MANAGEMENT CONSULTING
Marcello Colaianni

Consulente - Formatore - Auditor

Mobile + 39 393.3265594 | **Sito** www.marcellocolaianni.it
Mail marcello@marcellocolaianni.it
Blog marcellocolaianniblog.wordpress.com

Compliance 231 & Gestione del Rischio

Percorso integrato

A CHI SI RIVOLGE

Pensato in particolare per organizzazioni esposte a rischio-reato ex D. Lgs. 231/2001, o che partecipano a gare pubbliche e devono dimostrare adeguati assetti organizzativi — dalla PMI alla realtà più articolata, ovunque serva un presidio di compliance vivo e aggiornato, non un documento fermo nel cassetto.

DI COSA SI TRATTA

Un percorso che unisce la responsabilità amministrativa degli enti (D. Lgs. 231/2001) al Sistema di gestione per la Compliance (UNI ISO 37301).
La norma individua una molteplicità di **reati presupposto** la cui commissione — da parte dei vertici aziendali o di soggetti a questi subordinati, che agiscono dolosamente o colposamente, nell'interesse o a vantaggio dell'organizzazione — comporta **sanzioni amministrative** per la persona giuridica e **sanzioni penali** per la persona fisica responsabile del reato.

I due pilastri operativi del Decreto sono:

- **Il Modello di Organizzazione, Gestione e Controllo (MOGC)** — un documento programmatico che mappa i rischi-reato specifici dell'organizzazione e definisce protocolli, procedure e controlli per prevenirli. La sua adozione ed efficace attuazione costituisce l'esimente dalla responsabilità amministrativa.
- **L'Organismo di Vigilanza (OdV)** — organo autonomo e indipendente cui è affidato il compito di vigilare sull'osservanza e sull'aggiornamento del Modello, riferendo direttamente all'organo dirigente.

La "Gestione del Rischio" nel nome del pacchetto non è solo rischio-reato: include la continuità operativa dell'organizzazione di fronte a qualsiasi evento avverso — cyberattacchi, blackout, crisi di fornitura — presidiata dalla ISO 22301, innestabile nello stesso sistema di gestione Compliance.

Il catalogo dei reati presupposto è in continua evoluzione: da ultimo, il D. Lgs. 9 settembre 2026, n. 160 — attuativo della L. 132/2025 in materia di intelligenza artificiale, in vigore dal 30 settembre 2026 — ha introdotto il nuovo delitto di omessa adozione di misure di sicurezza nei sistemi di IA tra i reati presupposto ex D. Lgs. 231/01: un'organizzazione che utilizza sistemi di IA deve quindi aggiornare la risk assessment del Modello, i protocolli di controllo e i piani di vigilanza dell'OdV, indipendentemente dal fatto che adotti anche un percorso di AI Governance dedicato.

PERCHÉ ADEGUARSI

RISCHIO - il mancato adeguamento espone l'organizzazione a sanzioni pecuniarie severe e, nei casi più gravi, a misure interdittive che possono compromettere l'operatività aziendale - sospensione dell'attività, esclusione da contratti pubblici, confisca del profitto del reato.

VALORI - un Modello 231 strutturato e sorretto da un sistema di gestione Compliance rafforza reputazione, affidabilità e moralità percepita dall'esterno, segnalando al mercato un impegno concreto verso legalità ed etica d'impresa.

BISOGNO - il Modello 231 è un primo passo verso gli adeguati assetti organizzativi, amministrativi e contabili richiesti dal Codice della Crisi d'Impresa, ed è spesso requisito preferenziale o abilitante nella partecipazione a bandi di gara pubblici.

SERVIZI EROGATI

- **Redazione e aggiornamento del MOGC** - modello calibrato sui rischi-reato effettivamente rilevanti per l'organizzazione
- **Ruolo in Organismo di Vigilanza o supporto all'OdV** - con delega su ambiti specifici d'indagine
- **Progettazione del canale di whistleblowing** - presidio a supporto della collaborazione e della compliance interna
- **Audit di conformità 231** - verifica periodica di adeguatezza e operatività del sistema
- **Formazione** - percorsi per vertici aziendali e personale coinvolto nella gestione dei rischi-reato
- **Implementazione ISO 37301** - sistema di gestione per la Compliance, che mantiene il Modello 231 vivo e aggiornato attraverso un ciclo di miglioramento continuo, e offre il framework naturale per integrare nello stesso sistema whistleblowing, antiriciclaggio e continuità operativa
- **Implementazione ISO 22301** - continuità operativa e gestione delle crisi (cyberattacchi, blackout, interruzioni di fornitura), a supporto della resilienza complessiva del sistema di gestione del rischio
  - ➥ **Assistenza alla certificazione ISO 37301–22301:** supporto in sede di verifica ispettiva dell'Organismo di certificazione (Audit di 3^ parte)
  - ➥ **Assistenza**, relativa ai suddetti schemi, **in sede di qualificazione dei propri fornitori o da parte dei propri clienti** (Audit di 2^ parte)
  - ➥ **Assistenza**, relativa ai suddetti schemi, **in sede di verifiche ispettive interne** (Audit di 1^ parte)
  - ➥ Le suddette attività possono riferirsi ai singoli Sistemi di gestione oppure al Sistema di gestione integrato totale o parziale.
- **Presidio di Governance e Organizzazione** - deleghe, poteri, chiarezza dei ruoli CdA/OdV, flussi informativi verso l'organo dirigente.

IL MIO CONTRIBUTO

La materia richiede competenze multidisciplinari, non riconducibili a un unico profilo professionale: presidio GRC (costruzione e aggiornamento del Modello 231, Organismo di Vigilanza, sistemi di gestione ISO 37301/22301), competenze tecniche specialistiche a seconda del rischio-reato coinvolto (sicurezza informatica per i reati informatici, sicurezza sul lavoro e ambiente per i reati specifici) e competenze legali.

Curo la componente GRC in prima persona, coinvolgendo le altre professionalità per quanto attiene ai rispettivi punti specifici in cui la materia lo richiede.

APPROFONDIMENTI

Estensione futura (facoltativa): Antiriciclaggio (AML/CFT) *— da sviluppare come passo successivo ed in presenza di presupposti. Il terreno è già in parte condiviso con questo pacchetto: il rischio-reato AML rientra tra i presupposti del Modello 231 (art. 25-octies D. Lgs. 231/01) e i relativi presidi si innestano naturalmente nel sistema di gestione ISO 37301 già attivo.*

Estensione futura (facoltativa): Governance ESG e rendicontazione (criteri S e G) *— estensione naturale del sistema di gestione Compliance già attivo, limitata agli aspetti di governance, whistleblowing e responsabilità sociale della rendicontazione CSRD/ESRS; esclusa la componente ambientale (criterio E), che resta territorio tecnico specialistico non coperto da questo pacchetto.*

Ampiezza ISO: *oltre a 22301 e 37301, restano disponibili su richiesta anche altri sistemi di gestione ISO (qualità, ambiente, sicurezza sul lavoro, energia, anticorruzione, sicurezza delle informazioni, ecc.), non promossi attivamente in questo pacchetto.*

Rating di legalità: *il Regolamento AGCM (art. 3) attribuisce punteggio premiale a chi adotta un Modello organizzativo ex D. Lgs. 231/01 e/o modelli di prevenzione della corruzione. Riservato a imprese con fatturato minimo di 2 milioni di euro. Il nuovo Regolamento AGCM, in vigore dal 16 marzo 2026, estende la durata del rating a 3 anni e introduce un punteggio premiale per i rinnovi continuativi. Tra i benefici concreti: riduzione del 20% della garanzia provvisoria nelle gare pubbliche (D. Lgs. 36/2023), accesso agevolato al credito bancario. È un risultato aggiuntivo del lavoro già previsto in questo pacchetto, non un servizio a sé da erogare separatamente.*

Nota bene: il pacchetto è concepito in forma integrata per massimizzare le sinergie tra i servizi, ma ciascuna componente può essere richiesta anche singolarmente, in base alle esigenze specifiche del cliente.