

PERCORSO FORMATIVO — AMMINISTRAZIONE, CONTROLLO E AUDITING

Dispensa 3

Compliance e Risk Management

Dalla gestione del rischio al D.Lgs. 231/2001: mappatura dei rischi, modelli organizzativi, whistleblowing e sistema disciplinare.

A cura di Marco Consiglio

Formatore e Course Director — Contenuti aggiornati al 2026

Indice

1. Introduzione e obiettivi didattici	3
2. Che cos'è la compliance: le basi	4
3. Il Risk Management: concetti fondamentali	6
4. Il processo di gestione del rischio	8
5. Il D.Lgs. 231/2001: origini e finalità	10
6. I reati presupposto	12
7. Il Modello di Organizzazione, Gestione e Controllo (MOG)	14
8. L'Organismo di Vigilanza (OdV)	16
9. Il sistema disciplinare	18
10. Whistleblowing: quadro normativo e procedure	19
11. La mappatura dei rischi-reato	21
12. Protocolli di controllo e flussi informativi	23
13. Altri ambiti di compliance: cenni	24
14. Il ruolo del Compliance Officer	26
15. Caso pratico guidato	27
16. Glossario dei termini chiave	29
17. Checklist finale e autoverifica	30
18. Riferimenti e risorse aggiornate al 2026	31

1. Introduzione e obiettivi didattici

Questa dispensa costituisce il terzo modulo del percorso formativo dedicato ad amministrazione, controllo e auditing. Dopo aver esplorato i fondamenti dell'auditing (Dispensa 1) e gli strumenti del controllo di gestione (Dispensa 2), affrontiamo ora un ambito diventato negli ultimi decenni sempre più centrale nella vita delle organizzazioni: la compliance, intesa come conformità a norme, standard e regole, e la gestione del rischio ad essa collegata (risk management).

Il fulcro normativo di questa dispensa è il Decreto Legislativo 8 giugno 2001, n. 231, la norma italiana che ha introdotto la responsabilità amministrativa degli enti per reati commessi da propri dirigenti o dipendenti nell'interesse o a vantaggio dell'organizzazione stessa. Si tratta di una delle normative più rilevanti per chiunque si occupi, a vario titolo, di controllo, auditing o governance aziendale.

A chi si rivolge questa dispensa

Il testo si rivolge, come il resto del percorso, a un pubblico adulto ed esperto che desidera comprendere, partendo da zero, la logica della compliance normativa e degli strumenti con cui un'organizzazione previene, gestisce e mitiga i rischi legali e reputazionali connessi alla propria attività.

Come è strutturata la dispensa

Partiamo dai concetti generali di compliance e risk management, per poi addentrarci nel dettaglio del D.Lgs. 231/2001: la sua origine, i reati presupposto, il Modello di Organizzazione e Gestione, l'Organismo di Vigilanza, il sistema disciplinare e il whistleblowing. Chiudiamo con un breve sguardo ad altri ambiti di compliance rilevanti (privacy, antiriciclaggio, anticorruzione) e con un caso pratico guidato.

Obiettivi di apprendimento

1. Comprendere il significato di compliance e la sua differenza rispetto ad audit e controllo di gestione;
2. Conoscere le fasi fondamentali del processo di gestione del rischio;
3. Comprendere la logica e la portata del D.Lgs. 231/2001;
4. Riconoscere la struttura e le finalità di un Modello di Organizzazione, Gestione e Controllo;
5. Comprendere il ruolo dell'Organismo di Vigilanza e del sistema di whistleblowing;
6. Applicare i concetti base della mappatura dei rischi-reato a un caso concreto.

2. Che cos'è la compliance: le basi

Il termine compliance, dall'inglese to comply (conformarsi, ottemperare), indica l'insieme delle attività attraverso cui un'organizzazione si assicura di rispettare le norme di legge, i regolamenti, gli standard tecnici e le proprie procedure interne applicabili alla propria attività.

Non si tratta di un concetto nuovo in assoluto — ogni organizzazione ha sempre dovuto, in qualche misura, rispettare le leggi vigenti — ma negli ultimi decenni la compliance si è affermata come funzione organizzativa strutturata e specialistica, dotata di risorse, procedure e responsabilità dedicate, in risposta alla crescente complessità normativa e ai rischi, anche reputazionali, connessi alla sua violazione.

Compliance, audit e controllo di gestione: come si integrano

Avendo già introdotto, nelle dispense precedenti, l'audit e il controllo di gestione, è utile chiarire come la compliance si collochi rispetto a queste discipline, con cui condivide strumenti e, spesso, personale, pur mantenendo una finalità specifica.

Disciplina	Finalità principale	Prospettiva tipica
Controllo di gestione	Raggiungere gli obiettivi economici e strategici	Efficienza ed efficacia
Audit	Verificare l'affidabilità di processi e dati	Verifica indipendente ex post
Compliance	Prevenire violazioni normative e i rischi ad esse connessi	Prevenzione ex ante

Perché la compliance è diventata così rilevante

Diversi fattori concorrono a spiegare la crescente centralità della funzione compliance nelle organizzazioni contemporanee:

- L'aumento della complessità e della frequenza di aggiornamento del quadro normativo, in ambiti come privacy, sicurezza, ambiente, antiriciclaggio, mercati finanziari;
- L'introduzione, in molti ordinamenti, di forme di responsabilità dell'ente (e non solo della persona fisica autrice del reato), che rendono l'organizzazione stessa sanzionabile;
- La crescente sensibilità dei portatori di interesse (investitori, clienti, partner commerciali) verso la reputazione etica e legale delle organizzazioni con cui si relazionano;
- La diffusione di standard internazionali di compliance, come la norma ISO 37301 sui sistemi di gestione della conformità.

Una buona funzione di compliance non si limita a verificare il rispetto delle regole esistenti: contribuisce a costruire una cultura organizzativa in cui la legalità e l'integrità sono percepite come valori condivisi, non come vincoli imposti dall'esterno.

3. Il Risk Management: concetti fondamentali

Il risk management, o gestione del rischio, è la disciplina che si occupa di identificare, analizzare e gestire gli eventi incerti che potrebbero influenzare, positivamente o negativamente, il raggiungimento degli obiettivi di un'organizzazione. È uno dei pilastri concettuali su cui si fonda anche la compliance, poiché una funzione di conformità efficace non può prescindere da una corretta comprensione dei rischi a cui l'organizzazione è esposta.

Che cos'è, tecnicamente, il rischio

Coerentemente con quanto già introdotto nella Dispensa 1 a proposito del risk-based auditing, il rischio viene definito come la combinazione tra la probabilità che un evento si verifichi e l'impatto che tale evento avrebbe sul raggiungimento degli obiettivi organizzativi. È importante sottolineare che, nella definizione tecnica più moderna (si veda ad esempio lo standard ISO 31000), il rischio non è necessariamente negativo: può rappresentare anche un'opportunità mancata, oltre che una minaccia.

Le principali categorie di rischio aziendale

- Rischi strategici: legati alle scelte di posizionamento competitivo e di sviluppo dell'organizzazione;
- Rischi operativi: legati al funzionamento quotidiano dei processi interni (errori, guasti, interruzioni);
- Rischi finanziari: legati alla liquidità, al credito, ai tassi di interesse e di cambio;
- Rischi di compliance (o legali): legati alla violazione di norme, regolamenti o contratti;
- Rischi reputazionali: legati al danno d'immagine derivante da eventi negativi, anche non direttamente collegati a violazioni normative;
- Rischi tecnologici e informatici: legati alla sicurezza dei sistemi informativi e alla protezione dei dati.

Il concetto di appetito al rischio (risk appetite)

Un concetto centrale nel risk management moderno è l'appetito al rischio: il livello di rischio che un'organizzazione è disposta ad accettare nel perseguimento dei propri obiettivi. Non tutte le organizzazioni hanno lo stesso appetito al rischio: un ente pubblico o una struttura sanitaria avranno tipicamente un appetito al rischio molto basso, specie sui rischi di compliance, mentre una start-up tecnologica potrà accettare livelli di rischio più elevati su alcune dimensioni, in cambio di maggiori opportunità di crescita.

Definire esplicitamente il proprio appetito al rischio, anche in modo qualitativo, aiuta un'organizzazione a prendere decisioni coerenti nel tempo, evitando che scelte importanti vengano fatte caso per caso, senza una cornice di riferimento condivisa.

Lo standard ISO 31000

Lo standard internazionale ISO 31000 fornisce linee guida generali, applicabili a qualunque tipo di organizzazione e settore, per la gestione del rischio. Non è uno standard certificabile in senso stretto (a differenza di ISO 9001 o ISO 45001), ma rappresenta un riferimento concettuale ampiamente adottato per strutturare i processi di risk management, incluso quello alla base dei modelli organizzativi ex D.Lgs. 231/2001 che approfondiremo nei capitoli successivi.

4. Il processo di gestione del rischio

Indipendentemente dallo standard specifico adottato, il processo di gestione del rischio si articola tipicamente in fasi ricorrenti, che è utile conoscere in dettaglio poiché costituiscono la base metodologica anche della mappatura dei rischi-reato prevista dal D.Lgs. 231/2001.

Fase 1 — Identificazione del rischio

Consiste nell'individuare in modo sistematico i possibili eventi di rischio rilevanti per l'organizzazione, attraverso interviste, analisi documentale, workshop con i responsabili di processo, analisi di eventi passati (anche di altre organizzazioni del settore).

Fase 2 — Analisi del rischio

Per ciascun rischio identificato, si analizzano le cause potenziali e le possibili conseguenze, distinguendo i fattori che potrebbero far scaturire l'evento (i cosiddetti risk driver) dagli effetti che ne deriverebbero.

Fase 3 — Valutazione del rischio

Si attribuisce a ciascun rischio un livello di priorità, tipicamente calcolato come combinazione di probabilità e impatto, spesso rappresentato attraverso una matrice di rischio (risk matrix), che permette una visualizzazione immediata delle aree più critiche.

Esempio semplificato di matrice di rischio

Probabilità Alta + Impatto Alto → Rischio Critico (priorità massima di intervento)

Probabilità Alta + Impatto Basso → Rischio Moderato (monitoraggio regolare)

Probabilità Basso + Impatto Alto → Rischio Significativo (piani di contingenza)

Probabilità Basso + Impatto Basso → Rischio Marginale (accettazione con monitoraggio periodico)

Fase 4 — Trattamento del rischio

Per ciascun rischio rilevante, l'organizzazione decide una strategia di trattamento, tra quattro opzioni tipiche:

1. Evitare il rischio: rinunciare all'attività che lo genera (ad esempio non entrare in un determinato mercato);
2. Ridurre il rischio: introdurre controlli o procedure che ne riducano probabilità e/o impatto;
3. Trasferire il rischio: spostarne parzialmente l'onere su un soggetto terzo (ad esempio tramite polizze assicurative o clausole contrattuali);
4. Accettare il rischio: quando il costo di ulteriori interventi supererebbe il beneficio atteso, consapevolmente e con adeguata documentazione della decisione presa.

Fase 5 — Monitoraggio e revisione

Il rischio non è mai una fotografia statica: cambiamenti normativi, organizzativi, di mercato o tecnologici possono modificare nel tempo probabilità e impatto dei rischi identificati. Il processo di risk management richiede quindi un monitoraggio continuo e una revisione periodica della mappa dei rischi, con una logica ciclica non dissimile da quella già incontrata a proposito del controllo di gestione.

Una mappa dei rischi costruita una sola volta, e mai più aggiornata, perde rapidamente di utilità: il risk management è un processo continuo, non un adempimento da completare una tantum.

5. Il D.Lgs. 231/2001: origini e finalità

Il Decreto Legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", ha introdotto nell'ordinamento italiano un principio fino ad allora estraneo alla nostra tradizione giuridica: la responsabilità dell'ente (società, associazione, ente) per alcuni reati commessi, nel suo interesse o a suo vantaggio, da amministratori, dirigenti o dipendenti.

Il principio del "societas delinquere non potest" e il suo superamento

La tradizione giuridica italiana si fondava storicamente sul principio secondo cui solo le persone fisiche possono essere ritenute responsabili di un reato (*societas delinquere non potest*, "la società non può commettere reato"). Il D.Lgs. 231/2001 supera parzialmente questo principio, introducendo una responsabilità dell'ente che si affianca, senza sostituirla, a quella della persona fisica autrice materiale del reato.

Perché si parla di responsabilità "amministrativa" e non "penale"

Formalmente, il legislatore ha definito questa responsabilità come amministrativa, pur essendo accertata dal giudice penale nell'ambito dello stesso procedimento riguardante il reato commesso dalla persona fisica. Questa scelta terminologica, spesso oggetto di dibattito dottrinale, non deve trarre in inganno circa la severità delle conseguenze: le sanzioni previste per l'ente possono essere estremamente rilevanti.

Le sanzioni previste per l'ente

- Sanzione pecuniaria: calcolata attraverso un sistema per quote, che tiene conto della gravità del fatto e delle condizioni economiche dell'ente;
- Sanzioni interdittive: possono includere l'interdizione dall'esercizio dell'attività, la sospensione o revoca di autorizzazioni e licenze, il divieto di contrattare con la Pubblica Amministrazione, l'esclusione da agevolazioni e finanziamenti, il divieto di pubblicizzare beni o servizi;
- Confisca del profitto derivante dal reato;
- Pubblicazione della sentenza di condanna, con evidenti effetti reputazionali.

La condizione esimente: il Modello 231

Il cuore applicativo del decreto, dal punto di vista organizzativo, risiede in un principio fondamentale: l'ente non risponde se dimostra di aver adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione, Gestione e Controllo (comunemente denominato Modello 231 o MOG) idoneo a prevenire reati della specie di quello verificatosi, e se ha affidato la vigilanza sul suo funzionamento a un apposito Organismo di Vigilanza dotato di autonomi poteri di iniziativa e controllo.

Il D.Lgs. 231/2001 non impone alle organizzazioni un obbligo generalizzato di adottare un Modello 231: l'adozione resta, in linea di principio, facoltativa. Tuttavia, in assenza di un modello idoneo, l'ente risponde automaticamente in caso di reato commesso nel suo interesse o vantaggio da soggetti apicali o sottoposti: per questo motivo, nella pratica, l'adozione del modello è fortemente raccomandata per qualunque organizzazione strutturata.

6. I reati presupposto

Il D.Lgs. 231/2001 non si applica a qualunque reato, ma soltanto a un elenco tassativo di fattispecie, definite reati presupposto, progressivamente ampliato nel corso degli anni attraverso numerosi interventi legislativi successivi al testo originario del 2001.

Le principali famiglie di reati presupposto

Pur non essendo questa la sede per un elenco esaustivo — la materia richiede un aggiornamento normativo costante — è utile conoscere le principali categorie di reati oggi rilevanti ai fini del decreto:

- Reati contro la Pubblica Amministrazione (corruzione, concussione, induzione indebita, truffa ai danni dello Stato);
- Reati societari (false comunicazioni sociali, aggrataggio, ostacolo alla vigilanza);
- Reati di criminalità organizzata e reati transnazionali;
- Reati di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro di provenienza illecita;
- Reati in materia di sicurezza sul lavoro (omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme antinfortunistiche);
- Reati ambientali;
- Reati informatici e trattamento illecito di dati;
- Reati in materia di diritto d'autore;
- Reati tributari (introdotti tra gli interventi più recenti sul decreto);
- Reati in materia di salute pubblica e sicurezza dei prodotti.

Perché conoscere questo elenco è importante, ma non sufficiente

Un errore diffuso, anche tra professionisti non specializzati, è pensare che basti "conoscere l'elenco" dei reati presupposto per costruire un buon Modello 231. In realtà, ciò che rende davvero efficace il modello è la capacità di calare questi reati astratti nella realtà concreta dell'organizzazione: quali, tra queste fattispecie, sono realisticamente ipotizzabili nel contesto specifico in cui l'ente opera? Un'associazione culturale di piccole dimensioni, ad esempio, avrà un'esposizione molto diversa rispetto a un'impresa edile che opera con appalti pubblici.

L'importanza dell'aggiornamento continuo

L'elenco dei reati presupposto è stato più volte ampliato dal legislatore italiano dal 2001 a oggi, e nulla esclude ulteriori estensioni future, anche in recepimento di normative europee. Una buona funzione di compliance deve quindi prevedere un monitoraggio costante degli aggiornamenti normativi, aggiornando di conseguenza la mappatura dei rischi e, se necessario, il Modello di Organizzazione stesso.

Un Modello 231 costruito una sola volta e mai aggiornato, magari acquistato come semplice modello standard da un fornitore esterno senza un reale adattamento alla specifica realtà organizzativa, rischia di rivelarsi del tutto inefficace ai fini esimenti previsti dal decreto: la giurisprudenza ha più volte sottolineato la necessità di un modello realmente calato sulla concreta organizzazione dell'ente.

7. Il Modello di Organizzazione, Gestione e Controllo (MOG)

Il Modello di Organizzazione, Gestione e Controllo, comunemente abbreviato in Modello 231 o MOG, è il documento (o, più correttamente, l'insieme organico di documenti, procedure e regole) attraverso cui l'ente struttura il proprio sistema di prevenzione dei reati presupposto.

Gli elementi costitutivi di un Modello 231

Sebbene ogni modello debba essere costruito su misura per la specifica organizzazione, esistono elementi ricorrenti che ogni Modello 231 dovrebbe includere, secondo l'impostazione consolidata sia in dottrina sia nella prassi applicativa:

5. Mappatura delle attività a rischio-reato (approfondita nel capitolo 11);
6. Protocolli di controllo specifici per ciascuna area a rischio identificata (approfonditi nel capitolo 12);
7. Un Codice Etico (o Codice di Comportamento), che definisce i principi e i valori a cui l'organizzazione e i suoi collaboratori devono ispirarsi;
8. Un sistema disciplinare, idoneo a sanzionare il mancato rispetto delle misure previste dal modello (approfondito nel capitolo 9);
9. L'istituzione di un Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e controllo (approfondito nel capitolo 8);
10. Un piano di formazione e comunicazione, per assicurare che il modello sia effettivamente conosciuto da tutti i destinatari;
11. Un sistema di whistleblowing per la segnalazione di illeciti (approfondito nel capitolo 10).

Parte generale e parti speciali

Un Modello 231 si articola tipicamente in una Parte Generale, che descrive il quadro normativo di riferimento, la struttura del modello, il ruolo dell'Organismo di Vigilanza e il sistema disciplinare, e diverse Parti Speciali, ciascuna dedicata a una specifica famiglia di reati presupposto rilevante per l'organizzazione, con l'indicazione dei protocolli di controllo specifici per le relative aree a rischio.

I requisiti di idoneità del modello secondo il decreto

L'art. 6 del D.Lgs. 231/2001 individua espressamente i requisiti che un modello deve possedere per poter produrre l'effetto esimente della responsabilità dell'ente:

- Individuare le attività nel cui ambito possono essere commessi i reati;
- Prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

- Individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- Prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- Introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Un modello "sulla carta" non basta

La sola adozione formale del documento non è sufficiente: il decreto richiede che il modello sia efficacemente attuato, cioè realmente applicato nella pratica quotidiana dell'organizzazione, con adeguata formazione del personale, effettiva operatività dei protocolli di controllo e reale autonomia dell'Organismo di Vigilanza. Questo aspetto sarà oggetto, tipicamente, di specifica verifica anche da parte di un auditor interno o esterno chiamato a valutare l'effettività del sistema di compliance.

8. L'Organismo di Vigilanza (OdV)

L'Organismo di Vigilanza, comunemente indicato con l'acronimo OdV, è l'organo a cui il decreto affida il compito di vigilare sul funzionamento e sull'osservanza del Modello 231, nonché di curarne l'aggiornamento nel tempo.

I requisiti richiesti dalla norma e dalla prassi applicativa

- Autonomia e indipendenza: l'OdV deve poter operare senza condizionamenti da parte degli organi gestori dell'ente, con una collocazione gerarchica adeguata (tipicamente in staff al massimo vertice aziendale);
- Professionalità: i componenti devono possedere competenze adeguate, spesso multidisciplinari (legali, organizzative, di controllo interno, di auditing);
- Continuità di azione: l'OdV deve operare con costanza nel tempo, non limitandosi a interventi occasionali o episodici;
- Onorabilità: i componenti devono essere privi di conflitti di interesse o precedenti che ne comprometterebbero la credibilità.

La composizione dell'Organismo di Vigilanza

La legge non impone una composizione specifica, lasciando alle organizzazioni la libertà di scegliere la soluzione più adeguata alla propria dimensione e complessità. Nella prassi si riscontrano diverse soluzioni:

- OdV monocratico: composto da un solo membro, tipicamente in organizzazioni di dimensioni contenute;
- OdV collegiale: composto da più membri, spesso con un mix di componenti interni ed esterni all'organizzazione, per bilanciare conoscenza diretta dei processi interni e indipendenza di giudizio;
- OdV in composizione mista con altre funzioni di controllo (ad esempio, in alcuni casi, con il collegio sindacale), soluzione ammessa a determinate condizioni, ma generalmente sconsigliata nelle organizzazioni di maggiore complessità per il rischio di sovrapposizione di ruoli.

Le principali attività dell'Organismo di Vigilanza

12. Verificare periodicamente l'adeguatezza e l'effettiva applicazione del Modello 231, anche attraverso audit mirati sulle aree a rischio;
13. Ricevere e gestire le segnalazioni di presunte violazioni, incluse quelle pervenute attraverso il canale di whistleblowing;
14. Proporre l'aggiornamento del modello in caso di modifiche normative, organizzative o di processo rilevanti;

15. Coordinarsi con le altre funzioni di controllo dell'organizzazione (audit interno, compliance, risk management), evitando duplicazioni ma garantendo un flusso informativo adeguato;
16. Relazionare periodicamente agli organi di vertice sull'attività svolta e sullo stato di attuazione del modello.

Un Organismo di Vigilanza privo di reale autonomia — ad esempio composto esclusivamente da soggetti in rapporto di subordinazione gerarchica con chi dovrebbe vigilare, o privo di risorse e poteri di iniziativa effettivi — rischia di rendere il modello inefficace ai fini esimenti, anche qualora la documentazione formale risultasse, sulla carta, ineccepibile.

9. Il sistema disciplinare

Come già anticipato, uno dei requisiti di idoneità del Modello 231 è la presenza di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure previste dal modello stesso. Si tratta di un elemento spesso sottovalutato, ma essenziale: un modello privo di conseguenze concrete in caso di violazione perde gran parte della propria efficacia deterrente.

A chi si applica il sistema disciplinare

Il sistema disciplinare deve poter trovare applicazione nei confronti di tutti i destinatari del modello, distinguendo tipicamente tra categorie di soggetti con regole procedurali diverse:

- Dipendenti (dirigenti e non dirigenti): soggetti alle procedure disciplinari previste dal Contratto Collettivo Nazionale di Lavoro applicabile e dallo Statuto dei Lavoratori;
- Amministratori: le violazioni possono comportare, a seconda dei casi, la proposta di revoca dell'incarico o altre misure previste dallo statuto sociale;
- Collaboratori esterni, fornitori, partner commerciali: le conseguenze sono tipicamente regolate attraverso apposite clausole contrattuali, che possono prevedere la risoluzione del rapporto in caso di violazioni gravi del Modello 231 o del Codice Etico.

La proporzionalità delle sanzioni

Un buon sistema disciplinare deve prevedere una gradazione delle sanzioni proporzionata alla gravità della violazione riscontrata, dal semplice richiamo verbale fino, nei casi più gravi, al licenziamento per giusta causa (per i dipendenti) o alla risoluzione contrattuale (per i collaboratori esterni). È inoltre opportuno che le sanzioni possano essere applicate anche in assenza di un accertamento penale definitivo del reato: il sistema disciplinare sanziona infatti la violazione delle procedure interne previste dal modello, non il reato in sé, la cui eventuale sussistenza è materia di competenza esclusiva dell'autorità giudiziaria.

Un principio da ricordare

Il sistema disciplinare previsto dal Modello 231 sanziona il mancato rispetto delle regole procedurali interne (ad esempio, la mancata compilazione di una checklist obbligatoria, l'omessa comunicazione all'OdV di un'informazione rilevante), indipendentemente dal fatto che tale violazione abbia effettivamente condotto, o meno, alla commissione di un reato. Questo aspetto, spesso frainteso, è centrale per comprendere la reale finalità preventiva — e non meramente repressiva — del sistema.

10. Whistleblowing: quadro normativo e procedure

Il termine whistleblowing (letteralmente "soffiare nel fischietto") indica la segnalazione, da parte di un soggetto interno o comunque collegato all'organizzazione, di condotte illecite o irregolarità di cui sia venuto a conoscenza nell'ambito della propria attività lavorativa o professionale.

L'evoluzione normativa in Italia

La disciplina italiana in materia di whistleblowing si è progressivamente rafforzata nel corso degli anni, sia in ambito pubblico sia, successivamente, in ambito privato, anche in attuazione di una specifica direttiva dell'Unione Europea in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione. Le organizzazioni che adottano un Modello 231, in particolare, sono tenute a integrare al proprio interno canali di segnalazione conformi ai requisiti previsti dalla normativa vigente.

Le caratteristiche di un buon sistema di whistleblowing

- Riservatezza (o, ove tecnicamente possibile, anonimato) dell'identità del segnalante, adeguatamente tutelata durante tutto il processo di gestione della segnalazione;
- Accessibilità e semplicità del canale di segnalazione, tipicamente attraverso una piattaforma digitale dedicata, ma anche mediante canali alternativi (ad esempio segnalazione scritta cartacea, per chi non avesse accesso agevole agli strumenti digitali);
- Tutela del segnalante da ogni forma di ritorsione (demansionamento, licenziamento, discriminazione, molestie), sia diretta sia indiretta;
- Tempestività nella gestione della segnalazione, con termini definiti per la presa in carico e per il riscontro al segnalante, ove possibile senza comprometterne la riservatezza;
- Tutela anche del segnalato, che ha diritto a un processo equo e alla presunzione di correttezza fino a diverso accertamento, evitando che il sistema si trasformi in uno strumento di delazione strumentale.

Le fasi tipiche di gestione di una segnalazione

17. Ricezione della segnalazione attraverso il canale dedicato, con eventuale conferma di ricezione al segnalante;
18. Prima valutazione di ammissibilità (la segnalazione rientra nell'ambito di applicazione della normativa e delle procedure interne?);
19. Istruttoria e verifica dei fatti segnalati, condotta con modalità che tutelino la riservatezza di tutte le parti coinvolte;
20. Conclusione dell'istruttoria, con eventuale attivazione del sistema disciplinare o di altre misure correttive, ove i fatti risultino fondati;

21. Riscontro al segnalante, nei limiti consentiti dalla riservatezza dell'istruttoria e dalla normativa applicabile;
22. Archiviazione della documentazione, con modalità che garantiscano la protezione dei dati personali coinvolti.

Un sistema di whistleblowing percepito come inaffidabile — ad esempio perché in passato non ha garantito adeguata riservatezza, o perché le segnalazioni non hanno mai prodotto conseguenze concrete — perde rapidamente credibilità presso i potenziali segnalanti, vanificandone l'utilità preventiva. La fiducia nel sistema si costruisce nel tempo, con coerenza tra le procedure dichiarate e la pratica effettiva.

11. La mappatura dei rischi-reato

La mappatura dei rischi-reato (o risk assessment 231) è il processo attraverso cui l'organizzazione individua, in relazione alla propria specifica attività, quali reati presupposto siano concretamente ipotizzabili, in quali processi o aree aziendali, e con quale livello di esposizione. Costituisce il fondamento di ogni Modello 231 realmente efficace, applicando alla materia specifica i principi generali di risk management già illustrati nei capitoli 3 e 4.

Le fasi tipiche della mappatura

23. Analisi del contesto organizzativo: struttura societaria, settore di attività, mercati di riferimento, rapporti con la Pubblica Amministrazione, presenza di operazioni infragruppo;
24. Individuazione dei processi sensibili: le aree aziendali in cui, per la loro natura, potrebbero astrattamente essere commessi i reati presupposto rilevanti (ad esempio gestione degli appalti pubblici, gestione degli omaggi e delle spese di rappresentanza, selezione dei fornitori, gestione della cassa, rapporti con enti certificatori o ispettivi);
25. Individuazione dei reati astrattamente ipotizzabili per ciascun processo sensibile identificato;
26. Valutazione del livello di rischio residuo, tenendo conto dei controlli già esistenti (ad esempio segregazione dei compiti, sistemi autorizzativi, tracciabilità documentale);
27. Individuazione delle eventuali carenze di controllo (control gap) e definizione dei protocolli integrativi necessari a colmarle.

Un esempio pratico semplificato

Consideriamo, a titolo esemplificativo, il processo di gestione degli omaggi e delle spese di rappresentanza in un'impresa che opera anche con clienti pubblici. Il rischio-reato astrattamente ipotizzabile è quello di corruzione, qualora un omaggio di valore eccessivo o non adeguatamente documentato venisse interpretato come un tentativo di influenzare indebitamente un funzionario pubblico. La mappatura porterebbe a individuare, come protocollo di controllo, ad esempio: la definizione di un tetto massimo di valore per gli omaggi consentiti, l'obbligo di autorizzazione preventiva per omaggi verso soggetti pubblici, la tracciabilità documentale di ogni omaggio erogato.

Documentare correttamente la mappatura

Coerentemente con quanto già visto nella Dispensa 1 a proposito delle carte di lavoro, anche la mappatura dei rischi-reato deve essere adeguatamente documentata, in modo da poter dimostrare, in caso di necessità, il percorso logico seguito e le motivazioni alla base delle scelte operate. Una mappatura ben documentata costituisce, essa stessa, un elemento di prova dell'effettiva diligenza organizzativa dell'ente.

Un aggiornamento non episodico

La mappatura dei rischi-reato non è un esercizio da svolgere una tantum al momento dell'adozione del modello, ma un processo da aggiornare periodicamente e ogni volta che intervengano modifiche significative: nuove linee di business, nuovi mercati geografici, operazioni straordinarie (fusioni, acquisizioni), o semplicemente l'ampliamento dell'elenco dei reati presupposto da parte del legislatore, come illustrato nel capitolo 6.

12. Protocolli di controllo e flussi informativi

Individuati i processi sensibili e i relativi rischi–reato, il Modello 231 deve prevedere protocolli di controllo specifici, cioè regole operative concrete finalizzate a prevenire la commissione dei reati identificati, e adeguati flussi informativi verso l'Organismo di Vigilanza.

Le caratteristiche di un buon protocollo di controllo

- Concretezza: deve tradursi in comportamenti operativi verificabili, non in mere dichiarazioni di principio;
- Segregazione dei compiti: nessun soggetto dovrebbe poter gestire, da solo, l'intero ciclo di un'operazione sensibile (ad esempio autorizzare, eseguire e controllare lo stesso pagamento);
- Tracciabilità: ogni fase rilevante del processo deve lasciare traccia documentale, coerentemente con il principio più volte richiamato in questa dispensa e nelle precedenti;
- Proporzionalità: il livello di controllo deve essere proporzionato al livello di rischio del processo, evitando burocratizzazioni eccessive su attività a basso rischio.

Esempi di protocolli tipici

28. Doppia firma o approvazione gerarchica per operazioni sopra una determinata soglia economica;
29. Rotazione periodica del personale su ruoli particolarmente esposti a rischio (ad esempio nella gestione degli acquisti);
30. Procedure strutturate di due diligence per la selezione di fornitori, agenti e consulenti, specie in Paesi a maggior rischio di corruzione;
31. Registri specifici per la tracciabilità di omaggi, sponsorizzazioni, liberalità;
32. Procedure autorizzative rafforzate per i rapporti con pubblici ufficiali o incaricati di pubblico servizio.

I flussi informativi verso l'Organismo di Vigilanza

Perché l'OdV possa svolgere efficacemente il proprio ruolo di vigilanza, il Modello 231 deve prevedere specifici flussi informativi obbligatori, che assicurino all'Organismo un accesso tempestivo e sistematico alle informazioni rilevanti. Tra gli esempi più comuni:

- Comunicazione periodica di indicatori relativi alle aree a rischio monitorate (ad esempio numero di operazioni sopra soglia, esito dei controlli su fornitori sensibili);
- Segnalazione immediata di eventi rilevanti (ispezioni, procedimenti giudiziari, contestazioni da parte di autorità di vigilanza);
- Trasmissione dell'esito di eventuali audit interni condotti sulle aree sensibili;

- Comunicazione di modifiche organizzative rilevanti (nuove linee di business, riorganizzazioni, operazioni straordinarie).

Un protocollo di controllo scritto ma non realmente applicato nella pratica quotidiana è, ai fini del D.Lgs. 231/2001, quasi peggio che l'assenza di un protocollo: la giurisprudenza tende infatti a valutare con particolare severità la distanza tra il modello formale dichiarato e la sua effettiva attuazione operativa.

13. Altri ambiti di compliance: cenni

Il D.Lgs. 231/2001, per quanto centrale, non esaurisce il panorama della compliance normativa che un'organizzazione moderna deve presidiare. È utile, a completamento del quadro generale offerto in questa dispensa, un breve cenno ad altri ambiti rilevanti, alcuni dei quali verranno eventualmente approfonditi in dispense dedicate del percorso.

13.1 Protezione dei dati personali (privacy)

La normativa in materia di protezione dei dati personali, di matrice europea, impone alle organizzazioni obblighi specifici in tema di trattamento dei dati, misure di sicurezza tecniche e organizzative, informativa agli interessati, gestione di eventuali violazioni dei dati (data breach). La figura del Responsabile della Protezione dei Dati (RPD, o DPO nell'acronimo inglese) è obbligatoria per determinate categorie di soggetti.

13.2 Antiriciclaggio

La normativa antiriciclaggio impone, a determinate categorie di soggetti obbligati (istituti finanziari, ma anche professionisti, operatori immobiliari e altre categorie specificamente individuate), obblighi di adeguata verifica della clientela, registrazione delle operazioni e segnalazione di operazioni sospette alle autorità competenti.

13.3 Anticorruzione nel settore pubblico

Per gli enti pubblici e per i soggetti che con essi interagiscono stabilmente, esiste un quadro normativo specifico in materia di prevenzione della corruzione, che prevede l'adozione di Piani Triennali di Prevenzione della Corruzione e Trasparenza (PTPCT) e la nomina di un Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), figura per molti aspetti assimilabile, nella logica sottostante, all'Organismo di Vigilanza previsto dal D.Lgs. 231/2001 in ambito privato.

13.4 Sistemi di gestione della compliance: la norma ISO 37301

Accanto agli obblighi normativi specifici, si è progressivamente affermato uno standard internazionale volontario, la norma ISO 37301, che fornisce un framework generale per la costruzione di un sistema di gestione della compliance, applicabile trasversalmente a qualunque ambito normativo rilevante per l'organizzazione, secondo una logica per molti aspetti affine a quella già incontrata a proposito di altri sistemi di gestione certificabili (qualità, sicurezza, ambiente).

Un principio unificante

Pur nella diversità degli ambiti normativi specifici, tutte le discipline di compliance qui richiamate condividono una logica di fondo comune: identificazione dei rischi normativi rilevanti, definizione di procedure e controlli preventivi, formazione dei soggetti coinvolti, monitoraggio continuo e capacità di reagire tempestivamente alle violazioni riscontrate. Chi ha compreso a fondo la logica del D.Lgs.

231/2001, illustrata in questa dispensa, possiede già gran parte degli strumenti concettuali necessari per orientarsi in questi ambiti affini.

14. Il ruolo del Compliance Officer

Il Compliance Officer (o responsabile compliance) è la figura professionale, sempre più diffusa nelle organizzazioni di media e grande dimensione, incaricata di presidiare in modo continuativo il sistema di conformità normativa, in stretto raccordo con l'Organismo di Vigilanza, laddove quest'ultimo sia un organo distinto.

Le competenze chiave del Compliance Officer

- Conoscenza approfondita del quadro normativo rilevante per il settore specifico di attività dell'organizzazione;
- Capacità di tradurre requisiti normativi complessi in procedure operative chiare e applicabili;
- Capacità di formazione e comunicazione, per diffondere efficacemente la cultura della compliance a tutti i livelli organizzativi;
- Capacità di analisi del rischio, secondo la metodologia illustrata nei capitoli 3 e 4;
- Autorevolezza e capacità di dialogo con il vertice aziendale, necessarie per garantire che le segnalazioni di criticità vengano prese realmente in considerazione.

Compliance Officer, Organismo di Vigilanza e Internal Audit: un ecosistema di controllo

Nelle organizzazioni più strutturate, queste tre funzioni — compliance, Organismo di Vigilanza (quando distinto da un ruolo interno) e audit interno — operano in stretto coordinamento, evitando sovrapposizioni ma garantendo una copertura complessiva del sistema di controllo. È buona prassi che tali funzioni si scambino informazioni periodicamente e coordinino, ove possibile, i rispettivi piani di verifica, evitando duplicazioni di attività verso le stesse aree aziendali in tempi ravvicinati.

Una funzione di compliance efficace non si limita a un ruolo di controllo formale: contribuisce attivamente, insieme al management, alla costruzione di processi organizzativi che siano, fin dalla loro progettazione, coerenti con il quadro normativo applicabile — un approccio spesso definito "compliance by design", per analogia con il concetto di "security by design" proprio dell'ambito informatico.

15. Caso pratico guidato

Concludiamo la parte teorica con un caso pratico semplificato, che ripercorre le fasi principali della costruzione di un sistema di compliance ex D.Lgs. 231/2001, applicando i concetti illustrati nei capitoli precedenti.

Il contesto

Un'impresa di costruzioni di medie dimensioni, che partecipa regolarmente a gare d'appalto pubbliche, decide di adottare per la prima volta un Modello 231, avendo ricevuto sollecitazioni in tal senso da un importante committente pubblico, che ne condiziona la partecipazione a future gare alla dimostrazione di un adeguato sistema di controllo interno.

Passo 1 — Analisi del contesto e mappatura dei rischi

Viene condotta un'analisi del contesto organizzativo, che evidenzia due aree particolarmente sensibili: la partecipazione a gare pubbliche (rischio di corruzione e turbativa d'asta) e la gestione della sicurezza nei cantieri (rischio di reati colposi in materia di sicurezza sul lavoro, particolarmente rilevante in questo settore).

Passo 2 — Costruzione dei protocolli di controllo

Per l'area gare pubbliche, viene introdotto un protocollo che prevede: la separazione tra chi predispone l'offerta tecnico-economica e chi autorizza eventuali contatti con la stazione appaltante, un registro degli omaggi e degli inviti a eventi ricevuti da funzionari pubblici, una procedura di due diligence sui subappaltatori. Per l'area sicurezza, il modello richiama e integra il sistema di gestione della sicurezza già esistente in azienda (approfondito, per chi fosse interessato, in una successiva dispensa dedicata specificamente al tema), rafforzando i flussi informativi verso l'Organismo di Vigilanza in caso di infortuni o quasi-infortuni rilevanti.

Passo 3 — Istituzione dell'Organismo di Vigilanza

Data la dimensione dell'impresa, si opta per un Organismo di Vigilanza collegiale, composto da un professionista esterno con competenze legali, un responsabile interno della funzione sicurezza e un membro con competenze di controllo di gestione, per assicurare una visione multidisciplinare adeguata alle aree di rischio identificate.

Passo 4 — Formazione e comunicazione

Viene predisposto un piano di formazione differenziato: una formazione generale sul Codice Etico e sui principi del Modello 231 per tutto il personale, e una formazione specifica e più approfondita per i soggetti operanti nelle aree a maggior rischio (ufficio gare, direzione cantieri, amministrazione).

Passo 5 — Attivazione del canale di whistleblowing

Viene attivato un canale di segnalazione dedicato, con adeguate garanzie di riservatezza, comunicato a tutto il personale e ai principali collaboratori esterni attraverso il sito istituzionale dell'impresa e specifiche clausole contrattuali.

Che cosa insegna questo caso

Il caso mostra come la costruzione di un Modello 231 richieda un lavoro di analisi realmente calato sulla specifica attività dell'organizzazione — in questo caso il settore delle costruzioni e degli appalti pubblici — piuttosto che l'adozione di un modello standardizzato e generico, coerentemente con quanto già sottolineato nel capitolo 6 a proposito dell'importanza di un modello effettivamente su misura.

16. Glossario dei termini chiave

Come per le dispense precedenti del percorso, riportiamo un glossario di sintesi dei principali termini tecnici introdotti.

Compliance	Conformità dell'organizzazione a norme di legge, regolamenti, standard tecnici e procedure interne applicabili.
Risk management	Disciplina che si occupa di identificare, analizzare e gestire gli eventi incerti rilevanti per il raggiungimento degli obiettivi organizzativi.
D.Lgs. 231/2001	Normativa italiana che introduce la responsabilità amministrativa degli enti per reati commessi nel loro interesse o vantaggio.
Reato presupposto	Fattispecie di reato espressamente prevista dal D.Lgs. 231/2001 come idonea a generare la responsabilità dell'ente.
Modello 231 (MOG)	Modello di Organizzazione, Gestione e Controllo adottato dall'ente per prevenire la commissione dei reati presupposto.
Organismo di Vigilanza (OdV)	Organo dotato di autonomi poteri di iniziativa e controllo, incaricato di vigilare sul funzionamento e l'osservanza del Modello 231.
Whistleblowing	Segnalazione di condotte illecite o irregolarità da parte di un soggetto interno o collegato all'organizzazione.
Mappatura dei rischi-reato	Processo di identificazione dei processi sensibili e dei reati presupposto astrattamente ipotizzabili in relazione alla specifica attività dell'ente.
Protocollo di controllo	Regola operativa concreta finalizzata a prevenire la commissione di un reato presupposto in un'area di rischio identificata.
Codice Etico	Documento che definisce i principi e i valori a cui l'organizzazione e i suoi collaboratori devono ispirarsi nella propria condotta.
Compliance Officer	Figura professionale incaricata di presidiare in modo continuativo il sistema di conformità normativa dell'organizzazione.

17. Checklist finale e autoverifica

Come nelle dispense precedenti, dedichiamo un momento all'autoverifica personale prima di proseguire il percorso.

Domande di autoverifica

33. Sapresti spiegare, con parole tue, il principio di responsabilità dell'ente introdotto dal D.Lgs. 231/2001?
34. Ricordi che cosa si intende per "reato presupposto" e perché l'elenco non è definito una volta per tutte?
35. Sapresti elencare i principali elementi costitutivi di un Modello 231?
36. Ricordi i requisiti di indipendenza richiesti all'Organismo di Vigilanza?
37. Sapresti descrivere le fasi principali di gestione di una segnalazione di whistleblowing?
38. Ricordi le fasi tipiche del processo di gestione del rischio (identificazione, analisi, valutazione, trattamento)?
39. Sapresti spiegare la differenza tra compliance, audit e controllo di gestione?

Come procedere

Se le risposte sono arrivate con sicurezza, si può proseguire con la Dispensa 4, dedicata a Bilancio, Nota Integrativa e Affidabilità Fiscale (ISA/CPB), che completa il modulo generale del percorso prima di affrontare le dispense settoriali specifiche. In caso di incertezza, si consiglia di rileggere i capitoli corrispondenti: i concetti di rischio, controllo e prevenzione qui illustrati torneranno, applicati a contesti specifici, in numerose dispense settoriali successive.

18. Riferimenti e risorse aggiornate al 2026

Per approfondimenti autonomi, si segnalano le principali fonti normative e professionali di riferimento citate in questa dispensa:

- Decreto Legislativo 8 giugno 2001, n. 231, e successive modifiche e integrazioni;
- Confindustria — Linee Guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo;
- Associazione Italiana Internal Auditors (AIIA) — risorse professionali su risk management e controllo interno;
- Normativa nazionale ed europea in materia di whistleblowing;
- Norma internazionale ISO 31000 — Risk management, linee guida;
- Norma internazionale ISO 37301 — Sistemi di gestione della compliance, requisiti.

Data la natura in continua evoluzione della materia — sia per gli ampliamenti dell'elenco dei reati presupposto, sia per gli aggiornamenti in tema di whistleblowing e protezione dei dati — si raccomanda di verificare periodicamente lo stato più aggiornato della normativa presso le fonti istituzionali di riferimento.

Chiusura della Dispensa 3

Con questa dispensa si chiude il terzo modulo del percorso, dedicato a compliance e risk management. Le competenze qui acquisite — mappatura dei rischi, modelli organizzativi, whistleblowing — costituiscono, insieme agli strumenti di audit e controllo di gestione già visti nelle dispense precedenti, il nucleo trasversale del percorso, propedeutico alle dispense settoriali dedicate a specifici ambiti professionali.

Marco Consiglio

Formatore e Course Director — 2026