



PARTE GENERALE MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI IBM ITALIA S.P.A.

ai sensi del Decreto Legislativo n. 231/2001

Aggiornamento approvato
dal Consiglio di Amministrazione
in data 23.09.2024

Indice

DEFINIZIONI, ABBREVIAZIONI ED ACRONIMI	3
1. INTRODUZIONE AL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO	6
2. SINTESI ILLUSTRATIVA DEL D.Lgs. n. 231/2001.	9
2.1 INTRODUZIONE.	10
2.2 FATTISPECE DI REATO.	12
2.3 APPARATO SANZIONATORIO	12
2.4 REATI COMMESSI ALL'ESTERO.	14
3. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI IBM ITALIA S.p.A.	15
3.1 MODELLO DI IBM ITALIA S.p.A.	16
3.2 DESTINATARI DEL MODELLO.	18
3.3 APPROCCIO METODOLOGICO	18
3.3.1 MAPPATURA PRELIMINARE DELLE AREE AZIENDALI E DELLE ATTIVITÀ SENSIBILI E ANALISI DEI RISCHI POTENZIALI	19
3.3.2 ANALISI DEL SISTEMA DI CONTROLLO PREVENTIVO ALLA COMMISSIONE DEI REATI AI SENSI DEL DECRETO	20
3.3.3 PIANO DI AZIONE PER IL MIGLIORAMENTO DEL SISTEMA DI CONTROLLO PREVENTIVO ALLA COMMISSIONE DEI REATI RILEVANTI AI SENSI DEL DECRETO	20
4. ORGANISMO DI VIGILANZA EX D.Lgs. n. 231/2001	21
5. SEGNALAZIONI WHISTLEBLOWING	25
6. SISTEMA DISCIPLINARE E SANZIONATORIO	27
6.1 SPECIFICITÀ DI ILLECITI	28
6.2 SANZIONI PER I DIPENDENTI	29
6.3 SANZIONI PER I DIRIGENTI	29
6.4 SANZIONI PER GLI AMMINISTRATORI E I SINDACI	29
6.5 SANZIONI NEI CONFRONTI DI COLLABORATORI, FORNITORI, CONSULENTI, PARTNER	30
7. FORMAZIONE, INFORMAZIONE E DIFFUSIONE DEL MODELLO	31
7.1 INFORMATIVA ALL'ESTERNO – CLAUSOLE CONTRATTUALI 231	32
8. ADOZIONE, AGGIORNAMENTO E ADEGUAMENTO DEL MODELLO	33



DEFINIZIONI, ABBREVIAZIONI ED ACRONIMI



DEFINIZIONI, ABBREVIAZIONI ED ACRONIMI

Amministratore Delegato o AD:

l'Amministratore Delegato della Società.

Area Aziendale:

ambito aziendale derivante da specifica suddivisione della Società in unità di business (Business Unit) e processi (Global Processes), coinvolto nell'implementazione e applicazione delle misure di prevenzione e controllo previste dal Modello stesso.

Attività Sensibili:

le attività della Società nel cui ambito risulta astrattamente configurabile il rischio di commissione dei reati presupposto.

Business Conduct Guidelines (BCG):

Codice Etico IBM "Guida al Comportamento negli Affari di IBM" contenente gli standard di etica aziendale di IBM, fornisce una guida generale per i dipendenti di IBM, comprese le sue consociate e affiliate.

CdA:

Consiglio di Amministrazione di IBM Italia S.p.A.

Collaboratori:

i soggetti che hanno sottoscritto con IBM Italia un contratto di collaborazione coordinata e continuativa.

Consulenti:

i soggetti che hanno stipulato con la Società rapporti contrattuali aventi ad oggetto una prestazione professionale.

Datore di Lavoro:

il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa. In caso di omessa individuazione, o di individuazione non conforme ai criteri sopra indicati, il datore di lavoro coincide con l'organo di vertice medesimo.

Destinatari:

tutti coloro che operano per il conseguimento dello scopo e degli obiettivi della Società. Fra i Destinatari del Modello sono annoverati i componenti degli Organi Sociali e di controllo, i dipendenti, i Collaboratori, i Fornitori, i Consulenti, i Partner.

Dipendenti:

persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura, con la Società nonché i lavoratori in distacco o in forza di contratti di lavoro parasubordinato.

D.Lgs. n. 231/2001 o il Decreto:

Decreto Legislativo 8 giugno 2001, n. 231, avente ad oggetto la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" e successive modifiche ed integrazioni.

Fornitori:

i fornitori di beni e servizi non professionali della Società che non rientrano nella definizione di Partner.

Key Officer:

referenti aziendali che, in base a funzioni e responsabilità, hanno una conoscenza approfondita delle aree/Attività Sensibili, nonché dei meccanismi di controllo in essere, in quanto direttamente coinvolti in esse.

Linee Guida Confindustria:

Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. n. 231/2001.

Macro Area Aziendale:

aggregati di organizzazioni definite da IBM a livello Corporation ("IBM organizations") e consistenti nell'insieme di funzioni e strutture finalizzate al raggiungimento degli obiettivi aziendali.

Modello:

il presente Modello di Organizzazione, Gestione e Controllo, redatto, adottato ed implementato ai sensi del D.Lgs. n. 231/2001.

Organismo di Vigilanza o OdV o Organismo:

l'organismo interno di controllo, di natura collegiale, preposto alla vigilanza sul funzionamento e sull'osservanza del Modello adottato dalla Società nonché al relativo aggiornamento.

Partner:

le controparti contrattuali con le quali la Società addivenga ad una qualche forma di collaborazione contrattualmente regolata, ove destinati a cooperare con la Società nell'ambito delle Attività Sensibili.

Pubblica Amministrazione/PA:

qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autorizzativi. A titolo esemplificativo e non esaustivo, si possono indicare quali soggetti Pubblici, anche con particolare riferimento all'art. 1, comma 2 del D.Lgs. 165/01, i seguenti Enti o categorie di Enti: Enti ed Amministrazioni dello Stato ad ordinamento autonomo; tutti i soggetti pubblici non economici nazionali, regionali e locali; Autorità giudiziarie; Autorità di Pubblica Sicurezza; Ministeri. Rientrano nel perimetro di tale definizione anche le persone fisiche che si configurano come rappresentanti della Pubblica Amministrazione nell'ambito dell'esercizio delle proprie attività, quali: Pubblici Ufficiali; Incaricati di Pubblico Servizio; Esponenti della Pubblica Amministrazione; Funzionari della Pubblica Amministrazione.

Reati o Reati presupposto:

le fattispecie di reato che costituiscono presupposto della responsabilità amministrativa dell'ente prevista dal D.Lgs. n. 231/2001.

Sistema di Controllo Interno:

così come definito nel documento "IBM Framework of Internal Control (FIC) including Entity Level Controls (ELCs) and COSO Principles", rilasciato e aggiornato periodicamente dal Corporate Business Controls.

Società:

IBM Italia S.p.A. e/o IBM Italia.

Soggetti Apicali:

ai sensi dell'art. 5, comma 1, lett. a) del Decreto, 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 persone che esercitano, anche di fatto, la gestione e il controllo dell'ente.

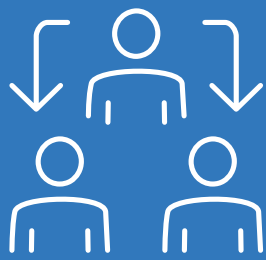
Soggetti Sottoposti:

ai sensi dell'art. 5, comma 1, lett. b) del Decreto "persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (ovvero Soggetti Apicali)".

Whistleblowing:

procedura per la gestione delle segnalazioni di condotte illecite alla luce dell'entrata in vigore del Decreto Legislativo 10 marzo 2023, n. 24, che ha dato attuazione alla "Direttiva (UE) 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali". Tale protezione è rivolta a tutti i soggetti che hanno un rapporto di lavoro o di altra natura con un'organizzazione – sia pubblica che privata – e che abbiano segnalato condotte illecite di cui siano venuti a conoscenza nell'ambito del proprio contesto lavorativo.





1. INTRODUZIONE AL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

1. INTRODUZIONE AL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Il presente documento costituisce il Modello di Organizzazione, Gestione e Controllo ai sensi e per gli effetti di cui al D.Lgs. n. 231/2001 di IBM Italia SpA (di seguito anche "IBM" o "Società"), adottato nella convinzione che, al di là delle prescrizioni del Decreto, che lo indicano come elemento facoltativo e non obbligatorio, possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto di IBM affinché seguano, nello svolgimento delle proprie attività, dei comportamenti corretti, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

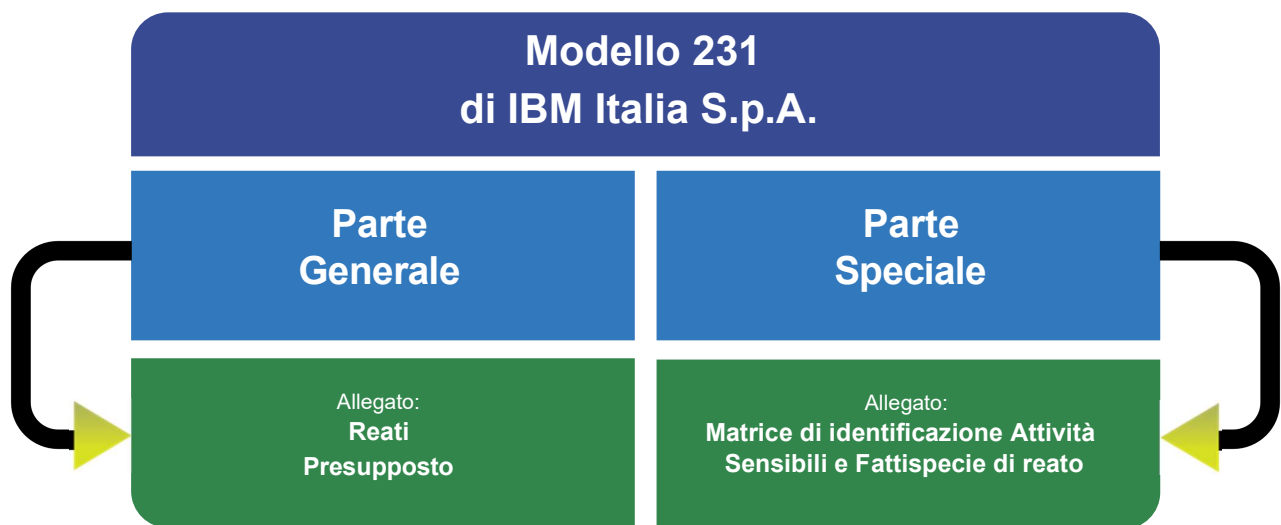
IBM Italia S.p.A., con l'adozione del Modello, si pone l'obiettivo di integrare il complesso dei principi generali di comportamento e di condotta già esistenti e applicabili per il tramite delle proprie Business Conduct Guidelines (BCG) nonché il framework del Sistema di Controllo Interno aziendale (meglio definito al successivo par. 3.1) al fine di ricordare, ove necessario, gli strumenti organizzativi e di controllo interni già esistenti, per rispondere alle finalità e alle prescrizioni richieste dal D. Lgs. n. 231/2001, sia in fase di prevenzione dei Reati, che di controllo dell'attuazione del Modello e dell'eventuale irrogazione di sanzioni.

Tale documento è il frutto dell'assessment della struttura societaria e dell'operatività di IBM effettuato con lo scopo di aggiornare il Modello pre-esistente e dotare quindi la Società di un valido ed efficace strumento organizzativo volto a prevenire la commissione di reati rilevanti ai sensi del D.Lgs. n. 231/2001, nonché, conseguentemente a costituire un'esimente dalla responsabilità amministrativa nel caso di commissione di reati presupposto da parte di Soggetti Apicali, Soggetti Sottoposti, o di Soggetti che agiscono per conto della Società e in suo nome.

Il presente Modello, richiedendo competenze multidisciplinari, è stato elaborato e predisposto grazie ad un gruppo di lavoro costituito da soggetti interni alla Società affiancati da un team di professionisti specializzati esterni per disporre di una valutazione indipendente e tecnico – professionale del Modello.

Il progetto di aggiornamento del Modello ha coinvolto, oltre al gruppo di lavoro stabilmente dedicato, anche le aree e le funzioni aziendali interessate.

Il Modello si compone di una Parte Generale e di una Parte Speciale e relativi Allegati, che tutti i Destinatari, in relazione al tipo di rapporto in essere con la Società, sono tenuti a conoscere e rispettare:



- “Parte Generale” in cui, dopo un richiamo ai principi generali enunciati dal Decreto, sono illustrate le componenti essenziali del Modello, con particolare riferimento a:
 - contesto di IBM Italia S.p.A.;
 - ruolo e compiti dell’Organismo di Vigilanza;
 - segnalazioni Whistleblowing;
 - sistema disciplinare, inteso come l’insieme delle misure da adottare in caso di mancata osservanza delle prescrizioni del Modello;
 - formazione del personale e diffusione del Modello nel contesto aziendale ed extra-aziendale;
 - adozione, aggiornamento ed adeguamento del modello;

e Allegato alla Parte Generale – Reati presupposto.

- “Parte Speciale” in cui sono:
 - identificate, in riferimento alla fattispecie di reato ritenute applicabili per la Società, le attività rilevanti nello svolgimento delle quali è astrattamente configurabile un rischio potenziale di commissione di reati;
 - indicati i presidi e i protocolli del Sistema di Controllo Interno adottati al fine di prevenire la commissione di tali reati;

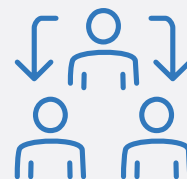
e Allegato alla Parte Speciale – Matrice di identificazione Attività Sensibili e Fattispecie di reato.

Il Modello si propone come finalità di:

- rafforzare il sistema di governance e di controllo interno;
- disporre di un sistema strutturato e organico di prevenzione presidio e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi all’attività aziendale con particolare riguardo alla prevenzione di eventuali comportamenti illeciti;
- diffondere, in tutti coloro che operano in nome e per conto di IBM nelle aree di attività a rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti ma anche nei confronti della Società;
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell’interesse di IBM che la violazione delle prescrizioni contenute nel Modello comporterà l’applicazione di apposite sanzioni ivi compresa la risoluzione del rapporto contrattuale;

- ribadire che la Società non tollera comportamenti illeciti, di qualsiasi tipo e indipendentemente da qualsiasi finalità, in quanto questi (anche nel caso in cui IBM fosse apparentemente in condizione di trarre vantaggio) sono comunque contrari ai principi etici ai quali la Società intende attenersi;
- censurare fattivamente i comportamenti posti in essere in violazione del Modello attraverso la comminazione di sanzioni disciplinari e/o attivazione di rimedi contrattuali;
- di conseguenza consentire l’esenzione della responsabilità amministrativa di IBM in caso di commissione di reati.

Il presente Modello è stato redatto sulla base degli strumenti organizzativi e di controllo esistenti alla data e potrà formare oggetto di eventuale aggiornamento sulla base dei continui cambiamenti ed integrazioni derivanti dall’evoluzione della normativa di riferimento e/o dalla eventuale integrazione e/o modifica degli strumenti organizzativi e di controllo di cui sopra e sui quali lo stesso si fonda.





2. SINTESI ILLUSTRATIVA DEL D.Lgs. n. 231/2001



2. SINTESI ILLUSTRATIVA DEL D.Lgs. n. 231/2001

2.1 INTRODUZIONE

Con il D.Lgs. n. 231/2001, in attuazione della delega conferita al Governo con l'art. 11 della Legge 29 settembre 2000, n. 300 è stata dettata la disciplina della "responsabilità degli enti per gli illeciti amministrativi dipendenti da reato".

In particolare, tale disciplina si applica agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica.

Il D.Lgs. n. 231/2001 trova la sua genesi primaria in alcune convenzioni internazionali e comunitarie ratificate dall'Italia che impongono di prevedere forme di responsabilità degli enti collettivi per talune fattispecie di reato.

Secondo la disciplina introdotta dal Decreto, infatti, le società possono essere ritenute "responsabili" per alcuni reati dolosi commessi o tentati, nell'interesse o a vantaggio delle società stesse, da esponenti dei vertici aziendali (i c.d. soggetti "in posizione apicale" o semplicemente "apicali") e da coloro che sono sottoposti alla direzione o vigilanza di questi ultimi (art. 5, comma 1, del D.Lgs. n. 231/2001).

La responsabilità amministrativa delle società è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato e si affianca a quest'ultima.

Tale ampliamento di responsabilità mira sostanzialmente a coinvolgere nella punizione di determinati reati il patrimonio delle società e, in ultima analisi, gli interessi economici dei soci, i quali, fino all'entrata in vigore del decreto in esame, non pativano conseguenze dirette dalla realizzazione di reati commessi, nell'interesse o a vantaggio della propria società, da amministratori e/o dipendenti.

Il D.Lgs. n. 231/2001 innova l'ordinamento giuridico italiano in quanto alle società sono ora applicabili, in via diretta ed autonoma, sanzioni di natura sia pecuniaria che interdittiva in relazione a reati ascritti a soggetti funzionalmente legati alla società ai sensi dell'art. 5 del Decreto.

La responsabilità amministrativa della società è, tuttavia, esclusa se la società ha, tra l'altro, adottato ed efficacemente attuato, prima della commissione dei reati, modelli di organizzazione, gestione e controllo idonei a prevenire i reati stessi; tali modelli possono essere adottati sulla base di codici di comportamento (Linee Guida) elaborati dalle associazioni rappresentative delle società, fra le quali Confindustria, e comunicati al Ministero della Giustizia.

La responsabilità amministrativa della società è, in ogni caso, esclusa se i soggetti apicali e/o i loro sottoposti hanno agito nell'interesse esclusivo proprio o di terzi.

In particolare, per le ipotesi di reato commesse da soggetti in posizione apicale, affinché l'ente benefici dell'esimente stabilita nel Decreto, è necessario che la Società dimostri che:

- sia stato adottato ed efficacemente attuato, prima della commissione del reato, un Modello di Organizzazione e Gestione e Controllo idoneo a prevenire reati della medesima tipologia rispetto a quello commesso;
- sia stato affidato ad un Organismo di Vigilanza dell'ente il compito di vigilare sul funzionamento, sull'aggiornamento e sull'osservanza del Modello;
- non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo stesso;
- l'autore del reato abbia agito eludendo fraudolentemente il Modello¹.

In ipotesi di reati commessi da soggetti sottoposti alla direzione o alla vigilanza di un apicale sarà, di contro, la pubblica accusa a dover fornire la prova che non sia stato adottato ed efficacemente attuato, prima della commissione del reato, un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire simili reati e, che il verificarsi del reato sia dipeso dall'inosservanza degli obblighi di direzione e vigilanza dei soggetti apicali.

Dunque, nel caso di reati commessi da soggetti apicali la mancata adozione ed efficace attuazione di un Modello darà potenzialmente luogo alla responsabilità amministrativa della Società.

Qualora invece i reati ex D.Lgs. n. 231/2001 siano stati commessi da soggetti sottoposti, la Società si presume innocente, essendo necessario che la pubblica accusa provi che la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza e che la Società non abbia vigilato adeguatamente.

Un Modello è ritenuto efficace se soddisfa le seguenti esigenze:

- individua le attività nel cui ambito possono essere potenzialmente commessi i reati presupposto (cosiddetta "mappatura" delle attività a rischio);
- prevede specifici protocolli diretti a descrivere le procedure operative, programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- definisce le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevede obblighi di informazione nei confronti dell'OdV;

¹ Si precisa che secondo la giurisprudenza devono essere tenuti in considerazione anche gli eventuali presidi organizzativi predisposti ed in vigore seppur non necessariamente richiamati nel Modello.

- introduce un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- prevede i canali di segnalazione interni di cui al D. Lgs. n. 24/2023.

Infine, è da ritenere che un Modello sia efficacemente attuato se prevede:

- una verifica periodica e l'eventuale modifica dello stesso, qualora siano scoperte significative violazioni delle prescrizioni, ovvero, intervengano mutamenti nell'organizzazione o nell'attività;
- irrogazioni di sanzioni in caso di violazione delle prescrizioni del Modello;
- adeguate iniziative di informazione e formazione del personale.

La Società, al fine di assicurare maggiore effettività al Modello ha, altresì, predisposto internamente un proprio modello disciplinare a cui si rimanda (Par.6 – Sistema disciplinare e Sanzionatorio).

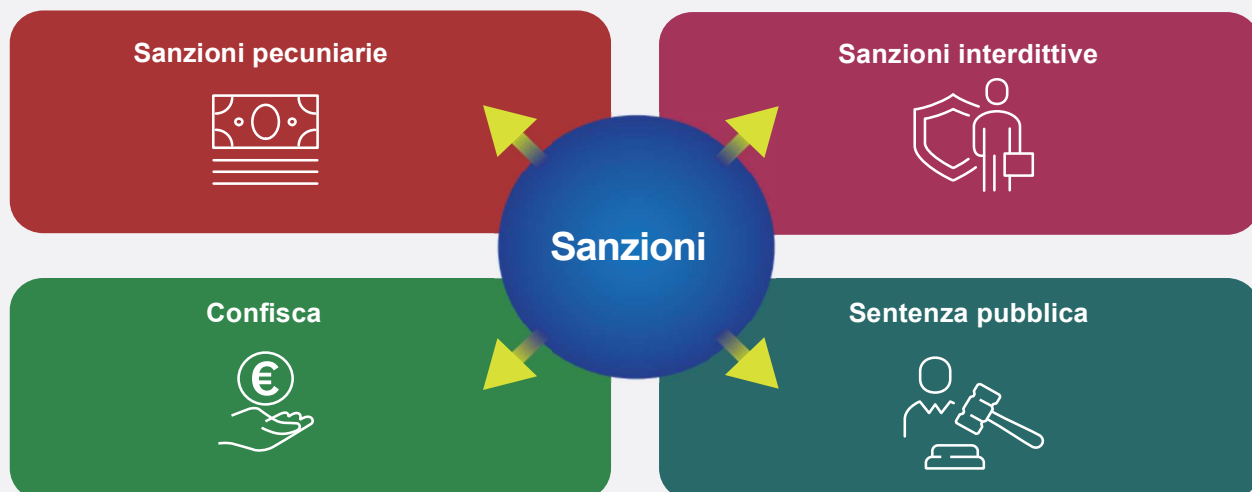
2.2 FATTISPECE DI REATO

La responsabilità amministrativa degli enti può conseguire dalla commissione dei reati presupposto così come previsti dal Decreto alla data di approvazione del presente Modello (e per il cui dettaglio si rimanda all'Allegato alla Parte Generale – "Reati presupposto").

Fattispecie di Reato suscettibili di configurare la responsabilità amministrativa dell'ente.

Art. 24 Reati contro la Pubblica Amministrazione*	Art. 24-bis Delitti informatici e trattamento illecito di dati	Art. 24 ter Delitti di criminalità organizzata	Art. 25 bis Falsità in monete, in carte di pubblico credito, in vaoluri di bollo e in strumenti o segni di riconoscimento	Art. 25 bis.1 Delitti contro l'industria e il commercio	Art. 25 ter Reati societari (compresa la corruzione tra privati, lett. s-bis)	Art. 25 quater Delitti con finalità di terrorismo o di eversione dell'ordine democratico
Art. 25 quater.1 Pratiche di mutilazione degli organi genitali femminili	Art. 25 quinquies Delitti contro la personalità individuale	Art. 25 sexies Abusi di mercato (market abuse)	Art. 25 septies Omicidio colposo o lesioni gravi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro	Art. 25 octies Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	Art. 25 novies Delitti in materia di violazione del diritto di autore	Art. 25 decies Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
Art. 25 undecies Reati ambientali	Art. 25 duodecies Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare	Art. 25 terdecies Razzismo e xenofobia	Art. 25 quaterdecies Frode in competizioni sportive, esercizio abusivo di gioco o di scommesse e giochi d'azzardo	L146/2006 Reati transnazionali	Art. 25 quindecies Reati tributari	Art. 25 sexiedecies Reati di contrabbando
Art. 25 octies.1 Delitti in materia di strumenti di pagamento diversi dai contanti	Art. 25 septiesdecies Delitti contro il patrimonio culturale	Art. 25 duodevicies Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici	Art. 25 octies Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	Art. 25 octies.1 Delitti in materia di strumenti di pagamento diversi dai contanti	Art. 25 septiesdecies Delitti contro il patrimonio culturale	Art. 25 duodevicies Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici.

2.3 APPARATO SANZIONATORIO



In caso di commissione o tentata commissione dei reati sopra menzionati l'ente può incorrere nelle seguenti sanzioni:

- la sanzione pecuniaria, la cui commisurazione è determinata in quote² e si articola in due fasi: in un primo momento il Giudice fissa l'ammontare del numero di quote e nella seconda fase procede a determinare il valore monetario della singola quota. Per la determinazione del numero di quote, il Giudice tiene conto della gravità del fatto, del grado della responsabilità dell'ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto o per prevenire la commissione di ulteriori illeciti. L'importo di ciascuna quota viene determinato dal Giudice tenendo in considerazione le condizioni economiche e patrimoniali dell'ente. L'ammontare della sanzione pecuniaria, pertanto, viene determinato per effetto della moltiplicazione del primo fattore (numero di quote) per il secondo (importo della quota);
- la sanzione interdittiva può consistere in:
 - interdizione dall'esercizio dell'attività;
 - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
 - divieto di contrattare con la Pubblica Amministrazione salvo che per ottenere le prestazioni di un pubblico servizio
 - esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
 - divieto di pubblicizzare beni o servizi;
- la confisca del prezzo o del profitto del reato³;
- la pubblicazione della sentenza di condanna⁴.

Le sanzioni interdittive hanno la caratteristica di limitare o condizionare l'attività sociale e, nei casi più gravi, arrivano a paralizzare l'ente (interdizione dall'esercizio dell'attività); esse hanno altresì la finalità di prevenire comportamenti connessi alla commissione di reati.

Tali sanzioni si applicano, nei casi espressamente previsti dal D. Lgs. 231/2001 quando ricorre almeno una delle seguenti condizioni:

- a) l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione e, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- b) in caso di reiterazione degli illeciti.

È possibile l'applicazione in via definitiva delle sanzioni interdittive nelle situazioni più gravi descritte nell'art. 16 del D. Lgs. 231/2001.

Il Decreto stabilisce, altresì, quale alternativa alla sanzione interdittiva, consistente nell'interruzione dell'attività dell'ente, la nomina da parte del Giudice, di un commissario giudiziale che consenta la prosecuzione dell'attività dell'ente per un periodo pari alla durata della pena inter-

dittiva applicata, quando ricorre almeno una delle seguenti condizioni:

- a) l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione potrebbe provocare un grave pregiudizio alla collettività;
- b) l'interruzione dell'attività dell'ente potrebbe provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

Si ricorda, infine, che il pubblico ministero può richiedere l'applicazione, in via cautelare, di una delle sanzioni interdittive previste dal Decreto nei casi in cui, tra i vari requisiti espressamente previsti dalla norma, sussistano gravi indizi per ritenere la sussistenza della responsabilità dell'ente e vi siano fondati e specifici elementi che facciano ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede.

Nel caso di commissione di un illecito dipendente da reato si applica sempre all'ente ritenuto responsabile a sanzione pecuniaria mentre la sanzione interdittiva si applica solo in relazione ai reati per i quali sia stata espressamente prevista.

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti indicati nel Capo I del Decreto, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre l'ente non sarà ritenuto responsabile nel caso in cui impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 del D.Lgs. n. 231/2001).

Deve, infine, osservarsi che l'Autorità Giudiziaria può, altresì, disporre il:

- sequestro preventivo delle cose di cui è consentita la confisca (art. 53 del D. Lgs.231/01);
- sequestro conservativo dei beni mobili e immobili dell'ente qualora sia riscontrata la fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento o di altre somme dovute allo Stato (art. 54 del D. Lgs.231/01).

2 L'importo di una quota va da un minimo di euro 258,23 ad un massimo di euro 1.549,37.
3 La confisca - disposta unitamente alla sentenza di condanna - si applica anche per equivalente nell'impossibilità di reperire il prezzo, il profitto o prodotto del reato.

4 La pubblicazione della sentenza di condanna (in caso di applicazione di una sanzione interdittiva) può essere richiesta dal Pubblico Ministero ed effettuata una sola volta, per estratto o per intero, a spese dell'ente, in uno o più giornali indicati, nonché mediante l'affissione nel comune ove l'ente ha la sede principale.

2.4 REATI COMMESSI ALL'ESTERO

Premesso che i reati commessi all'estero rappresentano una materia in continua evoluzione giurisprudenziale l'art. 4 del Decreto prevede che la responsabilità amministrativa possa configurarsi anche qualora i reati presupposto siano commessi all'estero, sempre che siano soddisfatti i criteri di imputazione oggettivi e soggettivi stabiliti.

Il Decreto, infatti, condiziona la possibilità di perseguire l'ente per reati commessi all'estero all'esistenza dei seguenti ulteriori presupposti:

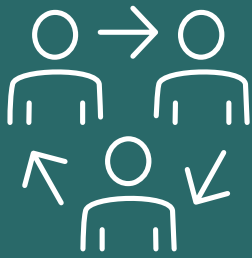
- il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'ente;
- l'ente deve avere la propria sede principale nel territorio dello Stato italiano;
- l'ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p. (nei casi in cui la legge prevede che il reo- persona fisica - sia punito a richiesta del Ministro della Giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti dell'ente stesso). Il rinvio agli artt. 7-10 c.p. è da coordinare con le previsioni dei reati di cui al Capo I del D.Lgs. n. 231/2001, sicché - anche in ossequio al principio di legalità di cui all'art. 2 del D.Lgs. n. 231/2001 - a fronte della serie di reati menzionati dagli artt. 7-10 c.p., la società potrà rispondere soltanto di quelli per i quali la sua responsabilità sia prevista da una disposizione legislativa ad hoc;
- sussistendo i casi e le condizioni di cui ai predetti articoli del Codice Penale, nei confronti dell'ente non proceda lo Stato del luogo in cui è stato commesso il fatto.

Peraltro, in applicazione del principio di territorialità⁵, non possono considerarsi escluse dall'applicazione della disciplina sulla responsabilità amministrativa quelle società estere che operano nel territorio italiano e i cui amministratori o dipendenti commettano uno o più dei reati indicati nel D.Lgs. n. 231/2001.

La presenza nel territorio nazionale di sedi secondarie di società estere non comporta, invece, la perseguibilità di questi enti anche per gli illeciti commessi nel paese di origine o comunque fuori dall'Italia. Esula dal campo applicativo del Decreto il fatto commesso nell'interesse di un ente straniero la cui lacuna organizzativa si sia realizzata interamente all'estero.



⁵ Chiunque commette un reato nel territorio dello Stato è punito secondo la legge italiana", art. 6, co.1 c.p.



3. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI IBM ITALIA S.p.A.



3. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI IBM ITALIA S.p.A.

3.1 MODELLO DI IBM ITALIA S.p.A.

IBM opera in Italia dal 1927 ed è parte di un gruppo multinazionale presente in oltre 175 paesi. Società leader nei progressi dell'AI, dell'automazione e delle soluzioni cloud ibride, si pone come mission lo sviluppo di tecnologie informatiche avanzate e l'integrazione delle stesse in soluzioni a sostegno dell'innovazione nelle imprese, nelle istituzioni e nella società.

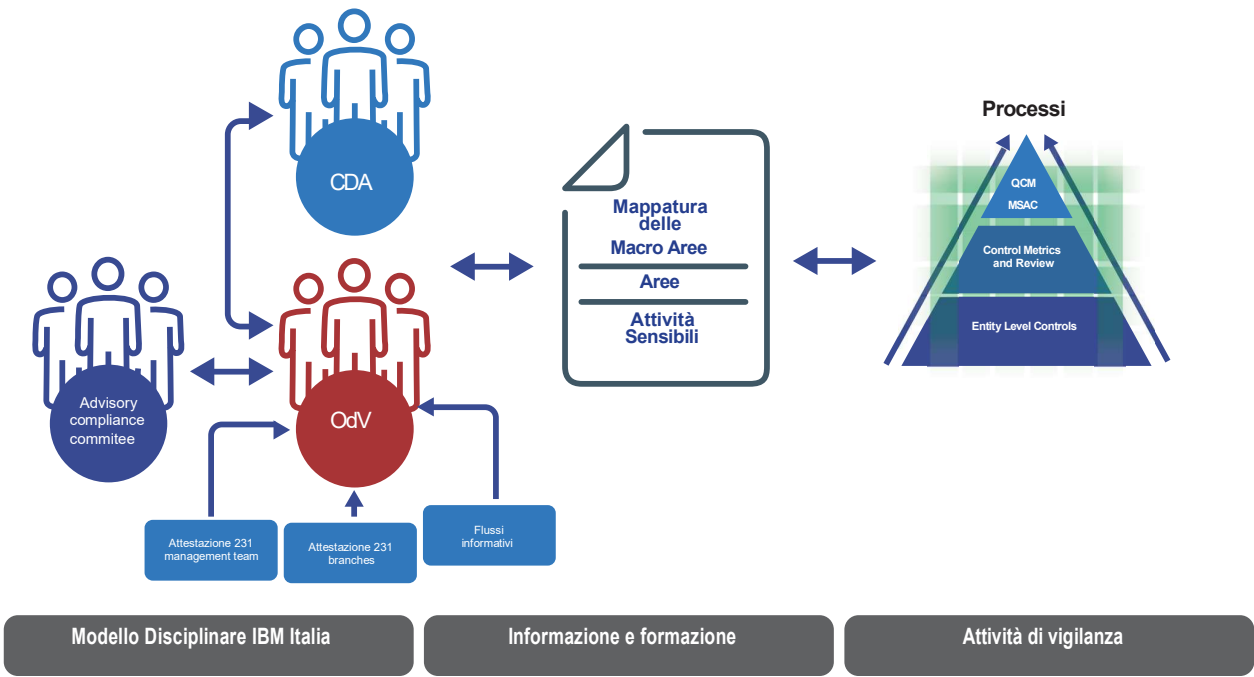
In particolare, IBM offre un ampio ventaglio di soluzioni tecnologiche e servizi di consulenza, un portfolio di middleware per la collaborazione, l'analisi predittiva, lo sviluppo software e la gestione dei sistemi, nonché i componenti più avanzati (server, memorie, supercomputer) per la costruzione delle infrastrutture digitali del futuro.

IBM, grazie all'esperienza che nasce dalle attività svolte

nella consulenza, nella tecnologia e nella ricerca, è in grado di accompagnare i clienti nel percorso di trasformazione indotto dalla crescente interconnessione digitale dell'economia e della società.

Il Modello di IBM Italia SpA si fonda su alcuni elementi che ne costituiscono le componenti essenziali e ne attestano l'esistenza e attendibilità della sua applicazione nell'ambito del contesto IBM.

BCG - Guida al comportamenti negli affari



Con riferimento alla *Governance* di IBM, quest'ultima si compone di Assemblea dei Soci, Consiglio di Amministrazione (di seguito anche "CdA") e Collegio Sindacale.

In particolare, l'Assemblea ha i poteri previsti dal Codice Civile e li esercita secondo le previsioni di legge e dello Statuto di Società. Altresì, l'Assemblea su proposta motivata del Collegio Sindacale, conferisce l'incarico di revisione legale dei conti e controllo contabile, deliberando con le maggioranze stabilite per l'Assemblea straordinaria, ad una primaria società di revisione avente i requisiti prescritti dalla normativa applicabile.

Il CdA, composto da non meno di 3 (tre) e non più di 15 (quindici) membri a seconda di quanto verrà stabilito all'atto della nomina dell'Assemblea, è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società.

Esso nomina, tra i propri componenti un Presidente, un Amministratore Delegato, al quale, nei limiti di legge e di Statuto, delega proprie attribuzioni. L'Amministratore Delegato cura, tra l'altro, che l'assetto organizzativo, amministrativo e contabile sia adeguato alla natura e alle dimensioni dell'impresa.

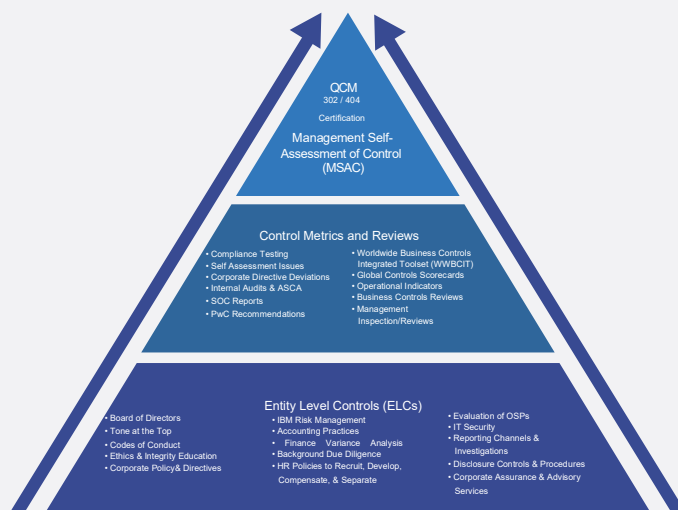
Il Collegio Sindacale si compone di 3 sindaci effettivi e di 2 sindaci supplenti.

IBM Italia, in linea con le politiche aziendali della IBM Corporation di gestione della qualità, ha intrapreso anche un percorso di certificazione rispetto ad alcune norme internazionali ad ulteriore conferma del proprio interesse verso un sistema di controllo interno strutturato e consapevole:

- ISO9001: Sistema di gestione della qualità, incentrato sul miglioramento continuo dei processi e sulla gestione dei rischi aziendali al fine di soddisfare le esigenze e le aspettative dei clienti e di altri stakeholders;
- ISO14001: Sistema di gestione ambientale, con la finalità di assicurare il controllo degli aspetti ambientali, ridurre gli impatti sull'ambiente e garantire la conformità legale;
- ISO45001: Standard di gestione della salute e della sicurezza sui luoghi di lavoro;
- SA8000 Corporate Social Responsibility, con la finalità di condurre gli affari in modo equo e dignitoso per i lavoratori e di dimostrare la propria adesione ai più elevati standard sociali.
- ISO20000/27001/27017/27018/22301: standard di Security e Business Continuity.

Il Codice Etico IBM - "Guida al Comportamento negli Affari (Business Conduct Guidelines - BCG) è la direttiva portante per il comportamento etico di tutti i dipendenti e contiene una serie di norme che tutti i dipendenti di IBM Italia S.p.A. e delle società dalla medesima controllate sono tenuti a rispettare. Il Codice Etico è portato a conoscenza e sottoscritto da tutti i dipendenti IBM Italia e delle società dalla medesima controllate; la sottoscrizione è richiesta annualmente ed è preceduta da un corso obbligatorio per tutti i Dipendenti.

Il framework del Sistema di Controllo Interno aziendale, stabilito a livello di IBM Corporation e applicato in IBM Italia SpA, è definito nel documento "IBM Framework of Internal Control (FIC) including Entity Level Controls (ELCs) and COSO Principles", rilasciato e aggiornato periodicamente dal Corporate Business Controls. Esso è basato sul modello di controllo interno e di Enterprise Risk Management pubblicato dal Committee of Sponsoring Organization (COSO) Internal Control – Integrated Framework (COSO 2013 Framework).



Nell'ambito del citato Sistema di Controllo Interno, la funzione Trust & Compliance di IBM fornisce una supervisione centralizzata e indipendente dei programmi di integrità, etica e conformità alle leggi ed alle regole applicabili di IBM ('Compliance'). Si tratta di una unità organizzativa di professionisti, prevalentemente giuristi, organizzata su base globale e con team dedicati a specifiche aree geografiche, tra cui l'Europa e l'Italia, e che collabora con i dipendenti di IBM per garantire che IBM svolga la propria attività con integrità ed in linea con il modello di Compliance.

La funzione Trust & Compliance gestisce inoltre un articolato programma di formazione il cui snodo centrale è la certificazione sulle Business Conduct Guidelines (BCG), ossia la presa d'atto ed accettazione, da parte di ciascun dipendente IBM del codice etico aziendale di IBM. Fornisce inoltre supporto, ove necessario, alle funzioni aziendali ed organizza attività di formazione su specifici processi ed eventi formativi in presenza denominati "Integrity Summits", volti ad integrare i citati programmi globali e le attività più focalizzate alla Compliance negli specifici paesi (tra le quali si annoverano i corsi di formazione in ambito D.Lgs. 231/2001 come meglio rappresentato al successivo par. 7)

La funzione di Trust & Compliance svolge infine un'attività di supporto, anche diretto, su numerosi processi a presidio delle attività ritenute più sensibili da un punto di vista delle normative anticorruzione ed è coinvolta, direttamente o indirettamente, nel controllo dell'attuazione dei programmi di Compliance.

Inoltre, il Modello contiene rimando specifico ad ulteriori documenti collegati, in particolare;

- Segnalazione di condotte illecite – Whistleblowing (Procedura per la gestione delle segnalazioni di condotte illecite alla luce dell'entrata in vigore del Decreto Legislativo 10 marzo 2023, n. 24);
- Procedura "Flussi Informativi verso OdV";
- Regolamento dell'Organismo di Vigilanza;
- Regolamento del Compliance Advisory Committee.

3.2 DESTINATARI DEL MODELLO

Il Modello è destinato a:

- amministratori e a tutti coloro che rivestono funzioni di rappresentanza, amministrazione e direzione, anche di fatto, della Società o comunque di una unità organizzativa dotata di autonomia finanziaria e funzionale, nonché ai componenti degli altri organi societari anche di controllo;
- dipendenti e soggetti a qualunque titolo sottoposti alla direzione o vigilanza del management aziendale della Società;
- coloro che, sebbene abbiano un rapporto contrattuale con altra/e società del Gruppo, nella sostanza operano in maniera rilevante o continuativa in nome o per conto o nell'interesse della Società.

In aggiunta, in forza di apposite clausole contrattuali, possono essere "Destinatari" anche i seguenti soggetti:

- collaboratori, consulenti o soggetti che operano per conto o in nome o nell'interesse della Società;
- fornitori, partner commerciali che operano in maniera rilevante o continuativa per conto o in nome o nell'interesse della Società.

3.3 APPROCCIO METODOLOGICO

La metodologia adottata per l'aggiornamento del Modello, in termini di organizzazione, definizione delle modalità operative, strutturazione in fasi ed assegnazione delle responsabilità tra le varie funzioni aziendali, è definita da IBM in conformità a quanto previsto dall'art.6 del D.Lgs. n. 231/2001, dalle più significative pronunce giurisprudenziali e dalle Linee Guida elaborate da Confindustria.

Considerato quanto appena descritto, il processo di aggiornamento del Modello, si svolge attraverso le fasi di seguito esplicate.

1.

Mappatura preliminare delle aree aziendali e delle attività sensibili e analisi dei rischi potenziali

2.

Analisi del sistema di controllo preventivo alla commissione dei reati rilevanti

3.

Piano di azione per il miglioramento del sistema di controllo preventivo alla commissione dei reati rilevanti

3.3.1 MAPPATURA PRELIMINARE DELLE AREE AZIENDALI E DELLE ATTIVITÀ SENSIBILI E ANALISI DEI RISCHI POTENZIALI

In questa fase è svolta l'analisi del contesto aziendale, al fine di individuare le Attività Sensibili a rischio di commissione di reati rilevanti per IBM ai sensi del Decreto.

L'identificazione preliminare delle Aree Aziendali e delle Attività Sensibili è stata attuata sulla base dello studio dello specifico contesto in cui opera IBM e attraverso l'esame della documentazione della Società (organigramma, processi, corpo normativo interno, procure, ecc.) nonché tenendo in considerazione la case history della Società.

In tale ambito sono stati individuati i reati potenzialmente realizzabili rispetto alle attività aziendali e i cd. Key Officer.

In base alla metodologia adottata di risk assessment, le seguenti tipologie di reati sono state ritenute potenzialmente applicabili in funzione delle attività e processi posti in essere dalla Società:

- i) Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24 del Decreto);
- ii) Delitti informatici e trattamento illecito di dati (art. 24 - bis del Decreto);
- iii) Delitti di criminalità organizzata (art. 24 - ter del Decreto);
- iv) Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (art. 25 del Decreto);
- v) Delitti contro l'industria e il commercio (art. 25 - bis.1 del Decreto);
- vi) Reati societari (art. 25-ter del Decreto);
- vii) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (25 - quater del Decreto);
- viii) Delitti contro la personalità individuale (art. 25 - quinquies del Decreto);
- ix) Reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (25 - septies del Decreto);
- x) Reati di ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25 - octies del Decreto);
- xi) Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25 - octies.1 del Decreto);
- xii) Delitti in materia di violazione del diritto d'autore (art. 25 - novies del Decreto);

- xiii) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 - decies del Decreto);
- xiv) Reati ambientali (art. 25 – undecies del Decreto);
- xv) Reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 – duodecies del Decreto);
- xvi) Reati tributari (art. 25 - quinquiesdecies del Decreto);
- xvii) Reati di contrabbando (art. 25 - sexiesdecies del Decreto);
- xviii) Reati transnazionali, introdotti dalla Legge 16 marzo 2006 n. 146, "Legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale".

Sempre in considerazione del core business di IBM Italia e della metodologia di risk assessment applicata, sono di seguito indicate alcune tipologie di reati previsti dal Decreto il cui rischio potenziale di commissione è stato ritenuto remoto:

- i) Reati in tema di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 - bis del Decreto);
- ii) Delitti di pratiche di mutilazione degli organi genitali femminili (art. 25 - quater.1 del Decreto);
- iii) Reati di abusi di mercato (art. 25 - sexies del Decreto);
- iv) Reati di razzismo e xenofobia (art. 25 - terdecies del Decreto);
- v) Reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo apparecchi vietati (art. 25 - quaterdecies del Decreto);
- vi) Delitti contro il patrimonio culturale (art. 25 - septiesdecies del Decreto);
- vii) Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25 - duodevicies del Decreto);

In ogni caso, il rischio di accadimento dei citati reati risulta ragionevolmente coperto:

- dal rispetto dei principi enunciati dalla documentazione adottata dalla Società in ambito organizzativo ed etico (BCG, procedure e policy adottate a livello di Gruppo IBM) che vincolano tutti i Destinatari alla più rigorosa osservanza delle leggi e delle normative applicabili;
- dalle regole di corporate governance;
- dal sistema di controllo interno;
- dall'insieme dei protocolli, procedure e sistemi di controllo predisposti per la prevenzione dei reati ritenuti rilevanti per la Società ai sensi del Decreto.

In aggiunta, eventuali integrazioni delle attività sensibili potranno essere disposte dal Consiglio di Amministrazione, anche su suggerimento dell'OdV.

Il risultato di tale analisi è stato rappresentato nell'Allegato alla Parte Speciale – “Matrice di identificazione attività sensibili e fattispecie di reato”.

3.3.2 ANALISI DEL SISTEMA DI CONTROLLO PREVENTIVO ALLA COMMISSIONE DEI REATI AI SENSI DEL DECRETO

Individuate le Attività Sensibili, i Key Officer e i relativi reati potenziali, si procede con una valutazione dei controlli preventivi esistenti a presidio delle Attività potenzialmente a rischio e con il loro eventuale adeguamento. L'analisi è finalizzata ad una valutazione del sistema esistente all'interno della Società in termini di capacità di contrastare efficacemente, cioè ridurre ad un livello accettabile, i rischi individuati, tenendo in considerazione i presidi generali di controllo e protocolli specifici rilevanti per ciascuna area aziendale e attività sensibile.

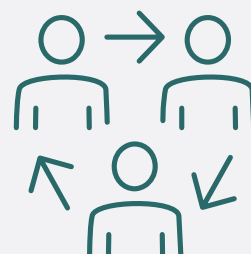
In tale fase si provvede, pertanto, alla rilevazione delle componenti del sistema di controllo preventivo esistente attraverso l'analisi della relativa documentazione e lo svolgimento di interviste ai Key Officer.

Il risultato di tale attività è formalizzato in un documento di Gap Analysis, nel quale sono evidenziate gli ambiti di miglioramento rilevati con riferimento al sistema di controllo preventivo esistente. Riguardo le risultanze di dettaglio della Gap Analysis, si rimanda alle schede intervista di Risk Assessment, predisposte a valle degli incontri con i Key Officer e da questi ultimi condivise e validate.

3.3.3 PIANO DI AZIONE PER IL MIGLIORAMENTO DEL SISTEMA DI CONTROLLO PREVENTIVO ALLA COMMISSIONE DEI REATI RILEVANTI AI SENSI DEL DECRETO

A fronte degli ambiti di miglioramento individuati, è predisposto un piano di azione teso a identificare, laddove necessario, i filoni di intervento da attuare al fine di rafforzare il livello di presidio verso la commissione dei reati rilevanti ai sensi del Decreto.

Il risultato di tale attività è formalizzato in un documento di Piano di Azione, portato a conoscenza dei Key Officer coinvolti nelle attività progettuali, dell'Organismo di Vigilanza e del CdA, nel quale sono evidenziati, a fronte degli ambiti individuati, gli interventi di miglioramento del sistema di controllo interno preventivo alla commissione dei reati rilevanti D.Lgs. n. 231/2001, da implementare - con gradi diversi di priorità - al fine di rafforzare il sistema di controllo preventivo.





4. ORGANISMO DI VIGILANZA EX D.Lgs. n. 231/2001



4. ORGANISMO DI VIGILANZA EX D.Lgs. n. 231/2001

Il D.Lgs. n. 231/2001 prevede un esonero dalla responsabilità nell'ipotesi in cui la società abbia, tra l'altro, adottato modelli di organizzazione, gestione e controllo a prevenzione dei reati stessi ed abbia affidato il compito di vigilare ed aggiornare tale modello ad un Organismo di Vigilanza dotato di autonomi poteri di iniziativa e di controllo.

Requisiti dell'Organismo di Vigilanza

Le caratteristiche dell'Organismo, affinché possa svolgere le attività sulla base delle indicazioni contenute negli artt. 6 e 7 del Decreto sono, fra gli altri:

Indipendenza

L'OdV, nominato dal Consiglio di Amministrazione di IBM, riferisce funzionalmente allo stesso.

L'OdV opera con la necessaria indipendenza nei confronti delle funzioni aziendali avendo libero accesso alle informazioni necessarie al fine di poter svolgere adeguatamente i propri compiti e non essendo direttamente coinvolto nelle attività gestionali/operative che costituiscono oggetto della sua attività di controllo.

Professionalità

Si riferisce alle competenze professionali, alla conoscenza e all'esperienza che l'Organismo di Vigilanza deve possedere per poter svolgere la sua attività in maniera efficace.

Onorabilità

L'OdV possiede tutti i requisiti di onorabilità richiesti per il ruolo, con particolare riferimento alle Linee Guida Confindustria.

Autonomia

All'OdV sono attribuite adeguate risorse per lo svolgimento delle sue funzioni con autonomi poteri di iniziativa e controllo. Le risorse consistono essenzialmente in:

1. autonomo budget di spesa che egli può impiegare per attività di aggiornamento (es. partecipazioni a corsi, iscrizione ad associazioni di settore, abbonamenti a riviste specialistiche di settore);

2. possibilità di avvalersi delle funzioni aziendali;
3. risorse che può dedicare a specifiche attività di revisione legate all'applicazione del D.Lgs. n. 231/2001 in Italia;
4. possibilità di richiedere l'esecuzione di audit specifici relativi al Decreto da parte di un soggetto indipendente, quali ad esempio società di consulenza o studi legali esterni, che potranno operare con il supporto di risorse interne a IBM Italia volta per volta identificate.

Continuità d'azione

La continuità d'azione si riferisce alla necessità di avere una struttura dedicata esclusivamente e a tempo pieno alla vigilanza sul modello.

L'autonomia e la continuità d'azione dell'OdV sono garantite dalla previsione, nell'ambito del processo di budgeting, di congrue risorse finanziarie, umane e logistiche coerenti con i risultati attesi e ragionevolmente ottenibili.

Composizione, nomina e decadenza

Le funzioni di OdV sono affidate ad un organo collegiale, composto da 3 membri di cui due esterni e un componente interno.

Nell'esercizio delle loro funzioni, i membri dell'OdV non devono trovarsi in situazioni, anche potenziali, di conflitto di interesse derivanti da qualsivoglia ragione di natura personale, familiare o professionale. In tale ipotesi essi sono tenuti ad informare immediatamente gli altri membri dell'Organismo e devono astenersi dal partecipare alle relative deliberazioni. Di tali ipotesi viene data menzione nella relazione periodica dell'OdV.

Il funzionamento dell'Organismo è stabilito nello specifico Regolamento di cui lo stesso si dota, e deve, tra l'altro, prevedere:

- che i contenuti delle riunioni dell'OdV e le decisioni assunte nel corso delle stesse siano verbalizzati;
- la calendarizzazione dell'attività dell'OdV, definendo una periodicità almeno trimestrale degli incontri dell'OdV.

L'OdV dura in carica per un anno dalla nomina ed è rieleggibile. Al fine di evitare situazioni di vacatio, l'OdV resta in carica fino alla data della successiva delibera dell'Organo Amministrativo che provvede alla sua sostituzione o conferma.

Il venir meno dei requisiti soggettivi in capo ad un componente dell'OdV ne determina l'immediata decadenza dalla carica.

In caso di decadenza, decesso, dimissione o revoca di un componente dell'OdV, il Consiglio di Amministrazione provvede tempestivamente alla sostituzione del membro cessato. In ogni caso, al fine di evitare situazioni di vacatio,

l'Organismo di Vigilanza resta in carica fino alla data della successiva delibera dell'Organo Amministrativo che provvede alla sua sostituzione o conferma. Nelle more dell'integrazione dell'organo da parte del Consiglio di Amministrazione, i componenti ancora in carica continuano a svolgere regolarmente i compiti assegnati all'Organismo di Vigilanza.

Non può essere nominato componente dell'Organismo di Vigilanza, e, se nominato decade, l'interdetto, l'inabilitato, il fallito o chi è stato condannato, ancorché con condanna non definitiva, ad una pena che importi l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi, ovvero sia stato condannato, anche con sentenza non definitiva o con sentenza di applicazione della pena su richiesta delle parti ex art. 444 c.p.p. (c.d. sentenza di patteggiamento), per aver commesso uno dei Reati previsti dal Decreto.

L'eventuale revoca di un componente dell'OdV potrà avvenire soltanto per giusta causa, mediante delibera del Consiglio di Amministrazione, sentito il parere del Collegio Sindacale, ove per "giusta causa" si intende una grave negligenza nell'assolvimento dei compiti connessi con l'incarico quali, tra l'altro:

- l'omessa comunicazione al Consiglio di Amministrazione di un conflitto di interessi che impedisca il mantenimento del ruolo di componente dell'Organismo stesso;
- l'omessa comunicazione al Consiglio di Amministrazione di procedimenti pendenti per uno dei reati presupposto previsti dal Decreto;
- la sentenza di condanna (o di patteggiamento), ancorché non passata in giudicato, per uno dei reati presupposto previsti dal Decreto o, comunque, la sentenza di condanna (o di patteggiamento), ancorché non passata in giudicato, ad una pena che comporti l'interdizione anche temporanea dagli uffici direttivi delle persone giuridiche o delle imprese;
- la violazione degli obblighi di riservatezza in ordine alle notizie e informazioni acquisite nell'esercizio delle funzioni proprie dell'Organismo di Vigilanza;

L'eventuale riforma della sentenza di condanna (o di patteggiamento) non definitiva determina il superamento della causa di ineleggibilità ma non incide sull'intervenuta revoca dalla carica.

Qualora la revoca avvenga senza giusta causa, il componente revocato potrà chiedere di essere immediatamente reintegrato in carica.

Costituisce, invece, causa di decadenza dell'Organismo di Vigilanza l'accertamento di un grave inadempimento da parte dell'Organismo di Vigilanza nello svolgimento dei propri compiti di verifica e controllo.

Il componente può recedere in ogni momento dall'incarico con preavviso scritto di almeno 30 giorni, da comunicarsi al Consiglio di Amministrazione a mezzo di raccomandata A.R.

In ottemperanza alla delibera di nomina del CdA di IBM,

l'OdV, nello svolgimento dei propri compiti, si avvale di un comitato denominato Compliance Advisory Committee.

Il Compliance Advisory Committee svolge attività di supporto all'OdV e coordinamento tra l'OdV e le funzioni aziendali; si tratta di un organo incaricato dell'attuazione delle decisioni dell'OdV e di facilitare la ricezione dei flussi informativi.

Le regole di funzionamento ed il ruolo del Compliance Advisory Committee sono contenute in un apposito Regolamento.

Funzioni e poteri

I compiti, le attività ed il funzionamento dell'OdV sono disciplinati dal proprio Regolamento.

All'OdV sono affidate le seguenti funzioni:

- vigilare sull'effettiva e concreta applicazione del Modello, verificando la congruità dei comportamenti all'interno della Società rispetto allo stesso;
- valutare la concreta adeguatezza nel tempo del Modello a svolgere la sua funzione di strumento di prevenzione di reati;
- effettuare gli approfondimenti sulle segnalazioni di violazione delle BCG e del Modello;
- riportare periodicamente al CdA sullo stato di attuazione del Modello;
- elaborare proposte di aggiornamento del Modello, necessarie a seguito di modifica della normativa e/o della struttura organizzativa e/o nel caso in cui vengano scoperte significative violazioni;
- verificare l'attuazione e l'effettiva funzionalità delle modifiche apportate al presente Modello.

Nell'espletamento di tali funzioni, l'OdV ha il compito di:

- proporre e promuovere tutte le iniziative necessarie alla conoscenza del presente Modello e delle BCG all'interno ed all'esterno della Società;
- sviluppare sistemi di controllo e di monitoraggio volti alla prevenzione dei reati di cui al Decreto;
- effettuare verifiche mirate su determinati settori o specifiche procedure dell'attività aziendale e condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;
- verificare che gli elementi previsti dalla Parte Speciale siano comunque adeguati, efficaci e rispondenti alle finalità di cui al Decreto, provvedendo, in caso contrario, a proporre alla Società di effettuare un'attività di aggiornamento;
- coordinarsi con le altre funzioni aziendali, al fine di analizzare la mappa delle aree a rischio, monitorare lo stato di attuazione del presente Modello e proporre interventi migliorativi o integrativi in relazione agli aspetti attinenti all'attuazione coordinata del Modello (istruzioni

per l'attuazione del presente Modello, criteri ispettivi, definizione delle clausole standard, formazione del personale, provvedimenti disciplinari, ecc.);

- raccogliere, elaborare e conservare dati ed informazioni relative all'attuazione del Modello.

Per lo svolgimento delle funzioni e dei propri compiti sopra indicati, vengono attribuiti all'OdV i seguenti poteri:

- accedere in modo ampio e capillare ai vari documenti aziendali e, in particolare, a quelli riguardanti i rapporti di natura contrattuale e non, instaurati dalla Società con terzi;
- avvalersi del supporto e della cooperazione delle varie strutture aziendali e degli organi sociali che possano essere interessati, o comunque coinvolti, nelle attività di controllo;
- nell'ambito dei contratti secretati o che esigano particolari misure di sicurezza in conformità a disposizioni legislative, regolamentari o amministrative ai sensi dell'art. 162 del D.Lgs. n. 50/2016, ricevere informazioni rilevanti ai fini della prevenzione dei reati presupposto di cui al D.Lgs. n. 231/2001, per il tramite del personale aziendale adeguatamente abilitato sotto il profilo della conoscibilità delle informazioni riservate;
- conferire, in conformità alle procedure previste dalla Società, specifici incarichi di consulenza ed assistenza utilizzando il budget allocato dalla Società a professionisti esperti in materia legale e/o di revisione ed implementazione di processi e procedure.

L'OdV ha altresì facoltà di richiedere alla Funzione Internal Audit di IBM di condurre audit specifici su temi inerenti al Decreto.

È responsabilità dell'OdV assicurare che ogni esigenza di controllo ed ulteriori specifiche necessità emergenti nell'ambito delle attività aziendali ai fini del Decreto siano opportunamente indirizzate per loro copertura.

Flussi Informativi

L'art. 6, comma 2, lett. d), del D. Lgs. 231/2001, impone la previsione nel Modello di obblighi informativi nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza del Modello stesso. L'obbligo di un flusso informativo strutturato è concepito quale strumento per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello e per l'eventuale accertamento a posteriori delle cause che hanno reso possibile il verificarsi dei reati previsti dal Decreto.

(i) Flussi nei confronti dell'OdV

Tutti i destinatari del Modello comunicano all'OdV ogni informazione utile per agevolare lo svolgimento delle verifiche sulla corretta attuazione del Modello. In particolare, l'Organismo di Vigilanza deve essere tempestivamente informato:

- mediante apposito sistema di comunicazione

(OdV231@ibm.com), in merito a dati/informazioni relative alle Macro Aree/Aree/Attività Sensibili;

- attraverso il sistema di segnalazione whistleblowing (descritto al successivo par. 5) in merito, tra gli altri, alle condotte illecite ai sensi del D.Lgs. n. 231/2001 e violazioni del modello di organizzazione, gestione e controllo adottato ai sensi dello stesso.

Per ulteriori dettagli circa i flussi specifici si rimanda alla Procedura "Flussi Informativi verso OdV".

(ii) Flussi da parte dell'OdV

L'OdV di IBM riferisce al Consiglio di Amministrazione e/o al Collegio Sindacale, in merito all'attuazione del Modello e al verificarsi di eventuali criticità, segnalando, per le materie di rispettiva competenza, tutte le notizie che ritiene rilevanti ai sensi del Decreto, nonché le proposte di modifica del Modello.

L'OdV di IBM potrà essere convocato dal Consiglio di Amministrazione in qualsiasi momento, per il tramite del Presidente dell'OdV medesimo, per riferire in merito al funzionamento del Modello o a situazioni specifiche.

Più in particolare, l'OdV è tenuto, nei confronti del Consiglio di Amministrazione, a:

- comunicare tempestivamente eventuali problematiche connesse alle attività, laddove rilevanti;
- relazionare, su base almeno annuale in merito all'attività svolta ed all'attuazione del Modello.

L'OdV potrà richiedere di essere convocato dal suddetto Consiglio di Amministrazione per riferire sul funzionamento del Modello o su situazioni specifiche.

L'OdV potrà, valutando le singole circostanze:

- comunicare i risultati dei propri accertamenti ai responsabili delle Funzioni e/o dei processi, qualora dalle attività scaturissero aspetti suscettibili di miglioramento. In tale fattispecie sarà necessario che l'OdV ottenga dai responsabili dei processi un piano delle azioni correttive, con l'indicazione della relativa tempistica, per l'implementazione delle attività di miglioramento, nonché il risultato di tale implementazione;
- segnalare all'alta dirigenza eventuali comportamenti/azioni significativamente non in linea con il Modello.

Conservazione e archiviazione

Le risultanze più direttamente legate all'applicazione del Decreto (quali a titolo esemplificativo e non esaustivo, le schede di Risk Assessment, la Gap Analysis, le evidenze delle attività di controllo, ecc.) sono raccolte e conservate in un archivio dedicato a cura dell'OdV, secondo le modalità di gestione della documentazione di IBM.



5. SEGNALAZIONI WHISTLEBLOWING

5. SEGNALAZIONI WHISTLEBLOWING

Come previsto dall'art. 6, comma 2-bis, del D. Lgs. 231/2001, e dalle Business Conduct Guidelines (BCG) (Codice Etico IBM "Guida al Comportamento negli Affari di IBM") la Società prevede canali di segnalazione, il divieto di ritorsione e un sistema disciplinare conformi al Decreto Legislativo 10 marzo 2023, n. 24, attuativo della direttiva (UE) 1937/2019.

Per quanto sopra la Società si è dotata di una Procedura "Segnalazione di condotte illecite – Whistleblowing" con la quale esplicita le modalità per la segnalazione delle condotte illecite che rientrano nel campo di applicazione della citata normativa; tale Procedura è consultabile al seguente link: <https://www.ibm.com/downloads/cas/AY8RZ8R1>.

Ai sensi del Decreto Legislativo 10 marzo 2023, n. 24, IBM incoraggia l'utilizzo di canali di segnalazione interna sia in forma scritta che in forma orale, che consentano di presentare, a tutela dell'integrità della Società stessa, segnalazioni circostanziate di condotte illecite, rilevanti rispetto alle violazioni previste dal Decreto,

Tra i canali di segnalazione istituiti si annoverano:

- [Employee Concern](#), tramite compilazione di apposito Form;
- Casella e-mail IBM.Ombudsman@ibm.com rivolta ai Fornitori di IBM, reperibile sul sito internet che nella documentazione contrattuale;
- Casella e-mail tellibm@us.ibm.com rivolta ai Business Partner, reperibile sul sito internet che nella documentazione contrattuale;
- Casella e-mail trustww@us.ibm.com rivolta a tutti i Destinatari, reperibile sul sito internet.

Nella gestione delle segnalazioni, la Società garantisce la tutela della riservatezza dell'identità del segnalante, nonché, nella misura eventualmente richiesta dalla legge, dell'identità delle persone menzionate nella segnalazione.

In applicazione di quanto previsto dal Capo III del Decreto, IBM rispetta il divieto di ritorsione nei confronti del segnalante, così come anche indicato nelle Business Conduct Guidelines (BCG). Conseguentemente IBM non tollera alcuna forma di ritorsione (ad es., il licenziamento, la sospensione, la retrocessione di grado o la mancata protezione, il mutamento di funzioni, l'adozione di misure disciplinari o di altra sanzione, le molestie o l'ostracismo, la discriminazione o comunque ogni trattamento sfavorevole) contro il segnalante e gli altri soggetti destinatari delle misure di protezione del Capo III del Decreto derivante dalla segnalazione ed adotterà gli opportuni provvedimenti a tutela degli stessi.





6. SISTEMA DISCIPLINARE E SANZIONATORIO



6. SISTEMA DISCIPLINARE E SANZIONATORIO

Ai sensi degli articoli 6, comma 2, lett. E), e 7, comma 4, lett. B) del Decreto, il Modello può ritenersi efficacemente attuato solo se introduce un sistema sanzionatorio idoneo per la violazione delle misure in esso indicate.

IBM, nel rispetto delle vigenti disposizioni di legge e delle norme della contrattazione collettiva nazionale, ha adottato un sistema disciplinare per le violazioni dei principi e delle misure previsti nel Modello e nei protocolli aziendali, da parte dei suoi Destinatari.

In caso di:

- violazione delle **Business Conduct Guidelines (BCG)** che abbiano rilevanza in relazione ai reati presupposto di cui al D.Lgs. n. 231/2001;
- mancata applicazione del codice disciplinare in riferimento alla commissione dei menzionati reati;
- violazione del presente Modello ovvero commissione di reati presupposto ai sensi del D. Lgs.231/2001 da parte dei membri del Consiglio di Amministrazione;

l'OdV riferirà prontamente al menzionato Consiglio, il quale provvederà all'adozione delle misure più idonee nel rispetto di quanto previsto dalla vigente normativa, come sopra richiamata.

Il procedimento sanzionatorio tiene conto:

- delle norme del **Codice civile in materia societaria, di lavoro e contrattualistica**;
- della normativa **giuslavoristica in materia di sanzioni disciplinari** di cui all'articolo 7, legge 300/1970;
- dei principi generali cui si ispira il sistema sanzionatorio, di cui al presente paragrafo;
- del **CCNL applicato**;
- dei vigenti poteri di rappresentanza e di firma sociale e delle funzioni attribuite alla struttura aziendale;
- della necessaria distinzione e contrapposizione dei ruoli tra soggetto giudicante e soggetto giudicato.

Al fine di garantire l'efficacia del presente Sistema sanzionatorio, il procedimento di irrogazione della sanzione deve concludersi in tempi compatibili a garantire l'immediatezza e la tempestività dell'azione.

6.1 SPECIFICITA' DI ILLECITI

Costituisce illecito, ai fini del presente sistema sanzionatorio, a seconda della qualifica societaria e/o della posizione e/o delle competenze nella Società del soggetto, e a prescindere dalla rilevanza penale del fatto, ogni violazione alle regole contenute nel presente Modello e, in particolare, quelle di seguito indicate, in via esemplificativa e non esaustiva:

- l'inosservanza dei protocolli diretti a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire, ovvero alle modalità di gestione delle risorse finanziarie;
- la violazione degli obblighi di informazione nei confronti del Collegio Sindacale e/o dell'OdV;
- la falsificazione/mancata predisposizione della documentazione delle attività espletate in occasione di verifiche ispettive ed accertamenti da parte delle competenti Autorità;
- la distruzione, l'occultamento e/o l'alterazione della documentazione aziendale;
- la falsificazione delle relazioni e/o informazioni trasmesse all'OdV;
- l'ostacolo all'esercizio delle funzioni del Collegio Sindacale e/o dell'OdV;
- la violazione di obblighi di documentazione e tracciabilità delle attività aziendali;
- la violazione degli obblighi previsti nelle Business Conduct Guidelines adottate dalla Società;
- l'inosservanza, da parte dei soggetti apicali, degli obblighi di direzione e/o vigilanza che abbiano reso possibile la realizzazione di reati da parte dei soggetti sottoposti;
- l'abbandono, senza giustificato motivo, del posto di lavoro da parte del personale a cui siano state specificamente affidate mansioni di sorveglianza, custodia e controllo;
- la mancata documentazione, anche in forma riassuntiva, delle attività e dell'esito delle verifiche effettuate;
- l'effettuazione e/o ricezione di pagamenti in contanti per conto della Società, oltre i limiti consentiti dalla normativa pro tempore vigente;
- l'effettuazione di pagamenti a favore della Pubblica Amministrazione, enti governativi, soggetti correlati, funzionari pubblici, senza apposita documentazione attestante il tipo di operazione compiuta e senza relativa archiviazione;
- l'accesso alla rete informatica aziendale senza autorizzazione e relativi codici di accesso;
- l'assenza ingiustificata a corsi di formazione o aggiornamento relativi alla prevenzione dei reati;
- la mancata osservanza delle disposizioni aziendali in materia di igiene e sicurezza dei luoghi di lavoro nonché degli obblighi derivanti, secondo le proprie attribuzioni e competenze, dalla normativa applicabile, pro tempore

vigente, sulla stessa materia;

- la violazione di quanto previsto dal D.Lgs. n. 24/2023 in materia di segnalazioni di condotte illecite:
 - le condotte di chi pone in essere con dolo o colpa grave segnalazioni che si rivelano infondate;
 - i comportamenti ritorsivi o discriminatori in violazione delle previsioni del suddetto Decreto, ossia i comportamenti, atti od omissioni anche solo tentati o minacciati posti in essere in ragione della segnalazione e che provocano o possono provocare direttamente o indirettamente, un danno ingiusto/pregiudizio illegittimo, diretto o indiretto, alla persona segnalante (o a chiunque abbia collaborato all'accertamento dei fatti oggetto della segnalazione) per motivi collegati, direttamente o indirettamente alla sanzione;
 - le condotte di chi ostacola o tenta di ostacolare la segnalazione;
 - le violazioni delle misure di tutela del segnalante (e degli ulteriori soggetti individuati dal suddetto Decreto), anche con riferimento all'obbligo di riservatezza;
 - mancato o inefficiente svolgimento delle attività di verifica e analisi delle segnalazioni.

In ogni caso, ai fini della determinazione/commisurazione delle sanzioni, in rapporto ad ogni singolo illecito disciplinare, si considerano i seguenti fattori:

- se la violazione è commessa mediante azione od omissione;
- se la violazione è dolosa o colposa e, rispettivamente, quale sia l'intensità del dolo o il grado della colpa;
 - il comportamento pregresso (la condotta tenuta in precedenza nell'azienda, in particolare se l'interessato è stato già sottoposto ad altre sanzioni disciplinari e l'eventuale reiterazione della violazione del medesimo tipo o di tipo analogo);
- il comportamento successivo (se vi sia stata collaborazione, anche ai fini di eliminare o attenuare le possibili conseguenze derivanti dall'illecito in capo alla Società, l'ammissione delle proprie responsabilità e la sincera resipiscenza da parte dell'interessato);
- la posizione del soggetto rispetto alla Società (organo societario, apicale, sottoposto all'altrui direzione e vigilanza, terzo);
- il grado di prossimità con uno dei reati-presupposto previsti dal Decreto;
- tutte le altre circostanze del caso concreto (modalità, tempi, rilevanza della violazione in rapporto all'attività societaria, etc.).

Nel caso in cui, con una sola condotta, siano state commesse più infrazioni punite con sanzioni diverse, si applica la sanzione più grave.

Per i dipendenti, la recidiva nel biennio comporta automaticamente l'applicazione della sanzione disciplinare

più grave nell'ambito delle tipologie prevista.

6.2 SANZIONI PER I DIPENDENTI

Per i dipendenti di IBM, il sistema disciplinare farà riferimento al vigente Contratto Collettivo Nazionale del Lavoro Metalmeccanici, nel rispetto e in coerenza con le previsioni di cui all'articolo 7 della Legge 20 maggio 1970, n. 300 ("Statuto dei lavoratori"), sia in termini di procedimento che di tipologia delle sanzioni.

6.3 SANZIONI PER I DIRIGENTI

Per ciò che concerne il sistema disciplinare adottato da IBM nei confronti dei dirigenti, si applica quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti Industria nel rispetto e in coerenza con l'art. 7 dello Statuto dei Lavoratori.

6.4 SANZIONI PER GLI AMMINISTRATORI E I SINDACI

IBM Italia valuta con estremo rigore ogni violazione del presente Modello realizzata da coloro che rivestono i ruoli di vertice in seno alla Società, e che, per tale ragione, sono più in grado di orientare l'etica aziendale e l'operato di chi opera nella Società ai valori di correttezza, legalità e trasparenza.

Nel caso di violazione delle regole del Modello e del sistema normativo interno da parte degli amministratori, a partire dall'inosservanza degli obblighi di direzione o vigilanza di cui all'articolo 7, D.Lgs. n. 231/2001, l'OdV provvederà immediatamente ad informarne, con relazione scritta, l'Amministratore Delegato, il Presidente del Consiglio di Amministrazione e il Collegio Sindacale per i provvedimenti di competenza.

In ogni caso, la violazione delle Business Conduct Guidelines (BCG), del presente Modello ovvero la commissione di uno dei reati richiamati dal Decreto costituisce giusta causa per la revoca dell'amministratore dalla propria carica.

Gli Organi Sociali provvedono ai sensi di legge.

Qualora i suddetti amministratori siano anche dirigenti della Società potranno in ogni caso trovare applicazione le previsioni di cui al precedente paragrafo.

Qualora a commettere la violazione siano uno o più sindaci, l'OdV deve darne immediata comunicazione al Consiglio di Amministrazione, in persona del Presidente e dell'Amministratore Delegato, e al Collegio Sindacale, in persona del Presidente, se non direttamente coinvolto, mediante relazione scritta.

I soggetti destinatari dell'informativa dell'OdV potranno assumere, secondo quanto previsto dallo Statuto, gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'Assemblea dei soci, al fine di adottare le misure più idonee previste dalla legge.

Il Consiglio di Amministrazione, qualora si tratti di violazioni tali da integrare giusta causa di revoca, propone all'Assemblea l'adozione dei provvedimenti di competenza e provvede alle ulteriori incombenze previste dalla legge.

6.5 SANZIONI NEI CONFRONTI DI COLLABORATORI, FORNITORI, CONSULENTI, PARTNER

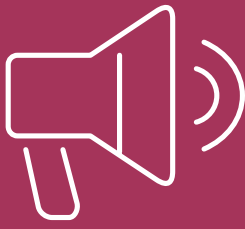
La violazione compiuta dai Collaboratori, Fornitori, Consulenti, Partner costituisce inadempimento rilevante anche ai fini della risoluzione del contratto in essere tra gli stessi e la Società, secondo clausole opportunamente sottoscritte, con eventuale applicazione di penali.

Nel caso di commissione di una violazione, di cui al precedente paragrafo 6.1., da parte di Collaboratori, Fornitori, Consulenti, Partner, la Società avrà titolo, in funzione delle diverse tipologie contrattuali adottate e/o del diverso stato di esecuzione degli obblighi derivanti dal contratto, (a) di recedere dal rapporto, nel caso in cui il contratto non abbia ancora avuto esecuzione, ovvero (b) di risolvere il contratto ai sensi dell'articolo 1456 del Codice Civile, nel caso in cui l'esecuzione del contratto abbia avuto inizio.

Ai Collaboratori, Fornitori, Consulenti, Partner è garantita la possibilità di accedere e consultare sul sito internet della Società il Business Conduct Guidelines (BCG) e la presente Parte Generale del Modello.

Inoltre, in tutti i contratti la controparte dovrà assumere l'impegno a risarcire, manlevare e tenere indenne IBM rispetto ad ogni costo, spesa, perdita, passività od onere, sostenuto e dimostrato che non si sarebbe verificato ove le dichiarazioni e garanzie rilasciate dalla controparte contenute nel contratto fossero state veritiere, complete, corrette ed accurate e gli impegni sopra descritti fossero stati puntualmente adempiuti.





7. FORMAZIONE, INFORMAZIONE E DIFFUSIONE DEL MODELLO



7. FORMAZIONE, INFORMAZIONE E DIFFUSIONE DEL MODELLO

Ai sensi dell'art. 6, comma 2, lett. b), del D. Lgs. 231/2001, la formazione interna costituisce uno strumento imprescindibile per un'efficace implementazione del Modello e per una diffusione capillare dei principi di comportamento e di controllo adottati dalla Società, al fine di una ragionevole prevenzione dei reati, da cui il Decreto fa scaturire la responsabilità amministrativa.

IBM, al fine di dare efficace attuazione al Modello e ridurre ad un livello ritenuto accettabile il rischio di commissione di reati per disinformazione od errore dei dipendenti o di terze parti in generale, intende assicurare una corretta diffusione dei contenuti dello stesso all'interno ed all'esterno della propria organizzazione, con differente grado di approfondimento in ragione del diverso livello di coinvolgimento delle stesse nelle attività sensibili a rischio.

In relazione alla comunicazione del Modello, IBM si impegna a diffonderlo a tutti i Dipendenti e i componenti degli organi statutari tramite pubblicazione sulla intranet aziendale.

Estratto del Modello (Parte Generale) è anche reso disponibile agli interessati tramite pubblicazione sul sito internet della Società.

Difatti, al fine di garantire un'efficace e razionale attività di comunicazione, la Società promuove ed agevola la conoscenza dei contenuti del Modello, anche attraverso una specifica attività formativa, a favore dei Dipendenti, con grado di approfondimento diversificato a seconda del grado di coinvolgimento nelle Attività Sensibili.

Ai fini della attività di informativa continua sul Modello 231, la Società richiede altresì, periodicamente, ai componenti del Country Leadership Team di rinnovare la certificazione di presa visione dell'informativa ai sensi del Decreto mediante un'apposita check-list accessibile alla seguente pagina intranet: <https://w3.ibm.com/w3publisher/d-lgs-231>.

La struttura dei corsi di formazione è definita dall'Organismo di Vigilanza in coordinamento con le funzioni aziendali competenti.

La partecipazione ai programmi di formazione in materia di D.Lgs. n. 231/2001 ha carattere di obbligatorietà.

Le attività di formazione hanno ad oggetto almeno:

- la sintesi della normativa di riferimento e dei concetti chiave del D. Lgs. n. 231/2001;
- le novità normative introdotte nel Decreto ed evoluzioni giurisprudenziali in tema di responsabilità amministrativa dell'ente;
- la struttura e il contenuto del Modello di Organizzazione, Gestione e Controllo;
- l'analisi dei presidi e dei principi adottati per la gestione del rischio di commissione dei reati presupposto.

Ai fini dell'efficacia delle attività formative sono previsti test intermedi e/o finali di verifica del livello di approfondimento

dei contenuti.

L'OdV monitora e verifica l'effettivo svolgimento delle attività di comunicazione e formazione, prestando ove occorra la propria collaborazione alle funzioni aziendali competenti.

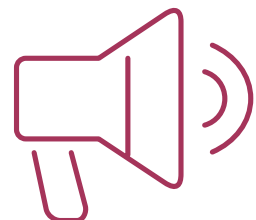
7.1 INFORMATIVA ALL'ESTERNO – CLAUSOLE CONTRATTUALI 231

Al fine di un adeguato presidio dei rischi in ambito D. Lgs. n. 231/2001, il Modello di Organizzazione, Gestione e Controllo, nella presente Parte Generale e le Business Conduct Guidelines (BCG) sono portati a conoscenza di tutti coloro con i quali IBM intrattiene rapporti contrattuali e sono resi disponibili tramite il sito internet di IBM.

L'impegno all'osservanza della legge e dei principi di riferimento del Modello e delle Business Conduct Guidelines (BCG) da parte di terzi aventi rapporti contrattuali con la Società è previsto da apposita clausola nell'ambito del relativo contratto.

Al riguardo, IBM adotta apposite clausole standardizzate che, a seconda dell'attività regolamentata dal contratto, impegnano le controparti al rispetto del D.Lgs. n. 231/2001, dei principi generali del Modello, e delle Business Conduct Guidelines (BCG), prevedendo altresì appositi rimedi contrattuali a tutela di IBM (quali il diritto di risoluzione e/o facoltà di sospendere l'esecuzione del contratto e/o clausole penali) per il caso di inadempimento.

Al fine di consentire, tuttavia, il necessario bilanciamento degli interessi di volta in volta coinvolti, i presidi e le clausole standard possono subire modifiche - anche in termini di inclusione degli stessi nel contratto.





8. ADOZIONE, AGGIORNAMENTO E ADEGUAMENTO DEL MODELLO



8. ADOZIONE, AGGIORNAMENTO E ADEGUAMENTO DEL MODELLO

Il presente Modello di Organizzazione, Gestione e Controllo è aggiornato periodicamente a cura dell'OdV. Per l'espletamento di tale compito l'OdV si avvale di tutte le funzioni aziendali di riferimento, tra le quali in particolare quelle facenti parte del Compliance Advisory Committee.

Il Consiglio di Amministrazione delibera in merito alle successive modifiche e integrazioni di carattere sostanziale del Modello.

Fra gli aggiornamenti di carattere sostanziale rientrano, a titolo esemplificativo:

- le modifiche significative della Parte Generale del Modello;
- l'inserimento nel Modello di specifiche sezioni della Parte Speciale relativamente a diverse fattispecie di reato che, per effetto di altre normative, risultino in futuro inserite o, comunque, collegate all'ambito di applicazione del Decreto;
- la soppressione di alcune parti del Modello;
- aggiornamenti al sistema di controllo adottato dalla IBM Corporation;
- l'aggiornamento del Modello a seguito di una significativa riorganizzazione della struttura aziendale e/o del complessivo modello di governance societaria.

In virtù della necessità di garantire un costante e tempestivo adeguamento del Modello, è riconosciuta all'Amministratore Delegato la facoltà di apportare modifiche o integrazioni di carattere specifico o di carattere formale al Modello, in occasione di argomenti già deliberati dal Consiglio di Amministrazione (ad esempio modifiche organizzative che abbiano un impatto sull'identificazione delle Macro Aree / Aree aziendali / Attività sensibili, modifiche sul testo dei protocolli di prevenzione, ecc.).

L'Organismo di Vigilanza:

- è previamente consultato per ogni modifica da apportarsi al Modello;
- indirizza tutte le proposte di aggiornamento del Modello all'Amministratore Delegato e al CdA.

La Società si occuperà di fornire un'adeguata formazione al personale ed ai componenti degli organi statutari in merito agli aggiornamenti del Modello, nonché di pubblicare sul sito internet la versione aggiornata del Modello.





IBM, il logo IBM, [ibm.com](https://www.ibm.com) sono marchi di International Business Machines Corp. registrati in diversi Paesi del mondo. Altri nomi di prodotti e servizi potrebbero essere marchi di IBM o di altre aziende. Un elenco aggiornato dei marchi IBM è consultabile alla pagina: [ibm.com/trademark](https://www.ibm.com/trademark). ©International Business Machines Corp. 2024.