativo sia immediatamente visibile a tutte le funzioni interessate e che le azioni di adeguamento siano prese in carico senza ritardi.

Questa piattaforma, oltre a supportare le fasi di valutazione e gestione dei rischi, facilita le attività di monitoraggio continuo e di *reporting* previste dal modello.

Sul fronte interno, essa consente un efficace *reporting orizzontale*: i *Compliance Specialist*, attraverso il sistema, trasferiscono periodicamente alla funzione centrale tutte le informazioni e i risultati delle attività di *compliance* dei rispettivi ambiti, alimentando una base dati comune.

Successivamente queste informazioni vengono aggregate e sintetizzate dalla funzione *Compliance* Integrata nelle opportune relazioni direzionali (*reporting* verticale), destinate al *Top Management* e agli organi societari, offrendo una visione completa sull'andamento del processo di *compliance* integrata e sullo stato dei rischi di non conformità a livello di Gruppo.

Tale flusso informativo strutturato consente al vertice aziendale di valutare periodicamente l'efficacia e l'adeguatezza del sistema di controllo interno in materia di *compliance*, ma anche di assumere decisioni pienamente consapevoli sulla gestione dei rischi legali e reputazionali.

Per concludere, il passaggio dalla fase teorica alla fase operativa del modello di *compliance* integrata si compone di un insieme coordinato di processi e strumenti (con la Mappatura dei Presidi di *Compliance* come base, e con *Compliance Dashboard*, *Legal Inventory* e piattaforma GRC come principali leve operative) che permettono all'azienda di presidiare in maniera integrata i propri obblighi normativi e i rischi di non conformità, garantendo così un sistema di *compliance* robusto, dinamico e pienamente incorporato nella gestione aziendale quotidiana.

3.4 Il percorso di certificazione ISO 37301: dalla progettazione all'ottenimento

Sono diverse le fasi progettuali che l'azienda ha dovuto conseguire per ottenere la certificazione ISO 37301, fasi che vanno dalla definizione iniziale del modello di conformità fino all'ottenimento formale del certificato.

In primo luogo, l'organizzazione ha progettato un modello di *Compliance* integrato, ovvero un sistema di gestione della conformità pensato per presidiare in modo strutturato tutti i rischi di non conformità rilevanti per il proprio contesto operativo.

Questo modello è stato sviluppato in linea con i requisiti dello *standard* ISO 37301:2021 e con le migliori prassi internazionali in materia di *compliance*.

Esso adotta un approccio *risk-based*, che ha lo scopo di identificare, valutare e mitigare i rischi di violazione normativa, diffondendo una solida *cultura della conformità* all'interno dell'ente.

In questo primo step, l'azienda ha stabilito i principi guida e le politiche di *compliance*, formalizzandoli in documenti interni quali linee guida e procedure, così da delineare chiaramente obiettivi, ambito e metodologie del sistema di gestione della *compliance*.

Di pari passo alla definizione del modello, è stata condotta una mappatura dettagliata dei requisiti normativi e degli obblighi di conformità applicabili.

L'organizzazione ha realizzato un catalogo unico delle disposizioni legislative, regolamentari e volontarie pertinenti alle proprie attività: un vero e proprio *Legal Inventory* aziendale. Ogni requisito è stato analizzato e associato ai processi aziendali interessati e alle strutture organizzative competenti, in modo da garantire che nessun obbligo venisse trascurato.

Grazie a questa mappatura è stato possibile evidenziare i *gap* rispetto alle prescrizioni della ISO 37301 e, di conseguenza, pianificare le necessarie azioni correttive o implementative. In sostanza, per ogni requisito dello *standard* si è verificata l'esistenza di controlli o misure equivalenti nel sistema esistente e, ove mancanti, si sono progettati nuovi presìdi di conformità. Allo stesso tempo, la catalogazione sistematica delle norme ha gettato le basi per un monitoraggio continuo dell'evoluzione normativa: il modello prevede infatti aggiornamenti periodici del *Legal Inventory* e l'analisi tempestiva di

nuove disposizioni, in modo da valutare proattivamente l'impatto di ogni novità legislativa sui processi aziendali.

Un passaggio cruciale del percorso è stata l'evoluzione del modello organizzativo della funzione *compliance*, che ha determinato il passaggio da un approccio "per ambiti" ad uno "per processi".

Inizialmente la gestione della *compliance* era organizzata in *silos* tematici, con presìdi separati per ciascun ambito normativo (es. normativa antiriciclaggio, *privacy*, responsabilità amministrativa ex D.Lgs. 231/2001, etc.).

Un'impostazione siffatta, sebbene focalizzata sulle singole materie, rischiava però di segmentare la visione d'insieme e di generare ridondanze nei controlli.

Alla luce delle linee guida aggiornate degli organismi di accreditamento (che hanno incentivato un approccio per processi ai fini della certificazione ISO 37301), l'azienda ha riorientato il proprio sistema di *compliance* su base processuale.

Ciò significa che le attività di conformità sono state ripensate considerando i processi aziendali *end-to-end*: per ogni macro-processo operativo dell'organizzazione sono stati individuati i rischi di non conformità trasversali alle diverse normative applicabili, valutandone gli impatti e assicurando che fossero implementati controlli adeguati all'interno del processo stesso.

Grazie a questo nuovo approccio integrato per processi si è ampliato il perimetro del sistema di gestione della *compliance*, estendendolo a tutte le funzioni e attività aziendali. In altri termini, la conformità non viene più presidiata in modo verticale per singola materia, ma in modo orizzontale e unitario all'interno dei flussi operativi, garantendo una visione olistica del rischio di non conformità.

Questa trasformazione ha consentito all'organizzazione di individuare con chiarezza i presidi e i ruoli necessari a far funzionare il sistema di gestione della *compliance* secondo il nuovo modello.

È stato istituito un presidio centrale di *compliance*, affidato a una funzione aziendale dedicata con il compito di coordinare e supervisionare l'intero processo. Inoltre, è stata creata una rete di presìdi specialistici distribuiti nelle varie aree di competenza: figure denominate *Compliance Specialist*, deputate a presidiare specifici ambiti normativi o settori di attività all'interno del gruppo, con l'obiettivo di assicurare localmente l'implementazione delle politiche di *compliance*.

A ciascun attore (presidio centrale, specialisti di ambito, specialisti di entità e persino i *process owner* dei vari processi aziendali) sono state attribuite responsabilità precise nel sistema: dalla identificazione e valutazione dei rischi di non conformità, all'attuazione dei controlli e delle misure correttive, fino al *reporting* periodico verso i vertici aziendali. Questa chiara definizione di ruoli e responsabilità, formalmente documentata, ha garantito un efficace coordinamento e una ripartizione strutturata dei compiti di *compliance*, evitando sovrapposizioni e colmando eventuali *gap* di presidio.

La gestione documentale del sistema di *compliance* è stato un altro elemento portante del percorso di certificazione.

Per soddisfare i requisiti di ISO 37301 in termini di "informazioni documentate", l'azienda ha dovuto predisporre, aggiornare e integrare un *corpus* di documenti organizzativi a supporto del modello di conformità.

In particolare, oltre al già menzionato documento sulla linea guida di *Compliance* Integrata (che delinea principi, ruoli e fasi del processo), sono state sviluppate dettagliate procedure operative e istruzioni aziendali relative ai vari sotto-processi di *compliance* (ad esempio la procedura per l'identificazione degli obblighi normativi, la metodologia di *compliance risk assessment*, il processo di monitoraggio e *reporting* delle eventuali non conformità, etc.).

La redazione e approvazione formale di questi documenti ha permesso di istituzionalizzare le prassi di *compliance* esistenti, colmando eventuali lacune e assicurando la tracciabilità delle attività svolte.

Inoltre, la documentazione funge da base di riferimento sia per il personale coinvolto (che vi trova indicazioni chiare su come svolgere i compiti di conformità) sia per gli *auditor* interni ed esterni, che possono così verificare la corrispondenza tra quanto previsto a livello procedurale e quanto effettivamente implementato.

Nel corso del progetto, grande importanza è stata data anche alla pianificazione degli *audit* interni del sistema di gestione della *compliance*.

In ottemperanza al ciclo di miglioramento continuo PDCA (*Plan-Do-Check-Act*) su cui si fondano gli *standard* ISO, l'organizzazione ha definito un programma di verifiche ispettive interne mirate a valutare periodicamente l'efficacia e l'aderenza del modello di *compliance* ai requisiti della norma. Prima di affrontare l'*audit* di certificazione ufficiale da parte dell'ente terzo, sono state condotte *audit* interni preparatori (a cura della funzione

Internal Audit aziendale o con il supporto di consulenti esterni specializzati) sull'insieme dei processi e dei controlli di *compliance* implementati.

Questi *audit* interni sono stati progettati e condotti tenendo specificamente in considerazione i requisiti previsti dalla norma ISO 37301[21], con l'obiettivo di verificare che i punti norma fossero effettivamente implementati e seguiti nelle pratiche operative dell'azienda. In questo modo, gli *audit* interni hanno permesso di valutare non solo l'esistenza dei controlli, ma anche la loro reale applicazione e l'aderenza agli *standard* richiesti dalla certificazione.

Grazie a queste verifiche è possibile individuare eventuali non conformità o punti di miglioramento, fornendo così all'azienda l'opportunità di porre rimedio con azioni correttive prima della valutazione finale per la certificazione.

Inoltre, una volta ottenuta la certificazione, la pianificazione degli *audit* interni periodici è divenuta parte integrante del sistema, assicurando il mantenimento nel tempo dei requisiti ISO 37301 e il continuo affinamento del modello in risposta ai cambiamenti organizzativi o normativi.

È importante sottolineare che, parallelamente alle attività tecniche e procedurali, l'azienda ha investito in modo significativo nelle attività di formazione e sensibilizzazione del personale sui temi della *compliance*.

La costruzione di un vero sistema di gestione della conformità richiede infatti che i principi etici e le norme vengano compresi e fatti propri da tutti gli attori aziendali, dai vertici fino ai livelli operativi.

Per questo sono stati sviluppati programmi di formazione mirati, sia per le figure direttamente coinvolte nel processo di *compliance* (come i *Compliance Specialist* e i responsabili di funzione), sia per l'intera compagine aziendale. Ad esempio, l'organizzazione ha erogato sessioni formative *ad hoc* in vista degli *audit*, come sessioni *pre-audit* informative per preparare le unità operative alla visita di certificazione.

Queste iniziative sono state accompagnate da campagne di comunicazione interna volte a rafforzare la "cultura della legalità" e il *commitment* aziendale verso l'integrità: *newsletter*, eventi dedicati e messaggi dal *top management* hanno contribuito a tenere alta l'attenzione sulla rilevanza strategica della *compliance*.

[21] V., supra, Cap. 2 pp. 27-28-29

Tutto ciò ha migliorato la consapevolezza del personale circa i propri obblighi e responsabilità in materia di conformità, favorendo comportamenti in linea con le norme e la segnalazione proattiva di eventuali criticità.
In definitiva, grazie a questo articolato percorso di progettazione e implementazione, l'azienda è riuscita a conformare il proprio sistema di controlli interni agli *standard* richiesti da ISO 37301 e a ottenere la relativa certificazione nei tempi prefissati.
È importante sottolineare che un simile sistema di gestione della *compliance* può essere integrato con altri sistemi di gestione certificabili in ambito di integrità aziendale: ad esempio, le procedure implementate risultano sinergiche con quelle richieste dalla norma ISO 37001 (specifica per i sistemi di gestione anticorruzione) e con i modelli organizzativi ex D. Lgs. 231 già adottati dall'azienda.
L'esperienza maturata lungo il percorso di certificazione ISO 37301 ha quindi rafforzato non solo il profilo di *compliance* aziendale, ma anche la capacità di integrare diversi presidi normativi in un unico sistema efficace ed efficiente, a garanzia di un'operatività conforme, etica e trasparente.

3.5 Considerazioni sui punti di forza del sistema implementato

L'analisi condotta evidenzia come il sistema di gestione per la *compliance*, certificato secondo la ISO 37301, presenti numerosi elementi di successo che ne hanno determinato l'efficacia. In primo luogo, l'organizzazione in esame, oltre ad essere tra le prime ad ottenere la certificazione ISO 37301 nel 2022, ha saputo dimostrare un approccio pionieristico e una spiccata proattività nell'adeguarsi ai migliori *standard* internazionali. Tutto ciò si riflette anche nell'eccezionale estensione del perimetro di conformità coperto: il modello implementato abbraccia un ventaglio amplissimo di ambiti normativi, riuscendo a gestire efficacemente obblighi eterogenei nonostante l'elevata complessità organizzativa.
Questo ampio raggio d'azione include sia normative settoriali sia requisiti legali trasversali (ad esempio in materia di responsabilità amministrativa d'impresa, trasparenza contabile e adempimenti fiscali), a conferma della solidità e versatilità del sistema di *compliance* adottato.

Un primo pilastro di tale solidità risiede nel robusto *framework di governance* predisposto.

L'architettura di *governance* per la *compliance* è stata delineata con chiarezza, definendo ruoli, responsabilità e flussi di *reporting* che garantiscono un presidio efficace del rischio di non conformità.

In particolare, è stata realizzata una forte responsabilizzazione delle funzioni aziendali: ogni unità organizzativa ha ben definite le proprie responsabilità in materia di conformità, secondo il principio che la *compliance* è parte integrante del lavoro di tutti all'interno di un'organizzazione.

Questo meccanismo di *accountability* diffusa, sostenuto dall'impegno diretto del vertice aziendale e da adeguati meccanismi di coordinamento (es. comitati di *compliance*, referenti di conformità nelle varie funzioni), ha favorito l'integrazione della gestione della conformità nelle operazioni quotidiane e nei processi decisionali dell'Ente.

Ne deriva che la conformità non è percepita come un onere esterno, ma risulta un elemento intrinseco alla gestione aziendale, con un forte allineamento tra obiettivi di *business* e requisiti normativi.

Inoltre, l'uso efficace di strumenti digitali avanzati a supporto del sistema di *compliance* costituisce un ulteriore elemento chiave.

L'organizzazione ha introdotto un *Legal Inventory* centralizzato, che cataloga sistematicamente le leggi e i regolamenti applicabili alle attività aziendali, assicurando una costante ricognizione degli obblighi normativi pertinenti.

Ad esso si affianca un *Compliance Dashboard* dinamico, attraverso cui vengono monitorati in tempo reale gli indicatori di conformità e lo stato di attuazione dei controlli, fornendo una visibilità immediata sul livello di *compliance* nelle diverse aree. In particolar modo, l'implementazione di una piattaforma informatica integrata di GRC (*Governance, Risk & Compliance*) ha apportato una valenza strategica alla digitalizzazione del sistema di *compliance*.

Questa piattaforma unificata consente di gestire in modo coordinato i processi di conformità, rischio e controllo, superando i silos informativi e creando un unico punto di riferimento per tutte le informazioni rilevanti.

I benefici derivanti da tale digitalizzazione sono molteplici: innanzitutto un aumento della sicurezza dei dati di *compliance*, grazie a robusti meccanismi di controllo degli accessi,

cifratura e tracciamento delle operazioni (*audit trail*) che proteggono le informazioni sensibili e ne assicurano l'integrità.

Al tempo stesso, si ottiene una piena tracciabilità di ogni attività o verifica svolta in ambito *compliance*, in modo che sia sempre possibile risalire ai dati, ai responsabili e alle tempistiche delle azioni intraprese, agevolando sia le attività di *audit* interno sia le eventuali verifiche esterne.

Inoltre, la standardizzazione e centralizzazione delle informazioni favorisce la comparabilità dei dati nel tempo e tra diverse unità organizzative, permettendo analisi trasversali e l'individuazione di *trend* o anomalie.

In sintesi, attraverso la piattaforma GRC l'intero patrimonio informativo legato alla conformità viene "messo a sistema", risultando prontamente fruibile e condivisibile: ciò migliora l'analisi e il *reporting*, riduce le ridondanze e gli errori manuali, e rende il presidio della *compliance* più tempestivo ed efficiente.

Questo approccio digitale integrato si allinea alle *best practice* moderne, secondo cui una piattaforma GRC robusta fornisce ai decisori una visione unificata dei rischi, dei controlli e dello stato di conformità, automatizzando il monitoraggio e rafforzando la trasparenza e *l'accountability* in tutta l'organizzazione.

I risultati ottenuti sono la conferma del valore strategico di questa scelta, poiché la digitalizzazione non solo supporta la complessità operativa del modello di *compliance*, ma costituisce essa stessa un vantaggio competitivo, elevando l'affidabilità e la credibilità complessiva del sistema.

Un ulteriore fattore di successo emerso è la forte diffusione della cultura della conformità all'interno dell'ente. Sin dalle fasi iniziali di implementazione, l'azienda ha investito in programmi di formazione dedicati e campagne di sensibilizzazione, con l'obiettivo di far comprendere a tutto il personale l'importanza del rispetto delle norme e degli *standard* etici.

La *leadership* aziendale ha avuto un ruolo cruciale in tal senso, promuovendo con il proprio esempio i valori di integrità e trasparenza e comunicando con chiarezza la non tolleranza verso comportamenti non etici o non conformi.

Questa costante azione di esempio da parte del vertice aziendale (*tone at the top*) e di coinvolgimento dei dipendenti ha contribuito a radicare principi etici solidi e una mentalità proattiva verso la conformità a tutti i livelli gerarchici. I dipendenti non sono

più meri esecutori di procedure obbligatorie, ma attori consapevoli che condividono la responsabilità di mantenere l'azienda allineata alle norme.

L'attenzione alla cultura di *compliance* è perfettamente in linea con lo spirito della ISO 37301, che pone l'accento sull'importanza di diffondere una cultura della conformità in tutta l'organizzazione come fondamento per il successo sostenibile.

Nel modello implementato, questo si traduce in un ambiente di lavoro in cui la conformità è parte integrante dei valori aziendali e dove esiste una chiara consapevolezza degli *stakeholder* circa l'impegno etico dell'Ente.

Tale approccio culturale, unito ai meccanismi formali di gestione, rafforza significativamente l'efficacia del sistema poiché incentiva la segnalazione di problemi, facilita la cooperazione interfunzionale e riduce il rischio di infrazioni dovute a comportamenti opportunistici o inconsapevoli.

Tra i punti di forza più rilevanti va evidenziata l'adesione ai principi fondamentali della ISO 37301, che è risultata pienamente incorporata nel disegno e nella prassi del sistema di *compliance*.

In particolare, il principio di integrità, inteso come rigorosa osservanza delle norme e dei valori etici, influenza sia le politiche aziendali sia le prassi operative, garantendo che ogni decisione o processo tenga conto degli *standard* di conformità applicabili.

Il ruolo della *leadership* è stato, come detto, determinante: il *top management* e gli organi di governo hanno assicurato un sostegno visibile e costante a tutte le politiche e ai processi necessari per conseguire gli obiettivi di *compliance*, mettendo a disposizione risorse adeguate e dimostrando nei fatti il proprio *commitment*.

Tutto questo ha conferito autorevolezza al programma di conformità e ha incoraggiato tutte le funzioni aziendali a contribuire attivamente.

Inoltre, il sistema è stato concepito e aggiornato secondo un approccio di miglioramento continuo, in ottemperanza al ciclo di *Deming* (*Plan-Do-Check-Act*) su cui si basano gli *standard* ISO.

Questo significa che l'azienda pianifica con cura le attività di *compliance*, le realizza operativamente, ne verifica regolarmente l'efficacia (attraverso *audit*, monitoraggi, indicatori di *performance*) e implementa azioni correttive o di miglioramento alla luce dei risultati emersi.

L'integrazione del modello di *compliance* nel più ampio Sistema di Controllo Interno e di Gestione dei Rischi (SCIGR) aziendale ha favorito tali dinamiche di miglioramento continuo e di visione olistica: la *compliance* è infatti coordinata con gli altri controlli aziendali e con la gestione del rischio, assicurando coerenza negli obiettivi di controllo e sinergia nelle attività di presidio.
Questo raccordo con il sistema di controllo interno consente, ad esempio, di allineare le verifiche di conformità con le attività di *audit* interno e di *risk management*, evitando duplicazioni e assicurando una copertura completa dei rischi su tutti i fronti.
L'adesione ai principi di integrità, *leadership* e miglioramento continuo non solo ha facilitato il conseguimento della certificazione ISO 37301, ma costituisce il motore per mantenere nel tempo un sistema di gestione vivo e resiliente, in grado di adattarsi all'evoluzione normativa e alle nuove sfide di *compliance*.
In conclusione, l'insieme di questi punti di forza (dalla solidità del *governance framework* alla responsabilizzazione diffusa, dall'uso strategico di strumenti digitali alla radicata cultura della conformità, fino all'allineamento con i principi della norma e all'integrazione nel sistema di controllo interno) ha permesso all'organizzazione di sviluppare un sistema di gestione della *compliance* altamente credibile ed efficace. Questo sistema non solo soddisfa i requisiti dello *standard* ISO 37301, ma fornisce un vero valore aggiunto all'azienda: migliora la capacità di prevenire e gestire i rischi legali ed etici, consolida la fiducia degli *stakeholder* grazie alla maggiore trasparenza e affidabilità dei processi, e contribuisce alla sostenibilità dell'impresa nel lungo periodo, creando una base solida per il successo futuro nel rispetto delle regole e dei valori condivisi.

3.6 Dalle criticità agli spunti di miglioramento: il contributo della consulenza

La gestione di un sistema di *compliance* integrata in conformità alla ISO 37301 porta con sé alcune criticità operative rilevanti. La norma evidenzia infatti l'esigenza di un approccio integrato al controllo dei rischi di *compliance*, segnalando come in molte realtà aziendali tali rischi siano gestiti in modo frammentato e poco efficiente.

In sostanza, aggiornamenti normativi e procedurali sono spesso recepiti da funzioni diverse senza un coordinamento sistematico, con il risultato che controlli e processi correlati non evolvono in modo sinergico.

Questo si traduce spesso in lacune o sovrapposizioni: ad esempio, una revisione del modello *privacy* può restare scollegata da quella del modello 231, determinando duplicazioni di obblighi e di documentazione. Secondo quanto riportato dalla letteratura di settore, la mancata comunicazione fra presidi specialistici genera ritardi decisionali, duplicazioni operative e anche demotivazione del personale, mettendo a rischio la coerenza complessiva delle azioni aziendali e la conformità normativa.

Un problema da non sottovalutare è l'obsolescenza documentale poiché se i documenti e le procedure non vengono rivisti regolarmente, finiscono per riflettere regole superate, compromettendo la conformità e la qualità del sistema, poiché vecchie versioni di *policy* possono continuare a circolare e a guidare le attività anche quando non più aggiornate.

Queste criticità concrete sono esemplificabili con situazioni tipiche: procedure non coordinate tra reparti (ad es. IT e controllo interno), ritardi nell'aggiornamento dei manuali di *compliance* o *gap* nel *training* specialistico. Se, per esempio, un nuovo decreto impone adeguamenti sul controllo interno ma tale informazione non raggiunge in tempo tutte le funzioni coinvolte, si crea una discontinuità operativa.

Analogamente, quando responsabili di *compliance* settoriali aggiornano autonomamente i propri strumenti di monitoraggio senza uniformare la documentazione, gli operatori possono ritrovarsi con istruzioni divergenti.

Tali situazioni di disallineamento sono frutto di una gestione ancora basata su *silos* funzionali, in questo modo l'ente rischia di non usufruire dei benefici di un sistema integrato.

Quindi, la difficoltà di mantenere allineati i presidi specialistici e di assicurare che tutti i documenti siano costantemente aggiornati emerge come criticità centrale nella gestione quotidiana del CMS.

Una leva fondamentale per superare queste criticità è il ciclo PDCA (*Plan-Do-Check-Act*) previsto dalla ISO 37301.

La norma incoraggia esplicitamente l'adozione di questo modello ciclico di miglioramento continuo, che richiede di "pianificare" obiettivi e processi, "attuare" le

attività pianificate, "verificare" i risultati ottenuti e infine "intervenire" per correggere le deviazioni.

In sostanza, vengono pianificati degli *audit* interni regolari, monitoraggi costanti e riesami periodici da parte della direzione per misurare l'efficacia del sistema e alimentare il miglioramento continuo.

La ISO 37301 richiede infatti non solo l'implementazione di controlli e procedure, ma anche il loro monitoraggio e il riesame formale da parte del *top management*, con l'esplicito obiettivo di *"conseguire il miglioramento continuo"* del sistema.

Va sottolineato che il PDCA deve essere concretamente attuato: se le fasi di controllo e di azione restano formali o inefficaci, il sistema di *compliance* rischia di cristallizzarsi. In altre parole, non basta progettare processi migliori (*Plan*) e metterli in atto (*Do*); è indispensabile anche misurare (*Check*) e correggere (*Act*) in modo sistematico ogni volta che emergono scostamenti o nuovi bisogni normativi.

Una *governance* agile e adattiva è necessaria per garantire la capacità del sistema di *compliance* di evolversi rapidamente in un contesto dinamico.

Questo significa superare un modello di *governance* rigido e centralizzato, orientandosi invece verso un approccio iterativo, distribuito e orientato all'azione. Come evidenziano le più recenti teorie di *adaptive governance*, la gestione aziendale deve farsi "*capability*" diffusa, dove decisioni e procedure sono continue funzioni di riallineamento fra strategia e operatività.

In altre parole, la *governance* deve essere intenzionale (guidata da obiettivi chiari), integrata in tutti i processi operativi e continuamente aggiustata in base ai *feedback* interni ed esterni. Solo così si garantisce la capacità di assorbire e adattarsi ai cambiamenti (regolamenti emergenti, pressioni di mercato, innovazioni aziendali).

L'idea chiave è che *"non si può governare il valore di domani con le regole di ieri"*[22]: ogni cambiamento normativo o strategico richiede un tempestivo riallineamento di *policy* e controlli. Di conseguenza, la struttura di *governance* deve includere meccanismi di monitoraggio proattivo (es. *team* dedicati alla *compliance* normativa in tempo reale) e un susseguirsi di interventi tempestivi. In questo modo l'azienda può evitare di restare

[22] David Nichols, "*Why Adaptive Governance is the Future of Digital Trust*", DVMS *Istitute*, 12 Aprile 2025, https://dvmsinstitute.com/2025/04/12/why-adaptive-governance-is-the-future-of-digital-trust/#:~:text=Adaptive%20governance%20is%20not%20a,It%20is

"ferma" mentre il contesto evolve, trasformando invece la *compliance* in un vettore di resilienza e reattività.

Nelle grandi organizzazioni caratterizzate da una struttura complessa e da un perimetro *multi-business*, la gestione della *compliance* integrata presenta sfide particolarmente rilevanti. La molteplicità di normative nazionali e sovranazionali, la necessità di armonizzare processi eterogenei e la continua variazione degli obblighi regolatori rendono spesso insufficiente il solo presidio interno.

In tali contesti, il ricorso alla consulenza esterna si configura come una scelta strategica, in quanto consente di integrare competenze specialistiche sempre aggiornate, assicurare un approccio metodologico strutturato e beneficiare di una visione oggettiva e indipendente rispetto a quella interna.

Inoltre, i consulenti esterni possono offrire un prezioso contributo in termini di *benchmarking*, trasferendo alle imprese esperienze e *best practice* maturate in altri settori e in diverse realtà organizzative, permettendo così di valutare la maturità del proprio sistema di *compliance* rispetto agli *standard* più avanzati.

La consulenza diventa quindi uno strumento indispensabile per affrontare la complessità normativa, per prevenire il rischio di obsolescenza delle procedure e per supportare il miglioramento continuo, garantendo un aggiornamento costante e un supporto operativo capace di ridurre ridondanze e inefficienze.

In questo quadro, il contributo della consulenza esterna si è rivelata una leva strategica per rafforzare il sistema di *compliance*. La consulenza esterna ha apportato un approccio metodologico strutturato e *best practice* di settore che hanno integrato la visione interna aziendale, contribuendo a colmare *gap* e a rendere più efficiente il presidio dei rischi di non conformità.

È stata ad esempio condotta una valutazione della maturità del programma di *compliance* e definito un modello operativo *target* su misura, allineato sia alle normative locali sia ai requisiti della ISO 37301.

Attraverso l'uso di *framework* proprietari, la consulenza esterna ha supportato l'integrazione e l'automatizzazione degli obblighi di *compliance*, consentendo all'organizzazione di rispondere in modo più rapido ed efficace a variazioni normative e a *gap* di controllo. In termini operativi, il *team* di consulenti ha facilitato il raccordo tra

le diverse funzioni aziendali, condividendo *benchmark* di settore e approcci trasversali, al fine di prevenire duplicazioni e migliorare la coerenza del sistema di controllo interno.
Un ulteriore contributo si è avuto nell'ambito della formazione: la consulenza esterna ha predisposto piani formativi specifici, sviluppato *workshop* e sessioni di *training* mirate per elevare le competenze interne e rafforzare la cultura della *compliance*, valorizzando il ruolo del *top management* nel promuovere un forte *tone at the top*.
Questo affiancamento operativo e formativo ha permesso di diffondere la cultura della conformità in tutta l'organizzazione, rafforzando il principio di *accountability* e rendendo più solido il sistema.
Un esempio concreto del contributo della consulenza esterna si è avuto in occasione del rinnovo della certificazione ISO 37301 tra il 2024 e il 2025, quando l'ente di certificazione ha evidenziato alcune non conformità che hanno richiesto un impegno straordinario da parte della società.
Verso la fine del 2024 l'ente di certificazione ha evidenziato alcune non conformità, segnalando aree di miglioramento che hanno richiesto un impegno mirato da parte della società e il supporto determinante della consulenza esterna. Quest'ultima ha affiancato la società in tutte le fasi di analisi, revisione metodologica e implementazione delle azioni correttive, garantendo l'adeguamento del sistema di gestione della *compliance* agli *standard* richiesti.
In particolare, durante le verifiche di sorveglianza del 2024 sono state individuate sei non conformità complessive, di cui una classificata come "maggiore" e cinque come "minori".
La non conformità maggiore riguardava la metodologia di valutazione del rischio, che non consentiva ancora di valorizzare in maniera piena i contributi specialistici provenienti dai diversi ambiti di *compliance*.
Per far fronte a questa osservazione la società, con il supporto diretto della consulenza esterna, ha adottato un approccio progressivo e mirato: nel breve lasso di tempo tra la fine del 2024 e l'inizio del 2025 sono stati selezionati tre ambiti pilota (Modello 231, ex art. 262 TUF e fiscale) sui quali è stata applicata la nuova metodologia di *risk assessment*, integrando in maniera più strutturata le valutazioni dei *Compliance Specialist* all'interno del *framework* complessivo.

Questo lavoro ha consentito all'ente di certificazione di verificare la bontà dell'impostazione aggiornata e di constatare che i criteri rivisti erano effettivamente in grado di valorizzare le specificità dei singoli ambiti.

Alla luce di ciò, in sede di verifica straordinaria ad inizio 2025, la non conformità maggiore è stata declassata a minore, con l'impegno di estendere progressivamente l'applicazione della nuova metodologia a tutti gli ambiti di *compliance* attraverso un piano di *deployment*.

La consulenza esterna ha avuto un ruolo decisivo in questa fase, guidando l'elaborazione dei nuovi criteri metodologici, supportando i *Compliance Specialist* nella loro applicazione sperimentale e predisponendo la documentazione necessaria a dimostrare all'ente la solidità del percorso intrapreso.

Il successivo piano di *deployment* ha confermato l'esito positivo della verifica straordinaria, con l'impegno di chiudere tutte le non conformità entro la fine del 2025.

Nella tabella seguente si riporta la sintesi operativa con le principali aree di criticità rilevate e le relative azioni di trattamento.

Tabella 1 – La gestione delle non conformità

#	Data Apertura	Classific.	Area di miglioramento		Descrizione non conformità	Azioni correttive implementate
1	2024	NCm	4.5/6.1	OBBLIGHI DI CONFORMITÀ	❖ L'inventario legislativo necessitava di maggiore dettaglio e di includere in modo uniforme sia fonti esterne che interne.	✓ Revisione dei criteri di censimento e integrazione della *Legal Inventory* con ulteriori fonti esterne e interne rilevanti per la società.
2	2025	NCm	4.6	VALUTAZIONE DEL RISCHIO	❖ La metodologia di valutazione del rischio incorporava pianamente le valutazioni effettuate dai *Compliance Specialist* per il proprio ambito di *compliance,*	✓ Revisione della metodologia e attuazione della stessa su un pilota di tre ambiti nel 2024, validato dall'ente all'inizio 2025. Successiva estensione della nuova metodologia a tutti gli ambiti di *compliance* per la verifica di sorveglianza da parte dell'ente entro la fine del 2025
3	2024	NCm	9.1.4	*REPORTING* RELATIVO ALLA *COMPLIANCE*	❖ Il reporting annuale al Vertice non approfondiva tutti gli aspetti relativi alla ISO 37301.	✓ Ridefinizione della struttura del reporting annuale e aggiornamento della Linea Guida e delle procedure operative.
4	2024	NCm	9.3	RIESAME DELLA DIREZIONE	❖ Il processo di riesame non era calendarizzato in modo pienamente conforme alle tempistiche ISO.	✓ Inserimento formale del riesame nell'agenda degli organi competenti e pianificazione più puntuale.
5	2024	NCm	7.3	CONSAPEVOLEZZA	❖ La valutazione dell'efficacia della formazione richiedeva una metodologia più strutturata.	✓ Introduzione di strumenti di misurazione e organizzazione di nuove sessioni formative e iniziative di sensibilizzazione.
6	2024	NCm	9.1.2	FONTI DI RITORNO SULLE PRESTAZIONI RELATIVE ALLA *COMPLIANCE*	❖ Assenza di indicatori specifici per misurare l'efficacia complessiva del sistema di *compliance*.	✓ Definizione e implementazione dei *Key Compliance Indicators* (KCI) per il monitoraggio del sistema di gestione.

Fonte: rielaborazione personale dell'autore, anno 2025

Di seguito si fornisce una descrizione più articolata delle non conformità rilevate e delle azioni correttive intraprese.

1. **Revisione della *Legal Inventory***: la prima non conformità riguardava la modalità di censimento dell'inventario legislativo. Data la mole di *compliance obligations* rilevanti per la società, inizialmente si era scelto di adottare modalità di censimento che aggregavano più requisiti normativi all'interno della stessa disposizione, poiché in diversi casi tali requisiti presentavano caratteristiche simili ed erano tra loro riconducibili. L'ente di certificazione ha tuttavia richiesto una maggiore precisione nello spacchettamento dei requisiti, così da poterli monitorare in maniera puntuale, oltre all'estensione dell'inventario normativo a ulteriori fonti di natura sia esterna (normative nazionali ed europee, accordi con autorità, *standard* volontari, *best practice*, norme superate ancora rilevanti) sia interna (*policy*, linee guida, procedure, istruzioni operative, contratti *intercompany*, modelli organizzativi, codici etici, contratti collettivi). Ai sensi dei punti 4.5 e 6.1 della ISO 37301, relativo agli obblighi di conformità, l'organizzazione deve infatti garantire un censimento accurato e completo delle proprie *compliance obligations*, comprendendo sia fonti esterne sia interne, per assicurare un presidio sistematico e coerente.

   La consulenza esterna ha svolto un ruolo decisivo armonizzando le diverse *legal inventory* già in uso nei vari ambiti e definendo criteri uniformi per l'intero gruppo. Attraverso interviste e sessioni di lavoro con i *Compliance Specialist*, sono state spiegate le nuove regole di censimento, supportando gli *owner* nel loro utilizzo e garantendo la creazione di un inventario unico, coerente e confrontabile.

2. **Metodologia di *Risk Assessment***: la seconda non conformità, inizialmente classificata come maggiore, riguardava la metodologia di valutazione del rischio, che non valorizzava ancora in modo pieno e uniforme i contributi specialistici provenienti dai diversi ambiti di *compliance*. Per rispondere a questa osservazione, tra la fine del 2024 e inizio del 2025 è stato avviato un progetto pilota su tre ambiti (Modello 231, ex art. 262 TUF e fiscale), applicando i nuovi criteri metodologici.

   Questa revisione è stata giudicata conforme, consentendo di declassare la non conformità a minore. Successivamente, attraverso un piano di *deployment*, la metodologia è stata estesa progressivamente a tutti gli ambiti di *compliance*. Ai sensi

del punto 4.6 della ISO 37301, la valutazione del rischio deve infatti basarsi su criteri chiari e condivisi, includendo sia analisi di alto livello sia contributi specialistici *bottom-up*, così da garantire una visione completa e bilanciata dei rischi di non conformità. La nuova impostazione si fonda su una "Metodologia Complessiva", che combina le valutazioni *bottom-up* (ossia quelle specialistiche dei *Compliance Specialist*, con metriche operative consolidate) e i criteri *top-down* di alto livello, necessari a gestire le *compliance obligations* non riconducibili a presidi specialistici. Sono stati inoltre aggiornati i questionari di autovalutazione delle misure di mitigazione e introdotti indicatori per misurare l'efficacia della formazione.

3. ***Reporting***: un'ulteriore non conformità ha riguardato il *reporting* relativo alla *compliance*, per il quale l'ente ha richiesto un maggiore livello di dettaglio e un allineamento più completo ai requisiti della ISO 37301.
   Per colmare tale esigenza, sono stati aggiornati la Linea Guida di *Compliance* Integrata di Gruppo e l'Istruzione Operativa sugli strumenti per l'implementazione del processo. In particolare, è stata ridefinita la struttura del *reporting* annuale, includendo un'analisi dettagliata dei requisiti della norma e garantendo l'emersione dei punti di forza e delle aree di miglioramento. Sono stati inoltre integrati nel sistema complessivo ulteriori documenti di sintesi, come la relazione annuale sui rischi e la *compliance* di gruppo. Ai sensi del punto 9.1.4 della ISO 37301, il *reporting* deve garantire un'informazione tempestiva, accurata e completa a tutti i livelli, consentendo alla direzione di assumere decisioni informate e promuovendo trasparenza e *accountability*.

4. **Riesame della Direzione**: un'altra osservazione ha riguardato il riesame della direzione, documento fondamentale previsto dagli *standard* ISO per verificare l'efficacia del sistema e pianificare azioni di miglioramento. L'ente ha richiesto una calendarizzazione più puntuale del processo, così da assicurare che il riesame fosse effettuato in linea con le scadenze previste e con la pianificazione del ciclo di gestione. In conformità al punto 9.3 della ISO 37301, il riesame della direzione deve essere regolarmente programmato e documentato, così da valutare l'adeguatezza, l'efficacia e l'allineamento del sistema agli obiettivi aziendali e agli obblighi di *compliance*.

L'azione correttiva è consistita nell'inserimento formale del tema all'ordine del giorno degli organi competenti (Comitato Controllo e Rischi e Consiglio di Amministrazione), così da garantire la piena conformità alle tempistiche richieste.

5. **Formazione e consapevolezza**: la quinta non conformità ha riguardato la valutazione dell'efficacia delle attività formative. L'ente ha richiesto l'adozione di una metodologia più dettagliata e strutturata per misurare in maniera puntuale la consapevolezza acquisita dai destinatari. Ai sensi del punto 7.3 della ISO 37301, la formazione e la consapevolezza del personale sono elementi essenziali per assicurare che tutti i membri dell'organizzazione comprendano i propri obblighi di *compliance* e siano in grado di agire in conformità.
   Per rispondere a questa esigenza è stato introdotto uno strumento metodologico specifico (ad esempio questionari e altri strumenti di misurazione), volto a rilevare il livello di apprendimento e consapevolezza raggiunto. Contestualmente, sono state organizzate nuove sessioni formative dedicate ai *Compliance Specialist* e ai *Process Owner*, nonché iniziative di sensibilizzazione aziendale come il "*Compliance Day*", finalizzate a diffondere una cultura della conformità sempre più radicata.

6. **Indicatori di *compliance* (KCI)**: nella sesta e ultima non conformità l'ente di certificazione ha segnalato l'opportunità di sviluppare indicatori specifici per monitorare in maniera sistematica l'efficacia del sistema di gestione della *compliance*. Per rispondere a questa richiesta, la società ha realizzato i *Key Compliance Indicators* (KCI), strumenti volti a misurare l'adeguatezza e l'efficacia complessiva del modello di *compliance*, non riferiti a singoli ambiti normativi, ma a tutto il sistema integrato. In linea con il punto 9.1.2 della ISO 37301, l'organizzazione deve infatti predisporre fonti di ritorno e indicatori sulle prestazioni della *compliance*, così da misurare e monitorare in maniera oggettiva il funzionamento del sistema. I dati raccolti vengono analizzati dalla funzione di *Compliance* Integrata, aggregati e successivamente riportati al vertice aziendale, garantendo una visione completa e trasparente sullo stato di attuazione del sistema.

In conclusione, il percorso di gestione delle non conformità ha rappresentato un passaggio cruciale per il rafforzamento del modello.

Dal 2024 al 2025 la società, con il costante supporto della consulenza esterna, ha trasformato sei rilievi iniziali (di cui uno maggiore) in altrettante opportunità di perfezionamento, implementando strumenti e metodologie che hanno reso il sistema di *compliance* più robusto, coerente e pienamente aderente agli *standard* internazionali.

CONCLUSIONI

In conclusione, questo percorso di studio e l'esperienza sul campo confermano come la *compliance* rivesta un ruolo sempre più centrale come leva di *governance* aziendale. Non si tratta più soltanto di evitare la violazione di norme, ma di trasformarla in un fattore culturale che accompagna l'organizzazione verso l'integrità e la sostenibilità, indirizzandola verso scelte operative e strategiche più consapevoli.

Una *compliance* efficace diventa così un elemento propulsore di fiducia, sia all'interno dell'azienda sia verso gli *stakeholder* esterni, contribuendo alla creazione di valore duraturo e reputazione positiva.

Ed è proprio l'adozione e la certificazione dello *standard* internazionale ISO 37301 a tradurre questa visione in prassi organizzativa concreta.

La norma fornisce un *framework* strutturato per sviluppare un sistema di gestione della *compliance* integrato con la gestione dei rischi, fondato sui principi di buona *governance*, integrità e trasparenza, e orientato al miglioramento continuo.

L'ottenimento della certificazione ISO 37301 offre un valore aggiunto tangibile: rappresenta una prova riconosciuta dell'impegno dell'azienda nel presidio dei rischi di conformità, rafforzando la trasparenza verso il mercato e la fiducia degli *stakeholder*. Inoltre, grazie all'approccio sistematico previsto dallo *standard*, l'organizzazione sviluppa meccanismi di controllo e *feedback* costanti che alimentano un ciclo virtuoso di miglioramento e adattamento continuo.

Parallelamente, l'implementazione di un sistema di *compliance* integrata in un grande Gruppo industriale ha messo in luce le sfide operative e gestionali connesse. Integrare la *compliance* nel Sistema di Controllo Interno e Gestione dei Rischi (SCIGR) significa orchestrare processi e responsabilità attraverso l'intera organizzazione, con un elevato livello di complessità.

Le normative da rispettare sono dettagliate e in continuo mutamento, ma ancora più complessa è la realtà dei processi aziendali; per affrontarla efficacemente è necessario un approccio multidisciplinare e l'adozione di strumenti condivisi, chiari e scalabili.

Ne deriva l'esigenza di una *governance* agile e reattiva, capace di favorire la collaborazione tra funzioni diverse e di adattarsi rapidamente ai cambiamenti normativi e di contesto, in modo da mantenere il sistema di *compliance* efficace nel tempo.

In questo scenario, la digitalizzazione emerge come un fattore strategico abilitante.
L'uso di piattaforme e soluzioni tecnologiche avanzate (ad esempio sistemi GRC integrati nei processi aziendali) consente di monitorare la conformità in modo continuo e automatizzato, collegando normative e controlli in un unico sistema coeso.
Tali soluzioni aumentano la visibilità sui processi e forniscono al *management* informazioni tempestive e contestualizzate, supportando decisioni più informate e reattive.
Al contempo, il supporto di consulenti specializzati si è rivelato determinante. In un progetto tanto complesso è spesso buona prassi avvalersi di un supporto consulenziale qualificato capace di affiancare l'azienda in tutte le fasi del processo di certificazione. Nel caso in esame, il contributo della consulenza esterna ha aiutato a interpretare correttamente i requisiti dello *standard*, a sviluppare strumenti operativi efficaci e a diffondere le *best practice*, accelerando e consolidando il percorso verso la conformità certificata.
L'analisi condotta ha permesso di evidenziare come la *compliance*, supportata da *standard* internazionali quali la ISO 37301, non rappresenti un mero obbligo burocratico, bensì un efficace strumento di crescita organizzativa.
L'integrazione tra l'approccio teorico e l'applicazione pratica in contesti aziendali complessi ha mostrato l'importanza di coniugare la visione strategica con l'attenzione al dettaglio operativo, così da garantire l'efficacia di un sistema di gestione della *compliance*.
Dall'analisi è emerso chiaramente che investire nella *compliance* significa investire nella sostenibilità e nella reputazione dell'impresa, generando benefici duraturi in termini di fiducia degli *stakeholder* e di resilienza aziendale.
In conclusione, la trattazione di questo tema così attuale e rilevante ha consentito di arricchire il quadro delle conoscenze sul ruolo strategico della *compliance*, offrendo strumenti concettuali e metodologici utili per interpretarne l'impatto nella prospettiva della *governance* contemporanea.

BIBLIOGRAFIA

Abriani N., Giunta F. (2012), "L'organismo di vigilanza", La Responsabilità Amministrativa delle Società e degli Enti (Rivista 231), pp. 205–215.

Agnese A. (2012), "Il Modello Organizzativo per i reati ambientali", La Responsabilità Amministrativa delle Società e degli Enti (Rivista 231), n. 3, p. 231.

ASSONIME (2019), "Prevenzione e governo del rischio reato: la disciplina 231/2001 e le politiche di contrasto dell'illegalità nell'attività d'impresa", Note e Studi, n. 5/2019.

Astrologo A. (2008), I modelli di organizzazione e di gestione: riflessioni sull'art. 30 del d.lgs. 81/2008, in D. Fondaroli (a cura di), Principi costituzionali in materia penale e fonti sovranazionali, Padova.

Bartolomucci S. (2014), "Censimento e ponderazione delle potenzialità commissive dei reati-presupposto tra risk mapping e precetti del d.lgs. 231/2001", Responsabilità Amministrativa delle Società ed Enti, n. 3.

Bleker S., Hortensius D. (2014), "ISO 19600: The development of a global standard on compliance management", Business Compliance, 2/2014.

Bricola F. (1970), "Il costo del principio 'societas delinquere non potest' nell'attuale dimensione del fenomeno societario", Rivista italiana di diritto e procedura penale.

Capparelli O., Lanzino L. (2016), Modelli di gestione del rischio e compliance ex D.Lgs. 231/2001, Milano.

CNDCEC – ABI – CNF – Confindustria (2019), Principi consolidati per la redazione dei Modelli organizzativi e l'attività dell'Organismo di Vigilanza, febbraio 2019.

Confindustria (2021), Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001, giugno 2021.

Coglianese C., Nash J. (2021), "Compliance Management Systems: Do They Make a Difference?", in B. van Rooij, D. Sokol (eds.), The Cambridge Handbook of Compliance, Cambridge University Press, Cambridge, pp. 571–593.

De Maglie C. (2002), L'etica e il mercato. La responsabilità penale delle società, Milano.

De Vero G. (2008), "La responsabilità penale delle persone giuridiche", in C.F. Grosso, T. Padovani, A. Pagliaro (a cura di), Trattato di diritto penale – Parte Generale, Milano.

Ficedolo C. (2022), "La certificazione del Modello 231 – L'ennesimo bollino o una vera opportunità", Risk & Compliance Italia, 3 ottobre 2022.

Foti A. (2022), "I sistemi di gestione e la norma UNI ISO 37301 a supporto dei Modelli 231", UNI – Ente Italiano di Normazione, 14 gennaio 2022.

Foti A. (2025), "La nuova norma UNI 11961:2024 sulla compliance a supporto dei sistemi integrati ISO ed i modelli 231", Risk & Compliance Italia, 22 febbraio 2025.

Garante per la Protezione dei Dati Personali (2023), Parere sullo schema di Linee guida in materia di protezione dei segnalanti (whistleblowing), Registro provv. n. 304 del 6 luglio 2023.

Garuti G. (2007), "Profili giuridici del concetto di 'adeguatezza' dei modelli organizzativi", Responsabilità Amministrativa delle Società ed Enti, n. 3.

Gennaro V. (2012), "Il modello di organizzazione, gestione e controllo e le esigenze di compliance integrata", Rivista 231, n. 4, p. 186.

Ielo P. (2006), “Compliance programs: natura e funzione nel sistema della responsabilità degli enti – Modelli organizzativi e D.Lgs. 231/2001”, Responsabilità Amministrativa delle Società ed Enti, n. 1.

Insinga L.G., Rossi F., Petrovic M. (2022), La compliance integrata per l’attuazione del Modello 231, Primiceri Editore, Padova.

ISO (2021), ISO 37301:2021 – Compliance management systems – Requirements with guidance for use, ISO, Ginevra.

Laudati A., Adotti A. (2021), “Le nuove Linee Guida di Confindustria per i Modelli 231: analisi delle novità introdotte e approfondimento sulla tematica della compliance integrata”, Rivista 231, n. 4, p. 281.

Li J. (2023), “Research on Key Questions and Strategies Model of Enterprise Compliance Management System Construction”, in Proceedings of the 2023 3rd International Conference on Business Administration and Data Science (BADS 2023), Atlantis Press, pp. 299–311.

Malega P., Majerník M. (2024), “Standardisation of Compliance Management and Process Quality in the Organization Based on the Integrated Management System”, Quality Innovation Prosperity, 28(3), pp. 82–101.

Maiello V. (2002), “La natura (formalmente amministrativa, ma sostanzialmente penale) della responsabilità degli enti nel D.Lgs. 231/2001”, Rivista trimestrale di diritto penale dell’economia.

Marinucci G. (2003), “‘Societas puniri potest’: uno sguardo sui fenomeni e sulle discipline contemporanee”, Rivista italiana di diritto e procedura penale.

Paliero C.E. (2001), “Il D.Lgs. 8 giugno 2001, n. 231: da ora in poi, societas delinquere (et puniri) potest”, Corriere Giuridico.

Pansarella M. (2018), “Problematiche giuridiche ed organizzative del whistleblowing nei modelli 231”, Responsabilità Amministrativa delle Società ed Enti, n. 1, pp. 283–287.

Piccinni M.L. (2012), “La Circolare della Guardia di Finanza n. 83607/2012: manuale operativo a contrasto dell’illegalità d’impresa e della delittuosità corporativa”, Responsabilità Amministrativa delle Società ed Enti, n. 3, p. 13.

Piergallini C. (2010), “La struttura del modello di organizzazione, gestione e controllo del rischio-reato”, in G. Lattanzi (a cura di), Reati e responsabilità degli enti, Milano.

Pintucci E. (2012), “Come realizzare sistema e manuale del Modello 231 integrati con gli altri sistemi di gestione”, Rivista 231, n. 4, p. 217.

Pintucci E. (2015), “La nuova ISO 9001 favorisce l’integrazione con il Modello 231”, Rivista 231, n. 2, p. 315.

Pirola G., Occhetta L. (2015), L’Organismo di Vigilanza – Guida ai controlli societari, Il Sole 24 Ore, Milano.

Presutti A., Bernasconi A. (2013), Manuale della responsabilità degli enti, Giuffrè, Milano.

Pulitanò D. (2007), “Criteri di imputazione all’ente della responsabilità ‘da reato’”, in A. Spagnolo (a cura di), La responsabilità da reato degli enti collettivi – Cinque anni di applicazione del D.Lgs. 231/2001, Milano.

Santi F. (2004), La responsabilità delle società e degli enti: i modelli di esonero delle imprese, Milano.

Santoriello C. (2015), “I modelli organizzativi richiesti dal D.Lgs. 231/2001 e le PMI – Una riflessione alla luce delle indicazioni di Confindustria”, Responsabilità Amministrativa delle Società ed Enti, n. 1.

Sbisà F., Spinelli E., Agostini B. (2017), “La responsabilità amministrativa degli enti: origine, natura, principi e criteri di imputazione”, in F. Sbisà (a cura di), Responsabilità amministrativa degli enti (D.Lgs. 231/2001), Itinera Guide Giuridiche Ipsoa.

Simonetti L. (2016), “La prevenzione dei reati ambientali attraverso l’adozione di ‘standard’ tecnici e organizzativi: il rapporto con i sistemi di gestione ambientale conformi alla norma UNI EN ISO 14001 o al regolamento EMAS”, TuttoAmbiente.it, 5 aprile 2016.

UNI (2016), UNI ISO 19600:2016 – Sistemi di gestione della compliance – Linee guida, Ente Italiano di Normazione, Milano.

UNI (2018), UNI ISO 31000:2018 – Gestione del rischio – Linee guida, Ente Italiano di Normazione, Milano.

UNI (2021), UNI ISO 37301:2021 – Sistemi di gestione per la compliance – Requisiti con guida all’applicazione, Ente Italiano di Normazione, Milano.

UNI (2024), UNI 11961:2024 – Linee guida per l’integrazione del sistema di gestione per la compliance UNI ISO 37301:2021 a supporto dei Modelli 231, Ente Italiano di Normazione, Milano.

Vernero P., Parena B., Artusi M.F. (2019), “Risk management e modelli organizzativi”, in AA.VV., Impresa e rischio – Profili giuridici del risk management, Giappichelli, Torino.

Zanichelli C. (2021), “Da Confindustria le nuove Linee Guida per la costruzione dei Modelli 231: novità e approccio sistematico”, Rivista 231.

SITOGRAFIA

Borsa Italiana – Comitato per la Corporate Governance. (2020). *Codice di Corporate Governance*. Borsa Italiana. Recuperato da https://www.borsaitaliana.it/comitato-corporate-governance/codice/2020.pdf

Bureau Veritas Italia. (2024). *Regolamento particolare per la certificazione ISO 37301:2021* (Rev. 02 del 12/07/2024). Recuperato da https://www.bureauveritas.it/sites/g/files/zypfnx256/files/media/document/CER-REP-05_ISO_37301_Regolamento_%20particolare_per_la_certificazione_ISO_37301_0.pdf

EQS Group – Homann, M. (2022). *ISO 37301 – What organisations need to know about the CMS standard*. EQS Group. Recuperato da https://www.eqs.com/en-us/compliance-knowledge/blog/iso-37301/

QMS Italia. (2021). *ISO 37301:2021 – Sistemi di gestione per la compliance*. QMS Italia. Recuperato da https://www.qmsitalia.it/iso-37301-2021/

Risk & Compliance Italia – Grasso, C. M. (2021). *Dalla ISO 19600 alla ISO 37301: l'evoluzione del Compliance Management System (CMS)*. Risk & Compliance Italia. Recuperato da https://www.riskcompliance.it/news/dalla-iso-19600-alla-iso-37301-levoluzione-del-compliance-management-system-cms/