



## BILANCIO

### ***Il modello di organizzazione, gestione e controllo***

di Gian Luca Nieddu, Matteo P. Marabelli

Master di specializzazione

### Modello Organizzativo 231 e Organismo di Vigilanza

Scopri di più



Nell'ordinamento giuridico italiano, una **società** può essere ritenuta **responsabile** per un **reato** commesso nel suo interesse o a **suo vantaggio**.

Questo tipo di responsabilità è stato introdotto nel 2001, con il D.Lgs. 231/2001, ed ha segnato un importante punto di svolta: infatti, la società è un soggetto che esiste unicamente nella realtà giuridica e potrebbe apparire quasi *innaturale* che esso venga ritenuto **responsabile di un reato** che, materialmente, è invece **commesso da una o più persone fisiche**. Il legislatore, infatti, ha ancorato questo tipo di responsabilità ad un elemento soggettivo di colpa: se la società non si è dotata degli opportuni strumenti per prevenire quel reato e non ha opportunamente vigilato, allora quel **reato è ascrivibile anche ad essa**.

In particolare, ai sensi dell'[\*\*articolo 5, D.Lgs. 231/2001\*\*](#), la società è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

1. **da persone che rivestono funzioni di rappresentanza**, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
2. da persone **sottoposte alla direzione o alla vigilanza** di uno dei predetti soggetti.

Diversamente, la società non risponde se uno dei soggetti indicati ha agito **nell'interesse esclusivo proprio o di terzi**.

Non tutti i reati comportano una responsabilità per la società, ma solo i **reati tassativamente previsti dal decreto** agli articoli 24-26, ossia quelli definiti come "**reato presupposto**".

Come accennato, l'ascrivibilità all'ente del reato commesso dalla persona fisica è stata ancorata ad un elemento soggettivo di colpa: ai sensi degli [\*\*articoli 6 e 7 del decreto\*\*](#), infatti, **l'ente non risponde se prova**, tra le altre cose, di aver adottato ed efficacemente attuato, prima della commissione del fatto, **modelli di organizzazione e di gestione idonei a prevenire reati**.



della specie di quello verificatosi.

Questo modello di organizzazione, gestione e controllo, è quello che più comunemente viene chiamato “**Modello 231**”. L’articolo 6 del decreto citato elenca le **caratteristiche essenziali che deve avere il modello**:

1. individuare le attività nel cui ambito possono essere commessi reati;
2. prevedere specifici **protocolli diretti** a programmare la formazione e l’attuazione delle decisioni dell’ente in relazione ai reati da prevenire;
3. individuare **modalità di gestione delle risorse finanziarie** idonee ad impedire la commissione dei reati;
4. prevedere obblighi di informazione nei confronti dell’organismo deputato a vigilare sul funzionamento e l’osservanza dei modelli;
5. introdurre un **sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello**.

Inoltre, ai sensi dell’[articolo 7](#) del decreto, “*il modello prevede, in relazione alla natura e alla dimensione dell’organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell’attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.*”

Dunque, le **cinque caratteristiche sopra elencate** dovranno essere declinate sulla base:

- della **natura dell’organizzazione**, ovvero della natura giuridica dell’ente e l’eventuale assoggettamento a norme specifiche;
- delle **dimensioni dell’organizzazione**;
- del **tipo di attività svolta**.

Al di là dei requisiti visti, la legge **non delinea un percorso di costruzione del modello** e non ne prevede dei contenuti tassativi. Diverse associazioni di categoria, quindi, hanno adottato **linee guida che nel corso del tempo** sono diventate prassi consolidata di riferimento.

In particolare, tra le più rilevanti, vi sono le [Linee Guida di Confindustria](#) per la costruzione del modello di organizzazione, gestione e controllo – ai sensi del Decreto Legislativo 8 giugno 2011, n. 231”, aggiornate a giugno 2021 ed il [documento](#) pubblicato dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili aggiornato al febbraio 2019 e rubricato “*Principi consolidati per la redazione dei modelli organizzativi e l’attività dell’organismo di vigilanza e prospettive di revisione del d.lgs. 8 giugno 2001, n. 231*”.

Seguendo l’impostazione delle **Linee Guida di Confindustria**, le fasi principali in cui il sistema di prevenzione dei rischi 231 dovrebbe articolarsi sono:

1. **identificazione dei rischi potenziali**: l’analisi del contesto aziendale per individuare in quali aree o settori di attività e secondo quali modalità si potrebbero astrattamente



verificare eventi pregiudizievoli per gli obiettivi indicati dal decreto 231;

2. **progettazione del sistema di controllo** (cd. “protocolli” per la programmazione della formazione e attuazione delle decisioni dell’ente): la valutazione del sistema esistente all’interno dell’ente per la prevenzione dei reati ed il suo eventuale adeguamento, in termini di capacità di contrastare efficacemente, ovvero ridurre ad un livello accettabile, i rischi identificati.

Al fine di condurre la **costruzione di questo modello in due fasi**, sono previsti tre passi operativi:

- **inventariazione degli ambiti aziendali di attività**: comporta il compimento di una revisione periodica esaustiva della realtà aziendale, con l’obiettivo di individuare le aree che, in ragione della natura e delle caratteristiche delle attività effettivamente svolte, risultano interessate dal potenziale compimento di taluno dei reati contemplati dalla norma;
- **analisi dei rischi potenziali**: deve aver riguardo alle possibili modalità attuative dei reati nelle diverse aree aziendali, individuate secondo il processo di cui al punto precedente. L’analisi, finalizzata ad una corretta progettazione delle misure preventive, deve condurre a una rappresentazione, il più possibile completa, di come le fattispecie di reato possono essere attuate rispetto al contesto operativo interno ed esterno in cui opera l’azienda;
- **Valutazione/costruzione/adeguamento del sistema di controlli preventivi**: le attività descritte si completano con una valutazione del sistema di controlli preventivi eventualmente esistente e con il suo adeguamento quando ciò si riveli necessario, ovvero con la sua costruzione quando l’ente ne sia sprovvisto. Il sistema di controlli preventivi dovrà essere tale da garantire che i rischi di commissione dei reati, secondo le modalità individuate e documentate nella fase precedente, siano ridotti ad un “livello accettabile”. Si tratta, in sostanza, di progettare quelli che il decreto 231 definisce *“specifici protocolli diretti a programmare la formazione e l’attuazione delle decisioni dell’ente in relazione ai reati da prevenire”*.

Il riferimento assunto dalla prassi per condurre questo processo è il documento *“Enterprise Risk Management - Integrated Framework”* del Comitato COSO (*Committee of Sponsoring Organizations of the Treadway Commission*). L’ultimo punto – la valutazione/costruzione/adeguamento del sistema di controlli preventivi – viene definito nel citato documento come **“Gap analysis”**, ossia l’individuazione dei gap/lacune esistenti tra le misure di prevenzione già in essere e quelle che dovrebbero esistere al fine di abbassare il rischio al di sotto della soglia accettabile.

Secondo le Linee Guida Confindustria, queste sono le componenti di un **sistema di controllo preventivo**:

1. **Codice etico o di comportamento con riferimento ai reati considerati**: l’adozione di principi etici, ovvero l’individuazione dei valori aziendali primari cui l’impresa intende



conformarsi è espressione di una determinata scelta aziendale e costituisce la base su cui impiantare il sistema di controllo preventivo.

2. **Sistema organizzativo sufficientemente aggiornato, formalizzato e chiaro:** ciò vale soprattutto per l'attribuzione di responsabilità, le linee di dipendenza gerarchica e la descrizione dei compiti (mansionari e *job description*), con specifica previsione di principi di controllo quali, ad esempio, la contrapposizione di funzioni; deve inoltre tenere traccia della copertura temporale degli incarichi.
3. **Procedure manuali ed informatiche (sistemi informativi):** devono essere tali da regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo (quadrature; approfondimenti informativi su particolari soggetti quali agenti, consulenti, intermediari). Una particolare efficacia preventiva riveste lo strumento di controllo rappresentato dalla separazione di compiti fra coloro che svolgono fasi o attività cruciali di un processo a rischio
4. **Poteri autorizzativi e di firma:** vanno assegnati in coerenza con le responsabilità organizzative e gestionali. Talune funzioni possono essere delegate a un soggetto diverso da quello originariamente titolare. Ma occorre definire preliminarmente in modo chiaro e univoco i profili aziendali cui sono affidate la gestione e la responsabilità delle attività a rischio reato, avendo riguardo anche al profilo dell'opponibilità delle procure a terzi. La delega deve costituire lo strumento per un più efficace adempimento degli obblighi imposti dalla legge all'organizzazione complessa, non per un agevole trasferimento di responsabilità. A tal fine può rivelarsi utile una puntuale indicazione delle soglie di approvazione delle spese effettuate dal delegato.
5. **Comunicazione al personale e sua formazione:** Con riferimento alla comunicazione, essa deve riguardare ovviamente il codice etico, ma anche gli altri strumenti quali i poteri autorizzativi, le linee di dipendenza gerarchica, le procedure, i flussi di informazioni e tutto quanto contribuisca a dare trasparenza nell'operare quotidiano. Accanto alla comunicazione, deve essere sviluppato un adeguato programma di formazione modulato in funzione dei livelli dei destinatari. Esso deve illustrare le ragioni di opportunità - oltre che giuridiche - che ispirano le regole e la loro portata concreta.
6. **Sistemi di controllo integrato:** essi devono considerare tutti i rischi operativi, in particolare relativi alla potenziale commissione di reati-presupposto, in modo da fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità generale e/o particolare. Occorre definire opportuni indicatori per le singole tipologie di rischio rilevato (ad esempio accordi di intermediazione che prevedano pagamenti off-shore) e i processi di *risk assessment* interni alle singole funzioni aziendali.