

LA GESTIONE DEL RISCHIO DI COMPLIANCE NELLE IMPRESE

Gestione proattiva e strategica del rischio di compliance per creare valore e rafforzare la governance resiliente

La gestione del rischio di compliance, tema noto e collaudato nel settore finanziario poiché disciplinato dalle leggi sui mercati e in continua evoluzione, è diventato centrale anche per grandi aziende e PMI. In un contesto di normativa crescente, incide su prodotti, servizi, organizzazione e risultati finanziari, generando rischi operativi, regolamentari e costi in caso di inadempienza ma anche opportunità, e richiede un'elevata capacità di conformità.

1. DEFINIZIONE ED EVOLUZIONE DEL TEMA DELLA COMPLIANCE

Con «compliance» si intende la conformità alle leggi, ai regolamenti, alle procedure, ai codici di condotta e agli standard, sia interni all'impresa sia esterni. Si tratta di un impegno preso dall'impresa e dai propri rappresentanti (consiglio d'amministrazione (CdA), direzione, collaboratori) a rispettare tutte le regole applicabili alla propria attività con lo scopo di evitare rischi legali, sanzioni, rischi reputazionali e, non da ultimo, la messa in pericolo della continuità aziendale (ad esempio a seguito del ritiro dell'abilitazione a operare oppure della perdita della propria reputazione).

Evidentemente la compliance fa parte di un modello operativo di governo d'impresa più ampio che comprende la governance, il sistema di controllo interno e la gestione di tutti i rischi che hanno un impatto sull'impresa. Oggi più che mai, in un contesto politico, economico e sociale in continua evoluzione e caratterizzato da una frequenza e intensità dei cambiamenti e delle sfide mai visti prima, le imprese sono tenute a monitorare e adattare la propria governance e il proprio sistema di controllo interno (incluse la gestione dei rischi e la compliance) con l'obiettivo di migliorarne costantemente l'efficienza e l'efficacia.

Lo standard ISO 37301 (Compliance Management Systems)[1] definisce la compliance come «l'adempimento di

tutti gli obblighi di compliance», dove per obblighi si intendono i requisiti legali, regolamentari e contrattuali, i codici di condotta e le politiche interne, mentre nel modello COSO Internal Control – Integrated Framework [2], la compliance è uno dei tre obiettivi fondamentali dell'Internal Control System (insieme a reporting e operations).

Il tema della compliance non nasce improvvisamente, ma si sviluppa in modo graduale in risposta a crisi sistemiche, scandali aziendali, globalizzazione dei mercati e la conseguente inflazione normativa. Più precisamente, il concetto di compliance nasce negli Stati Uniti negli anni 1970–1980 a seguito di scandali di corruzione delle multinazionali e la conseguente emanazione del Foreign Corrupt Practices Act (FCPA)[3] nel 1977. Nel 1985 nasce l'iniziativa COSO e nel 1992 viene pubblicata la prima versione Internal Control – Integrated Framework. A seguito degli scandali Enron, Worldcom, Parmalat (tanto per citarne alcuni), negli anni 1990–2000 il tema della compliance si consolida anche a seguito dell'emanazione del Sarbanes-Oxley Act (SOX)[4] nel 2002. Allo stesso tempo nasce la figura del compliance officer come funzione organizzata e documentata. A partire da inizio 2000 vi è una diffusione globale del modello statunitense e la proliferazione, a livello europeo e nazionale, della normativa antitfrode, sulla protezione dei dati, sulla concorrenza, sulla sicurezza sul lavoro, ecc. Le imprese sono quindi chiamate a organizzarsi per evitare importanti sanzioni amministrative, penali e reputazionali. Nell'ultimo ventennio la compliance è evoluta passando da un approccio reattivo a un approccio proattivo basato su un'analisi del rischio di compliance e su modelli e framework definiti e riconosciuti internazionalmente (cfr. *tabella 1*).

Le violazioni della compliance sono reati da prendere sul serio: i media riportano regolarmente episodi, più o meno gravi, di mancata compliance, ossia situazioni che evidenziano violazioni a livello individuale e/o aziendale della normativa applicabile a determinate attività o a specifici settori.



SANDRO PROSPERI,
ESPERTO CONTABILE
DIPLOMATO, CCSA,
CERTIFIED BOARD MEMBER
SUPSI, SOCIO E GERENTE
GOVERNANCE CONSULTING

I rischi sono pertanto concreti e presenti e le conseguenze (finanziarie e reputazionali) altrettanto pesanti per le imprese, grandi o piccole che siano. Alcuni esempi concreti: la Legge sulla protezione dei dati [5] prevede multe fino a CHF 250 000 in caso di violazioni e chi non rispetta la Legge contro la concorrenza sleale [6] è perseguibile penalmente.

In generale, a livello di compliance emergono le seguenti tendenze:

- numerosi settori sono sempre più soggetti a leggi e regolamenti che riguardano ambiti sempre più ampi;
- le grandi imprese sono sempre più chiamate a dimostrare il rispetto della normativa applicabile e questo ha un impatto concreto anche sulle PMI che fanno parte della loro catena di fornitura;
- le situazioni di non conformità emergono più facilmente grazie anche ai processi di «whistleblowing»;
- le situazioni di non conformità vengono sanzionate in modo più severo sia a livello di impresa sia a livello di responsabilità personale;
- l'attenzione e l'interesse del pubblico (media, investitori, clienti, ecc.) in ambito compliance è in crescita.

A seguito di quanto sopra, la compliance, che in passato era probabilmente sottovalutata in alcuni settori, è pian piano diventata nel tempo uno dei fattori principali di «preoccupazione e ansia» della direzione d'impresa.

2. AMBITI DI COMPLIANCE E NORMATIVA APPLICABILE PER LE IMPRESE

Va precisato che la compliance non si limita all'ambito legale di un'impresa, ma riguarda tutti gli ambiti aziendali, dalla produzione e/o fornitura di servizi, alla contabilità, alle risorse umane, ai sistemi informativi, ai clienti e concorrenti, agli incassi e pagamenti, ecc.

Immagine 1: MODELLO OPERATIVO DI GOVERNO D'IMPRESA



Vista la cospicua normativa applicabile (cfr. tabella 2), peraltro non esaustiva, si potrebbe affermare che la compliance è sempre più alla base delle «scelte» strategiche e organizzative delle imprese, PMI incluse, e che la non conformità alla normativa rappresenta un importante fattore di «rischio» di tipo finanziario e reputazionale. La compliance diventa una parte essenziale e indispensabile del sistema di responsabilità dell'impresa.

Tabella 1: EVOLUZIONE DELLA MATURITÀ DELLA FUNZIONE DI COMPLIANCE

Periodo	Fase/Approccio	Focus principale	Organizzazione	Driver
1970–1990	Embrionale	Osservanza formale di nuovi obblighi normativi (check-list)	Nessuna funzione dedicata (ufficio legale, HR, qualità)	Prime normative anti-corruzione, sicurezza, privacy
1990–2000	Reattivo e frammentato	Protezione da eventuali sanzioni	Funzione ibrida (spesso Legal & Compliance)	Scandali globali, modelli di controllo interno
2000–2010	Proattivo e risk-based	Prevenzione (da check-list a gestione del rischio di non conformità)	Funzione autonoma (separata da Legal) e nuovi strumenti (risk assessment, monitoring program, reporting)	Aumento esponenziale della complessità normativa, framework internazionali, aspetti reputazionali
2010–2020	Sistema di gestione del rischio di compliance integrato	Integrazione Governance, Risk & Compliance	Funzione autonoma strutturata e riconosciuta, GRC system, KPI, KCI, cultura aziendale (ethics & integrity)	Standardizzazione tramite ISO, tone at the top, protezione dei dati, ESG, whistleblowing
2020–oggi	Strategico (influenza su modello di business, gestione dei fornitori, innovazione, ESG, cyber, etica, ecc.)	Governance, etica, ESG, valore aziendale (migliora la resilienza aziendale)	Competenze di compliance a livello di CdA	Trasparenza richiesta dai portatori di interesse, nuove norme su sostenibilità e due diligence

Tabella 2: **AMBITI DI COMPLIANCE E NORMATIVA APPLICABILE**

Ambito di compliance	Normativa applicabile [7]
Governo di impresa	→ Codice delle obbligazioni (CO) – disposizioni su governance, contabilità, responsabilità degli amministratori → Linee guida Swiss Code of Best Practice for Corporate Governance di Economiesuisse (non è una legge, ma è riconosciuto come riferimento nazionale)
Produzione/ Fornitura di servizi	→ Leggi settoriali per ottenere un'abilitazione a operare → Legge sulla sicurezza dei prodotti (LSPro) → Ordinanza sulla sicurezza dei prodotti (OSPro) → Ordinanze tecniche di settore (macchine, attrezzature a pressione, apparecchi elettrici, giocattoli, ecc.) → Legge sulla protezione dell'ambiente (LPAMB) → Ordinanza sulla protezione dell'aria (OPAir) → Ordinanza sul traffico dei rifiuti (OTR) → Ordinanza sulla riduzione dei rischi inerenti ai prodotti chimici (ORRPChim) → Legge sugli appalti pubblici (LAPub) → Ordinanza sugli appalti pubblici (OAPub) → Eventuale legislazione estera applicabile
Contabilità	→ Principi contabili applicabili → Leggi fiscali/imposte e tasse/IVA/ecc. → Ordinanza sugli obblighi di diligenza e trasparenza in relazione a minerali e metalli originari di zone di conflitto e al lavoro minorile (ODiT) → Legge sulla parità dei sessi (LPar)
Risorse umane	→ Legge sul lavoro (LL) e Ordinanza sulla legge sul lavoro (OLL) → Ordinanza sulla prevenzione degli infortuni (OPI) → Ordinanza sulla sicurezza e la protezione della salute dei lavoratori nei lavori di costruzione (OLCostr) → Previdenza sociale/Assicurazioni sociali → Principi etici/Conflitti di interesse/Frode
Sistemi informativi	→ Legge federale sulla protezione dei dati (LPD) → Ordinanza sulla protezione dei dati (OPDa) → Linee guida dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) → Sicurezza informatica/Cyber Security
Clienti/Concorrenti	→ Legge sui cartelli e altre limitazioni della concorrenza (LCart) → Legge contro la concorrenza sleale (LCSI) → Legge sul controllo dei beni (LCB) → Ordinanza sul controllo dei beni (OCB) → Legge sugli embarghi (LEmb) → Proprietà intellettuale
Incassi/Pagamenti	→ Legge sul riciclaggio di denaro, LRD → Corruzione/Sanzioni

3. COMPLIANCE MANAGEMENT SYSTEM

Grazie a una gestione efficace della compliance, le imprese possono ricavare i seguenti benefici:

- rispettare le leggi e normative applicabili alla propria attività;
- proteggere le imprese stesse e i propri collaboratori da sanzioni penali e multe ingenti;
- aumentare la propria attrattiva presso clienti, partner, investitori, banche e collaboratori;
- identificare anticipatamente i rischi e intraprendere azioni tempestive e proattive contro qualsiasi illecito;
- proteggere la propria reputazione e il valore aziendale.

3.1 Componenti di un sistema di gestione del rischio di compliance. Come gestire quindi in modo proattivo e strategico la compliance al fine di trasformarla in un fattore di differenziazione e di vantaggio competitivo? Tramite un

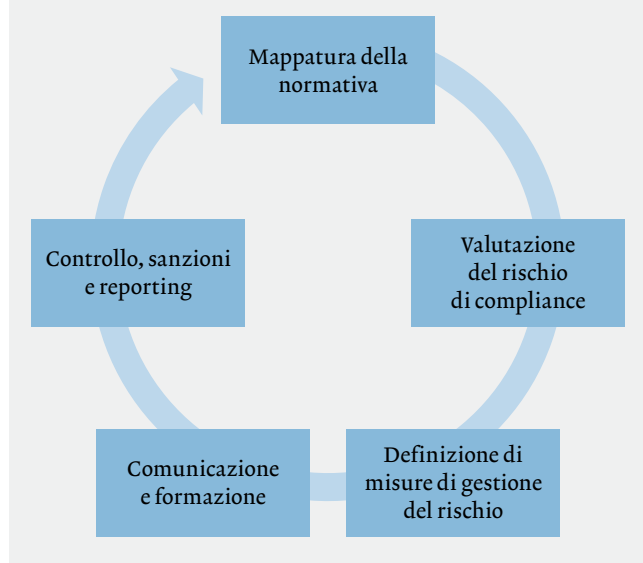
approccio sistematico di gestione del rischio di compliance (cfr. *tabella 2*) che prevede, ad esempio, le fasi seguenti.

3.1.1 Mappatura della normativa applicabile all'impresa. Si tratta di una mappatura sistematica delle normative e degli obblighi applicabili all'impresa, suddivisi per aree (ad esempio produzione e/o fornitura di servizi, contabilità, risorse umane, sistemi informativi, clienti e concorrenti, incassi e pagamenti, ecc.).

3.1.2 Valutazione del rischio di compliance. Questo processo valuta, per ciascun obbligo, la probabilità di violazione; l'impatto (sanzioni, stop produttivi, reputazione, costi); il livello di controllo già presente e l'esposizione residua.

3.1.3 Definizione di misure di gestione del rischio. Comprende il codice etico, i regolamenti, le procedure, i processi, le responsa-

Immagine 2: **MODELLO DI GESTIONE DEL RISCHIO DI COMPLIANCE**



bilità, le competenze e i controlli interni (preventivi, identificativi, correttivi).

3.1.4 Comunicazione e formazione. Ciò deve essere realizzato tramite programmi formativi mirati, campagne di sensibilizzazione, strumenti di whistleblowing, cultura dell'integrità.

3.1.5 Controllo, sanzioni e reporting. In questa fase vengono applicati controlli di secondo livello (da parte della funzione compliance) con rapporti periodici al vertice (CdA, comitati di controllo), indicatori di conformità (KCI), follow-up delle misure di gestione del rischio e aggiornamento continuo del processo di compliance.

3.2 Responsabilità. Il consiglio di amministrazione e la direzione dell'impresa valutano e approvano il modello di gestione del rischio di compliance assicurandosi che comprenda tutti gli elementi essenziali. Il consiglio di amministrazione e la direzione si assicurano che il modello venga prontamente aggiornato in caso di mutamenti a livello normativo o nell'organizzazione dell'impresa. Come in qualsiasi processo di identificazione e gestione del rischio, anche per il rischio di compliance la corretta identificazione e valutazione del rischio (e delle relative interrelazioni tra i vari rischi) sta alla base della definizione delle misure di gestione del rischio e dei relativi controlli.

4. IL RUOLO DELLA FUNZIONE DI COMPLIANCE

Sempre più imprese, anche PMI nel caso in cui il rischio di compliance venga considerato rilevante, creano all'interno della propria organizzazione una funzione di compliance specifica con l'intento di raggruppare sotto un unico cappello le attività di controllo e reporting in ambito compliance. Alcuni esempi concreti possono essere

→ imprese che sottostanno a numerose leggi per poter operare (settore finanziario, farmaceutico, alimentare, ecc.);

→ imprese con un'attività a forte impatto ambientale;

→ imprese che gestiscono un numero rilevante di dati privati (settore sanitario);

→ imprese che hanno rischi di compliance specifici (dichiarazione dell'indipendenza nel caso di pubblicazione di studi farmaceutici, ecc.).

Spesso la gestione di tali rischi di compliance (assieme ad altri possibili rischi di compliance) viene demandata a una funzione che non dispone veramente delle competenze specifiche necessarie (CFO, direttore amministrativo, direttore vendite, ecc.), a volte con il supporto di numerosi consulenti esterni, con possibili conseguenze rilevanti e sanzioni per l'impresa in caso di non conformità.

Oltre ad avere un ruolo consultivo nei confronti del consiglio di amministrazione e della direzione, una funzione di compliance interna può occuparsi in modo sistematico e coordinato delle attività seguenti:

→ monitoraggio della normativa applicabile,

→ individuazione e valutazione di potenziali rischi di non conformità,

→ definizione di eventi e indicatori di rischio,

→ supporto nella pianificazione delle misure di gestione del rischio,

→ comunicazione e formazione dei collaboratori,

→ svolgimento indipendente dei controlli di 2° livello per verificare il buon funzionamento del processo di gestione del rischio di compliance,

→ reporting al consiglio di amministrazione e alla direzione, nonché aggiornamento continuo del processo di gestione del rischio di compliance.

Quale funzione specialistica all'interno dell'impresa, la funzione di compliance (o il cosiddetto compliance officer) potrà mettere a disposizione dell'impresa degli strumenti a supporto della propria attività, quali un inventario della normativa applicabile, un database dei possibili rischi di compliance, un database dei possibili controlli di 2° livello da svolgere, un modello standardizzato di reporting per il consiglio di amministrazione e la direzione (cfr. tabella 3).

5. CONCLUSIONE

Non tutte le imprese, soprattutto quelle piccole con meno di 50 collaboratori, dispongono delle risorse per creare una propria funzione di compliance interna indipendente. Ciononostante, se non l'hanno già fatto, tutte dovrebbero iniziare a valutare in modo sistematico il rischio di compliance.

Per iniziare, ogni impresa potrebbe adottare le fasi seguenti:

→ Incaricare almeno una persona specifica all'interno dell'impresa che si occupi delle attività di compliance. È fondamentale che tale persona venga formata su come svolgere la funzione di compliance tramite appositi seminari esterni. Inoltre, è necessario comunicare il ruolo e le attività della funzione di compliance a tutti i collaboratori. Infine, è indispensabile predisporre un codice etico che fornisca un insieme di regole comportamentali per tutti i collaboratori dell'impresa, vertici compresi.

Tabella 3: **RUOLO DELLA FUNZIONE DI COMPLIANCE IN AMBITO NORMATIVO**

Identificazione e valutazione delle normative	Attuazione delle soluzioni organizzative	Controllo e reporting	Comunicazione, assistenza e formazione
Identificazione del perimetro operativo e delle normative di riferimento	Predisposizione di linee guida/direttive in materia e scelte organizzative adottate	Individuazione e misurazione dei rischi di compliance	Diffusione delle normative e dei documenti di pertinenza
Monitoraggio e gestione delle evoluzioni normative	Predisposizione di politiche, procedure o regolamenti	Verifica del rispetto delle prescrizioni normative	Consulenza alle strutture aziendali sull'applicazione di norme e codici di comportamento
Individuazione delle attività coinvolte	Sviluppo e rilascio di processi/applicazioni informatiche ove necessario	Mitigazione dei rischi e reporting al CdA e alla Direzione	Gestione delle segnalazioni di non conformità da parte delle strutture e proposta di soluzioni e modifiche organizzative
Verifica del livello di compliance e definizione delle linee di intervento	Verifica delle soluzioni organizzative	Gestione dei contatti con le autorità competenti	Formazione delle risorse

→ Condurre una valutazione del rischio di compliance per identificare i rischi più significativi. Questo per sviluppare poi misure atte a mitigare i rischi che l'impresa potrebbe incorrere.

→ Mettere a disposizione dei collaboratori un canale attraverso cui possano segnalare qualsiasi illecito, anche in modalità anonima (*whistleblowing*).

→ Infine, ma non meno importante: promuovere una cultura aziendale etica, basata su trasparenza e integrità tramite una comunicazione e formazione regolare per collaboratori e dirigenti.

Implementare un processo sistematico di gestione del rischio di compliance è un investimento in un futuro sostenibile e resiliente della propria impresa. ■

Note: 1) International Organisation for Standardisation (ISO). 2) Committee of Sponsoring Organisations of the Treadway Commission (COSO). 3) United States Congress, Criminal Division, Foreign Corrupt Practices Act Unit, <https://www.justice.gov/criminal/criminal-fraud/foreign-corrupt-practices-act>. 4) United States Congress, Sarbanes-Oxley Compliance Professionals Association (SOXCPA), Sarbanes-Oxley Act, <https://www.sarbanes-oxley-act.com/>. 5) Legge federale sulla

protezione dei dati (LPD) del 25 settembre 2020. 6) Legge federale contro la concorrenza sleale (LCSL) del 19 dicembre 1986. 7) Lista non esaustiva.

protezione dei dati (LPD) del 25 settembre 2020. 6) Legge federale contro la concorrenza sleale (LCSL) del 19 dicembre 1986. 7) Lista non esaustiva.