

Banca di Pescia e Cascina

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Redatto ai sensi del
Decreto Legislativo 231/2001

Sommario

1. Premessa.....	3
2. Definizioni	3
3. Struttura del Modello	4
4. Principi generali per l'elaborazione del Modello	4
5. La normativa di riferimento	5
5.1 I reati commessi da soggetti apicali.....	6
5.2 I reati commessi da sottoposti	6
5.3 Le fattispecie di reato.....	7
5.4 I requisiti del Modello	8
5.5 Gli obiettivi	8
5.6 La definizione di rischio accettabile	9
5.7 Gli altri elementi fondamentali del Modello 231	10
6. La redazione del Modello	10
7. Il sistema organizzativo	11
7.1 Le linee Guida di categoria	11
7.2 Il sistema organizzativo della banca	11
8. Il sistema dei controlli interni	12
8.1 Consigliere con delega al Sistema dei Controlli Interni ed il Comitato Rischi	12
8.2 Le attività sensibili (ex art.6 co.2 lett. a).....	13
8.3 I principi di controllo	13
9. L'Organismo di Vigilanza.....	14
10. I flussi informativi	14
11. Il sistema disciplinare	16
12. Formazione e Informazione.....	18
13. Il Whistleblowing.....	18
13.1 Whistleblowing e contenuto del Modello.....	18
14. La privacy	19

PARTE GENERALE

1. Premessa

Il presente documento descrive il Modello di Organizzazione e di Gestione adottato dalla Banca al fine di prevenire la realizzazione dei reati previsti dal Decreto Legislativo 231/2001.

Trattasi, in conformità alla previsione dell'art. 6 del D. Lgs. 231/2001, di un aggiornamento del Modello esistente, sia nella Parte Generale che in quella Speciale, reso opportuno sia per verificarne la perdurante idoneità a prevenire i reati, sia per adattarlo alle recenti novità legislative che hanno interessato il mondo del credito cooperativo, prima tra tutte la nascita del Gruppo Bancario Iccrea, costituito in seguito alla emanazione della Legge n. 49 del 2016 (e successive modifiche), che ha riformato il Sistema del Credito Cooperativo e ha previsto l'obbligo di adesione delle Banche di Credito Cooperativo a una Capogruppo formalmente autorizzata dagli Organi di Vigilanza.

2. Definizioni

I termini qui riportati saranno utilizzati con il seguente significato:

- "D.Lgs. 231" o, più semplicemente, "Decreto": il Decreto Legislativo 8 giugno 2001 n. 231, recante «Disciplina della responsabilità amministrativa delle persone giuridiche, delle associazioni e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300» ed ogni sua successiva modifica ed integrazione;

- "Reati 231": i reati indicati nel D.Lgs 231 e quelli, contenuti in diversi provvedimenti di legge, dalla cui realizzazione può derivare la responsabilità amministrativa dell'Ente ai sensi della medesima disciplina;

- "Modello 231" o "MOG": il Modello di Organizzazione e Gestione ex art. 6, c. 1, lett. a), del D.Lgs. 231/2001;

- "Banca": la Banca di Credito Cooperativo per cui il presente Modello è stato redatto;

- "Soggetti apicali": le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Banca - o di una sua unità organizzativa dotata di autonomia funzionale, se presente - nonché le persone che esercitano, anche di fatto, la gestione e il controllo della Banca (art. 5, comma 1, lettera a) del D.Lgs. n. 231/2001)

- "Sottoposti": le persone sottoposte alla direzione o alla vigilanza dei soggetti apicali (art. 5, comma 1, lettera b) del D. Lgs. n. 231/2001);

- "Fornitori": le controparti contrattuali della Banca quali, ad esempio, gli appaltatori ed i fornitori di opere, di beni e servizi nonché tutti coloro con i quali l'Ente stabilisce forme di collaborazione;

- "Linee Guida": le linee guida redatte dalle associazioni di categoria, con particolare riferimento a quelle pubblicate dall'ABI ("Linee Guida dell'Associazione bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche" del Marzo 2008) e dal Gruppo di lavoro interdisciplinare composto da ABI, CNDCEC, CNF e Confindustria ("Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del dlgs. 8 giugno 2001 n. 231") del Febbraio 2019);

- "Organismo di Vigilanza" o "ODV": l'Organismo dotato di autonomi poteri di vigilanza e controllo cui è affidata la responsabilità di vigilare sul funzionamento e l'osservanza del modello avente i requisiti di cui all'art. 6, comma 1, lettera b) del D.Lgs. n. 231/2001 e di curarne l'aggiornamento.

3. Struttura del Modello

Il presente Modello è composto da una Parte Generale ed una Speciale.

La Parte generale illustra la struttura del Modello, la normativa di riferimento, le modalità con cui la Banca ha implementato il Modello231 ed alcuni cenni al funzionamento dell'Organismo di Vigilanza.

La Parte Speciale è divisa in 2 Sezioni.

La Sezione I riporta l'elenco di tutte le tipologie di reato specificamente sanzionate dal Decreto ("Elenco dei reati 231"), indipendentemente dalla probabilità/possibilità che esse possano essere perpetrate dai soggetti apicali o dai sottoposti e collaboratori dell'Associazione, e le relative sanzioni. Grazie ad esso l'ODV dell'Ente è in grado di calcolare in modo oggettivo il c.d. "rischio inerente", sulla base della entità delle sanzioni che il legislatore ha previsto di comminare, per ogni categoria di reati, al verificarsi di ciascuno di essi.

La Sezione II, che costituisce il nucleo principale del Modello, ha invece ad oggetto l'esposizione dei risultati della attività di Analisi dei rischi specificamente svolta nell'Ente.

Completano il Modello, di cui costituiscono parte integrante e sostanziale, tutti i documenti di formazione interna, ancorché non conservati agli atti dell'Organismo di Vigilanza, che sono stati esaminati per la redazione del Modello e che vanno a formare l'insieme dei presidi e dei controlli esistenti per calmierare il rischio reato: statuto, processi, regolamenti, ordini di servizio, note operative etc., oltre al testo del Decreto Legislativo 231/2001.

4. Principi generali per l'elaborazione del Modello

I principi generali su cui è stato elaborato il Modello, come richiamati dalle Linee Guida, sono stati i seguenti:

1. **SPECIFICITÀ** - Le attività di analisi e i meccanismi di gestione del rischio descritti nel MOG sono stati elaborati tenendo conto della concreta organizzazione della Banca e dell'attività da essa svolta, in coerenza con gli accertamenti svolti presso la Struttura ed i colloqui avuti con il personale addetto sia in fase di prima redazione del Modello che nelle successive riunioni tenute dall'Organismo di Vigilanza.
2. **ADEGUATEZZA** - Poiché un Modello è adeguato solo quando dimostra la reale capacità di prevenire i comportamenti non voluti, nella sua redazione sono state rispettate le seguenti indicazioni, tratte anche dalla giurisprudenza più recente:
 - a. espressa indicazione delle fattispecie illecite rispetto alle quali l'esposizione della Banca risultata particolarmente sensibile o, al contrario, trascurabile;
 - b. bilanciamento tra i presidi esplicitati nel Modello ed il rinvio all'impianto documentale esistente;
 - c. richiamo a procedure e regolamenti, ove esistenti;
 - d. menzione dei controlli di primo livello (di linea, insiti nelle procedure operative), di secondo livello (ad es. Collegio Sindacale, Compliance, Risk

- management, AML) e di terzo (Internal Audit, Società di revisione);
- e. coordinamento e integrazione del Modello con eventuali altri sistemi di e/o terzo livello gestione e controllo aziendale, compreso il Sistema Informativo.
3. **ATTUABILITÀ** - Le misure organizzative ed i processi di lavoro devono essere concretamente attuabili in riferimento alla struttura dell'Ente e ai suoi processi operativi.
 4. **EFFICIENZA** - Il sistema dei controlli interni deve essere coerente con le caratteristiche dell'Ente e la complessità del Modello, con riferimento anche alla sostenibilità in termini economico-finanziari ed organizzativi.
 5. **DINAMICITÀ** - Il Modello e tutta la documentazione ad esso attinente devono essere oggetto di una costante attività di verifica e aggiornamento, attraverso un'analisi periodica e/o continuativa della sua efficacia ed efficienza.
 6. **UNITÀ** - Il Modello organizzativo deve essere sviluppato procedendo a una valutazione dei rischi e dei processi sensibili che abbracci l'intera organizzazione dell'Ente e non anche una sola parte.
 7. **CONDIVISIONE** - La diffusione nell'Ente dei principi stabiliti nel Modello garantisce l'attenzione al rispetto delle regole da parte di tutti coloro che lavorano per e con l'Ente stesso.
 8. **COERENZA** - I contenuti del Modello devono essere coerenti con le risultanze dell'attività di *risk assessment*.

5. La normativa di riferimento

Il D. Lgs. 231/2001, emanato in attuazione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300, ha inteso conformare la normativa italiana in materia di responsabilità degli enti a quanto stabilito da alcune Convenzioni internazionali ratificate dal nostro Paese, tra cui la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

La sua entrata in vigore ha portato all'introduzione di una forma di responsabilità amministrativa degli enti, autonoma rispetto alla responsabilità penale delle persone fisiche autrici dei reati, derivante dalla commissione - o dalla tentata commissione - di alcuni illeciti espressamente richiamati dal Decreto (c.d. "reati presupposto"). Scopo della disciplina è quello di coinvolgere gli Enti nella punizione di taluni reati commessi nel loro interesse o a loro vantaggio.

Requisito essenziale per la imputabilità dell'Ente è che tali reati siano stati commessi da soggetti apicali o da sottoposti nell'interesse o a vantaggio dell'Ente medesimo. Quest'ultimo infatti non risponde se gli illeciti sono stati perpetrati dai predetti soggetti nell'interesse esclusivo proprio o di terzi (art. 5, comma 2). Occorre inoltre che l'illecito sia stato commesso nell'interesse o a vantaggio dell'Ente, dove l'*interesse* sussiste quando l'autore del reato ha agito con l'intento di favorire l'ente, indipendentemente dal fatto che poi tale obiettivo sia stato raggiunto, mentre il *vantaggio* sussiste quando l'ente ha tratto, o avrebbe potuto trarre, dal reato un risultato positivo, anche se non necessariamente di natura economica.

La violazione delle norme del Decreto comporta per l'Ente, oltre a sanzioni pecuniarie di rilevante entità, la possibile applicazione di misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la P.A., l'interdizione dall'esercizio

dell'attività, l'esclusione o revoca di finanziamenti e contributi ed il divieto di pubblicizzare beni e servizi.

5.1 I reati commessi da soggetti apicali

Entrando più nel particolare, il Decreto distingue tra reati commessi da soggetti apicali (la cui individuazione deve essere effettuata tenendo conto delle mansioni e delle funzioni in concreto svolte da ciascun soggetto e dalla conseguente capacità di esercitare un'influenza significativa sulla Banca o su un ramo di essa) e reati commessi da sottoposti (sostanzialmente costituiti da tutti coloro che sono legati all'Ente da rapporto di lavoro subordinato o parasubordinato, nonché i collaboratori esterni).

L'art. 6 stabilisce che, in caso di reato commesso da un soggetto apicale (dovendosi intendere per esso colui che riveste funzioni di rappresentanza dell'Ente - ad es. il Presidente - colui che amministra o dirige l'Ente - ad es. un Consigliere di Amministrazione o un Direttore Generale - o colui che esercita, anche di fatto, la gestione e il controllo di parte della Banca - ad es. un Direttore Amministrativo con autonomia di funzioni e spesa), l'Ente è esonerato da qualunque responsabilità se prova che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un Organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo (ODV - Organismo di Vigilanza);
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo preposto.

Ciò sempre che il fatto-reato sia stato commesso eludendo fraudolentemente i controlli ed i presidi adottati dalla Banca.

In buona sostanza, nel caso di reato commesso da soggetti apicali sussiste in capo all'Ente una presunzione di responsabilità dovuta al fatto che tali soggetti esprimono e rappresentano la politica e, quindi, la volontà dell'Ente stesso; una presunzione, quest'ultima, che solo l'adozione del Modello e la relativa dimostrazione della sussistenza delle succitate condizioni consente di superare.

In tal caso, pur sussistendo la responsabilità personale in capo al soggetto apicale autore materiale del reato, l'Ente non è comunque responsabile anche laddove tale Soggetto abbia agito nell'interesse oppure a vantaggio della Banca.

5.2 I reati commessi da sottoposti

Analogamente, l'art. 7 del Decreto stabilisce la responsabilità amministrativa dell'ente per i reati dei sottoposti, se la loro commissione è stata resa possibile dall'inosservanza degli obblighi di direzione o di vigilanza.

In tale ipotesi, l'inosservanza di detti obblighi è esclusa se l'Ente dimostra di aver adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di organizzazione e gestione idoneo a prevenire reati della specie di quello verificatosi.

Pertanto, nell'ipotesi prevista dal succitato art. 7, contrariamente a quella di cui all'art.6, l'adozione del Modello di organizzazione costituisce una presunzione a suo favore, comportando l'inversione dell'onere della prova a carico dell'accusa che dovrà, quindi, dimostrare la mancata adozione ed efficace attuazione del Modello.

5.3 Le fattispecie di reato

La Sezione III del Decreto richiama i reati per i quali è configurabile la responsabilità amministrativa degli enti specificando l'applicabilità delle sanzioni per gli stessi.

Le prime versioni del Decreto, per via dell'origine comunitaria della disciplina in chiave anticorruzione, si riferivano ad una serie di reati tutti sostanzialmente riconducibili ai rapporti con la Pubblica Amministrazione, con l'obiettivo di sanzionare condotte di tipo corruttivo volte ad agevolare l'attività d'impresa. Nel corso degli anni l'elenco si è però notevolmente esteso, fino a ricomprendere gran parte delle fattispecie illecite riconducibili all'attività d'impresa.

Solo per completezza si fa presente che, alla data di redazione del presente aggiornamento le categorie di reati richiamate sono:

- vari delitti contro la Pubblica Amministrazione
- falsità in monete, in carte di pubblico credito e in valori di bollo
- reati societari, compresa la corruzione tra privati
- reati con finalità di terrorismo o di eversione dell'ordine democratico
- delitti contro la personalità individuale
- reati e illeciti amministrativi di manipolazione del mercato e di abuso di informazioni privilegiate
- reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro
- reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita
- reati informatici
- delitti di criminalità organizzata
- delitti in materia di violazione del diritto d'autore
- delitti contro l'industria e il commercio
- reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- relativi a pratiche di mutilazione degli organi genitali femminili
- reati ambientali
- reati di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare
- reati di razzismo e xenofobia
- reati transnazionali
- reati relativi alle attività di filiera degli oli vergini di oliva
- reati contro le frodi sportive
- reati fiscali

precisando comunque che la futura estensione della disciplina 231 ad altre categorie non inficerà la validità della presente Parte generale.

Come è facile intuire, non tutte le categorie di reato sono riconducibili alla attività effettivamente svolta dall'Ente (anzi: alcune di esse ne sono completamente estranee). Di ciò si terrà conto nella Parte speciale del presente Modello, in cui la valutazione del rischio-reato è tarata sulla attività effettivamente svolta dall'Ente e limitata alle sole categorie di illeciti in concreto rilevanti.

Si noti anche che non tutti i reati sono dolosi, ovvero per la cui realizzazione è necessaria la volontà e consapevolezza della loro realizzazione da parte dell'agente. Alcuni sono colposi, come quelli in materia di salute e sicurezza sul lavoro e taluni reati ambientali. Tale precisazione è importante sia per determinare la soglia di accettabilità del rischio reato (di cui si dirà nei paragrafi che seguono), sia per la concreta individuazione dei sistemi di controllo preventivo.

È importante anche sottolineare che i reati previste dal Decreto, per comportare la

responsabilità dell'Ente, non è necessario che siano commessi; tale responsabilità scatta anche solo se tentati. L'art. 26 co. 1 stabilisce infatti che, nei casi di realizzazione nella forma di tentativo dei delitti, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) siano semplicemente ridotte da un terzo alla metà, salvo precisare che ne sarà esclusa l'irrogazione laddove la Banca "impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento".

5.4 I requisiti del Modello

Il D.Lgs. 231 attribuisce un valore esimente al Modello di Organizzazione e Gestione nella misura in cui quest'ultimo risulti idoneo a prevenire i reati di cui al citato Decreto e, al contempo, le sue indicazioni vengano efficacemente attuate da parte degli organi dirigenti (in primis il Consiglio di Amministrazione).

Tale Modello, come sopra accennato, deve dunque rispondere ai seguenti requisiti:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi Reati 231;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della Banca in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

5.5 Gli obiettivi

Con l'introduzione del Modello 231 la Banca, attraverso l'individuazione delle "attività sensibili ex D.Lgs. 231" e la definizione di prassi operative "idonee a prevenire i reati", si propone i seguenti obiettivi:

- rendere consapevoli tutte le persone facenti parte della struttura associativa, sia di governo sia esecutiva, che eventuali comportamenti illeciti possono comportare sanzioni penali ed amministrative sia per il singolo che per l'Ente;
- garantire l'esistenza di idonei presidi e controlli volti a garantire ed assicurare la correttezza dei comportamenti della Struttura stessa e delle persone che la rappresentano, nel rispetto della normativa esterna ed interna;
- rafforzare i meccanismi di controllo, monitoraggio e sanzionatori atti a contrastare la commissione di reati;
- enfatizzare le scelte in materia di conformità, di etica, di trasparenza, di correttezza perseguite dalla Banca, come pubblicizzate anche sul sito internet istituzionale del Movimento del Credito Cooperativo.

Obiettivo ultimo dell'adozione del Modello è, in definitiva, ottenere l'esonero da responsabilità della Banca per fatti-reati commessi dai suoi esponenti aziendali e dai suoi dipendenti, provando che:

i. in caso di reato presupposto commesso dai cosiddetti "soggetti apicali":

a) l'organo dirigente ha adottato (e provato di avere efficacemente attuato) prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi ed ha affidato ad un proprio organismo, dotato di autonomi poteri di iniziativa e di controllo, l'onere di vigilare e di curare il loro aggiornamento;

b) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione ovvero non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di controllo di cui al precedente punto 1.

ii. in caso di reato presupposto commesso da persone sottoposte alla direzione e alla vigilanza di un apicale:

a) non vi è stata inosservanza degli obblighi di direzione o vigilanza. Tale inosservanza è in ogni caso esclusa se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

L'onere di provare l'avvenuta adozione delle misure preventive ricadrà sulla Banca nel solo caso in cui l'autore del reato sia un soggetto apicale. Qualora, al contrario, l'autore del reato sia un soggetto sottoposto all'altrui direzione o vigilanza, l'onere probatorio relativo alla mancata adozione delle misure preventive spetterà all'Autorità Giudiziaria.

Se quello sopra menzionato è lo scopo principale dell'adozione del Modello, non è da sottacere, in quanto altrettanto importante, un ulteriore obiettivo: eseguire una check list dell'attività (processi, presidi organizzati e documentali, controlli) e garantirsi, attraverso il lavoro dell'Organismo di Vigilanza e la sua interlocuzione con gli organi di governo, un costante monitoraggio.

L'implementazione del Modello si inserisce infatti in una più ampia politica aziendale volta, unitamente ad altri strumenti di governance (a partire dal Codice Etico) a sensibilizzare coloro che operano in nome e per conto della Banca affinché tengano, nell'espletamento delle proprie attività, comportamenti corretti e conformi alle normative interne, tali da prevenire il rischio di commissione di reati o quantomeno ridurre tale rischio ad un livello di accettabilità, come meglio spiegato nel paragrafo successivo.

5.6 La definizione di rischio accettabile

Ad un qualunque sistema di controllo, fatta eccezione per casi particolarissimi relativi ad attività estremamente pericolose, non si può chiedere la garanzia assoluta che un rischio non sfoci mai in un fatto illecito. Quello che invece si può ragionevolmente pretendere è che il rischio di verifica di tale fatto illecito sia minimizzato e ridotto ad un livello "accettabile".

Più in particolare, il rischio è considerato accettabile quando il controllo aggiuntivo per evitare il verificarsi di un evento ha un costo superiore a quello della risorsa da proteggere.

Ai fini 231, la soglia di accettabilità è rappresentata, nei *reati dolosi*, da

**un sistema di prevenzione tale da non potere essere aggirato
se non attraverso una condotta fraudolenta
da parte dell'autore materiale del reato**

Infatti, l'art. 6 del decreto prevede che l'Ente non risponda del reato se, tra le altre cose, riesce a provare che (lettera c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione.

Per i *reati colposi* il concetto di "elusione fraudolenta" appare difficilmente compatibile, mancando la necessità che vi sia stata volontà dell'evento lesivo, sia esso costituito dall'integrità fisica dei lavoratori o dell'ambiente. In questi casi, taluni hanno sostenuto la necessità di riferire il requisito dell'elusione fraudolenta del modello alla sola condotta inosservante della regola cautelare. Ne consegue, secondo tale interpretazione, che l'Ente, per andare esente da responsabilità, dovrebbe solo fornire la prova che non vi è stato alcun accordo con l'autore materiale del reato per eludere il modello. Dimostrazione, quest'ultima, compatibile con i reati colposi. Da ciò, inoltre, l'ulteriore corollario secondo cui

**il rischio, nei reati colposi, è considerato accettabile
quando l'evento dannoso si è verificato solo perché c'è stata una violazione delle
regole del MOG e delle normative di legge poste a presidio della sicurezza del luogo di
lavoro e dell'ambiente.**

5.7 Gli altri elementi fondamentali del Modello 231

Completano il Modello i seguenti elementi:

- il **SISTEMA ORGANIZZATIVO**, costituito dall'insieme organico di principi, regole, disposizioni, schemi organizzativi relativi alla gestione ed al controllo dell'attività sociale e strumentali, tra l'altro, alla realizzazione ed alla diligente gestione di un sistema di controllo delle attività sensibili – finalizzato alla prevenzione della commissione, o della tentata commissione, dei reati previsti dal Decreto. Ne fanno parte:

- lo Statuto sociale;
- il Codice etico;
- le deliberazioni del Consiglio di Amministrazione;
- le indicazioni del Collegio Sindacale;
- la normativa interna.

Tali disposizioni possono essere scritte od orali, di applicazione generale o limitate a categorie di soggetti od individui, permanenti o temporanee.

- l'**ORGANISMO DI VIGILANZA**, che è l'organo dell'Ente a cui è affidata la responsabilità di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento.

6. La redazione del Modello

Le attività svolte nella redazione del Modello e del presente aggiornamento sono state le seguenti:

a. Identificazione dei processi sensibili al rischio reato

La Banca, in ossequio a quanto previsto dall'art. 6 co. 2 lett. a), ha individuato le cosiddette "aree sensibili" o "a rischio", cioè i processi esposti al rischio di commissione di uno dei Reati 231.

In particolare, tale attività si è sostanziata:

- nella disamina della struttura aziendale, identificando soggetti apicali e sottoposti;
- nella individuazione dei processi aziendali, dei loro presidi documentali (Codici, Regolamenti, Ordini di Servizio, Note Operative) e dei relativi controlli;
- nella analisi dei reati previsti dal Decreto e individuazione delle possibili modalità di realizzazione della condotta illecita all'interno dei processi di lavoro (anche attraverso l'esemplificazione di alcune fattispecie concrete);
- nella individuazione della probabilità di accadimento del reato in relazione alla specifica attività sensibile precedentemente individuata.

L'esito di tale attività di verifica è riportato nella Parte Speciale. Si precisa che si tratta di un *work in progress*, tenuto conto che al suo interno saranno riportati di volta in volta i risultati del lavoro di costante valutazione ed aggiornamento da parte dell'Organismo di Vigilanza, che li sottoporrà alla disamina degli Organi di governo.

7. Il sistema organizzativo

7.1 Le linee Guida di categoria

L'art 6 comma 3 d.lg. 231 stabilisce che i Modelli di organizzazione, gestione e controllo possono essere adottati sulla base di Codici di comportamento (o Linee guida) redatte dalle associazioni rappresentative di categoria. Tra queste rientra anche l'Associazione Bancaria Italiana, che nel 2001 ha rilasciato una prima edizione aggiornata delle linee guida (poi aggiornata nel febbraio 2004) e che, nel febbraio 2019, ha partecipato alla stesura dei "Principi Consolidati per la redazione dei Modelli Organizzativi" insieme a CNF, Confindustria e CNDCEC.

Le Linee Guida ABI evidenziano la creazione all'interno delle banche, anche su impulso della Autorità di vigilanza, di un sistema integrato di controlli che coinvolge soggetti diversi. Particolare rilievo assume, in tale assetto organizzativo, la funzione di internal auditing, recentemente affidata alla Capogruppo ICCREA Banca.

Tale sistema consiste in un insieme di regole, procedure e funzioni di controllo che "devono mirare ad assicurare il rispetto delle strategie aziendali ed il conseguimento della efficacia e dell'efficienza dei processi aziendali; la salvaguardia del valore delle attività e la protezione dalle perdite; l'affidabilità e l'integrità delle informazioni contabili e gestionali; la conformità delle operazioni con la legge, con la normativa di vigilanza nonché con le politiche, i piani, i regolamenti e le procedure interne".

7.2 Il sistema organizzativo della banca

La Banca, in ossequio alle Linee Guida dell'ABI, ha variamente definito e documentato il proprio sistema organizzativo ed i relativi meccanismi di funzionamento, assolvendo all'impegno di aggiornarli costantemente per rispondere alle sue esigenze strategiche ed organizzative e per adeguarsi ai requisiti richiesti dalla normativa di legge e di settore.

Ferma restando l'osservanza di quanto previsto dalle fonti normative primarie e secondarie, i principali riferimenti documentali che regolano l'organizzazione della Struttura - e che sono stati esaminati ai fini della redazione del Modello - sono:

- a) lo Statuto: costituisce il documento fondamentale su cui è basato il sistema di governo societario della Struttura: definisce, la sede, l'oggetto sociale, il capitale sociale, nonché i compiti e le responsabilità dei soggetti apicali;
- b) il Codice Etico: rappresenta il compendio delle linee programmatiche e di condotta che guidano l'esistenza dell'Ente, fungendo da ausilio e supporto alla realizzazione ed implementazione di un valido modello di organizzazione e gestione;
- c) la Carta dei Valori, che esprime i valori sui quali si fonda l'azione della Banca, la sua strategia e la sua prassi. Racchiude le regole di comportamento e rappresenta gli impegni della Banca;
- d) la Carta della Coesione Sociale, strumento di riferimento per la gestione del rafforzamento del sistema a rete nonché una cornice valoriale che fissa i principi che orientano gli accordi collaborativi tra ciascuna BCC e gli altri soggetti del sistema del Credito Cooperativo.
- e) i Regolamenti aziendali: variamente definiti in base al grado di dettaglio (regolamenti, processi, note operative, ordini di servizio etc.), descrivono la struttura organizzativa e i processi di lavoro della Struttura, gli organi di governo, i compiti e le responsabilità

delle unità organizzative (un loro elenco completo è riportato nella Parte Speciale).

- f) Il Documento di Valutazione dei rischi ex art 17 del D. Lgs. n. 81/2008, che contiene una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro, nella quale sono specificati i criteri adottati per la valutazione stessa; l'individuazione delle misure di prevenzione e di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione dei rischi e il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza.

8. Il sistema dei controlli interni

La Banca, al fine di gestire e controllare con maggiore efficienza la propria attività, ha adottato alcune procedure di controllo volte ad assicurare il rispetto delle strategie aziendali e il conseguimento del corretto svolgimento dei processi operativi. Tali procedure sono così articolate:

1° livello

Controlli di linea, effettuati dalle stesse strutture produttive che hanno posto in essere le operazioni o incorporati nelle procedure e diretti ad assicurare il corretto svolgimento delle operazioni.

2° livello

Controlli sulla gestione dei rischi, condotti a cura di una struttura interna (Funzione di Risk Controlling/Management), contraddistinta dalla piena separatezza dalle funzioni operative, avente il compito di definire le metodologie di misurazione dei rischi, verificare il rispetto dei limiti assegnati alle varie funzioni operative e controllare la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio/rendimento, quantificare il grado di esposizione ai rischi e gli eventuali impatti economici; controlli di conformità normativa, svolti dalla Funzione indipendente all'uopo costituita con il compito specifico di promuovere il rispetto delle leggi, delle norme, dei codici interni di comportamento per minimizzare il rischio di non conformità normativa e i rischi reputazionali a questo collegati contribuendo, per gli aspetti di competenza, alla realizzazione del modello aziendale di monitoraggio e gestione dei rischi.

3° livello

Attività del Collegio Sindacale, delle funzioni di revisione interna (Internal Auditing) ed esterna (Società di revisione), volta a valutare l'adeguatezza e la funzionalità del complessivo Sistema dei Controlli Interni e ad individuare andamenti anomali delle procedure e della regolamentazione.

8.1 Consigliere con delega al Sistema dei Controlli Interni ed il Comitato Rischi

Nel sistema dei controlli interni riveste particolare importanza il "Consigliere con delega al Sistema dei Controlli Interni", nominato presso ciascuna Banca Affiliata del Gruppo nei casi in cui non venga istituito, sulla base di quanto previsto dalle politiche di governo societario del GBCI, un Comitato Rischi.

Il suddetto Comitato (ove istituito) svolge, in linea con le politiche del Gruppo, i seguenti compiti:

- fornisce il proprio parere al Consiglio di Amministrazione in relazione alle proposte di nomina dei Responsabili delle Funzioni Aziendali di Controllo e del Delegato SOS;

- interloquisce direttamente con i Responsabili delle Funzioni Aziendali di Controllo della propria Entità e ne segue costantemente le attività e le relative risultanze;
- monitora l'esecuzione delle linee di indirizzo definite dal Consiglio di Amministrazione, nonché dagli Organi Aziendali della Capogruppo, avvalendosi dell'apporto delle Funzioni Aziendali di Controllo, valutando costantemente l'adeguatezza e l'efficacia del Sistema di Controllo Interno;
- esamina preventivamente i piani delle attività, le relazioni annuali e gli ulteriori flussi informativi relativi alle attività di controllo svolte dalle Funzioni Aziendali di Controllo ed indirizzate al Consiglio di Amministrazione;
- esprime valutazioni e formula pareri al Consiglio di Amministrazione sul rispetto dei principi cui devono essere uniformati il Sistema dei Controlli Interni e l'organizzazione aziendale.

8.2 Le attività sensibili (ex art.6 co.2 lett. a)

Nel corso dell'analisi effettuata sono stati espressamente individuati, per ogni attività sensibile, gli strumenti del sistema organizzativo interno (Regolamenti, Controlli etc.) posti a presidio, valutandone il grado di idoneità rispetto alla capacità di prevenzione dei comportamenti illeciti.

Per l'individuazione delle attività sensibili è stata analizzata, insieme al personale della Banca, la realtà operativa aziendale. In particolare, per ogni attività a potenziale rischio di commissione reati sono stati raccolti i seguenti dati:

- l'effettivo svolgimento dell'attività sensibile presso la struttura, al fine di limitare l'analisi al perimetro di effettivo rischio aziendale;
- il soggetto responsabile dell'attività (Unità Organizzativa o Funzione);
- il processo di riferimento;
- le contromisure adottate (normativa, poteri di firma e poteri autorizzativi, segregazione dell'attività, tracciabilità, altri presidi);
- l'indicazione delle criticità emerse e delle aree di miglioramento, sempre in ottica di prevenzione dei reati

prendendo in considerazione i regolamenti aziendali come sopra definiti e le Unità operative (uffici, funzioni) interessate a presidiare e/o controllare le suddette attività.

Le risultanze di tale analisi costituiscono, come sopra precisato, il contenuto della Parte Speciale del presente Modello.

8.3 I principi di controllo

In linea generale, i principi di controllo che devono sovrintendere all'attività dell'Ente possono essere così riassunti:

- a) ogni operazione deve essere documentabile e successivamente verificabile;
- b) la verificabilità deve essere garantita nel tempo attraverso misure, anche informatiche, che prevengono la perdita e l'alterabilità dei dati;
- c) ogni processo non può essere svolto in autonomia da un solo soggetto (c.d. principio di segregazione);
- d) i poteri dei singoli, oltre a non essere illimitati, devono essere chiaramente definiti e conosciuti all'interno dell'organizzazione;
- e) i poteri autorizzativi devono essere coerenti con le responsabilità;
- f) i controlli devono essere documentati.

9. L'Organismo di Vigilanza

In attuazione delle disposizioni previste dal Decreto, il Consiglio di Amministrazione ha deliberato di costituire un Organismo di Vigilanza con la responsabilità di vigilare sul funzionamento e l'osservanza del Modello 231 e di individuarne gli eventuali interventi correttivi, proponendone allo stesso Consiglio di Amministrazione l'aggiornamento.

L'Organismo di Vigilanza, che gode di autonomia finanziaria avendo ricevuto dal CdA massima disponibilità a far fronte ad ogni motivata richiesta di fondi per lo svolgimento della sua attività indipendentemente dalla individuazione di uno specifico budget, è tenuto a:

- promuovere, coordinandosi con le funzioni aziendali competenti, idonee iniziative per la diffusione della conoscenza e della comprensione dei principi del Modello 231, definendo specifici programmi di informazione/formazione e comunicazione interna;
- riferire periodicamente al Consiglio di Amministrazione e al Comitato dei Sindaci circa lo stato di attuazione del Modello 231;
- definire e comunicare alle strutture della Banca, previa informativa al Consiglio di Amministrazione, i flussi informativi che debbono essergli inviati con indicazione dell'unità organizzativa responsabile dell'invio, della periodicità e delle modalità di comunicazione;
- definire e comunicare a tutte le strutture della Banca le modalità con cui effettuare le segnalazioni;
- valutare le eventuali segnalazioni;
- accertare e segnalare al Consiglio di Amministrazione, per gli opportuni provvedimenti, le violazioni del Modello 231 che possano comportare l'insorgere di responsabilità;
- proporre al Consiglio di Amministrazione l'adozione di eventuali provvedimenti disciplinari a seguito di violazioni del Modello 231.

Per completezza si riportano qui di seguito le indicazioni dettate dalla Capogruppo sulle principali responsabilità ascrivibili all'Organismo di Vigilanza ex d.lgs. n. 231/2001:

“L'Organismo di Vigilanza ai sensi del D.Lgs. 231/2001 (di seguito alternativamente anche “OdV”), ove presente presso le singole Entità del GBCI, vigila sull'efficace attuazione, sul funzionamento, sull'osservanza e sull'aggiornamento del modello di organizzazione, gestione e controllo previsto dalla normativa in parola e sulla sua adeguatezza a prevenire e contrastare la commissione dei reati presupposto del Decreto. Al fine di adempiere alle proprie responsabilità in materia, l'OdV propone e verifica le iniziative più idonee a diffondere presso gli Organi Aziendali, tra il personale e i fornitori di beni e servizi del GBCI la conoscenza ed il rispetto del Codice Etico di Gruppo e del modello suddetto. L'OdV per l'adempimento dei compiti allo stesso attribuiti, può avvalersi del supporto delle Funzioni Aziendali di Controllo per ottenere informazioni, in possesso di quest'ultime, in merito alla valutazione dei rischi in relazione agli ambiti di proprio interesse. Le Funzioni Aziendali di Controllo forniscono all'Organismo di Vigilanza informazioni su particolari violazioni o carenze rilevanti riscontrate nelle materie di interesse durante lo svolgimento delle proprie attività pianificate”.

10. I flussi informativi

L'Organismo di Vigilanza ha la responsabilità di vigilare sul funzionamento e l'osservanza del Modello 231 e di provvedere al relativo aggiornamento.

Cardine di tale funzione è l'attività di segnalazione, da parte dei destinatari della normativa, di tutti quegli eventi che potrebbero far sorgere una responsabilità della Banca ai sensi del Decreto.

A tal fine l'Organismo di Vigilanza:

- accede a tutti i documenti ed informazioni aziendali rilevanti per lo svolgimento delle funzioni ad esso attribuite senza necessità di autorizzazioni, fermo restando l'obbligo di riservatezza relativamente alle informazioni acquisite;
- si avvale, previa richiesta al Consiglio di Amministrazione, di soggetti terzi di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello 231;
- richiede alla Struttura di fornire tempestivamente le informazioni, i dati e/o le notizie necessarie per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso;
- riceve ogni comunicazione rilevante o comunque pertinente ai fini del rispetto della normativa 231;
- riceve le comunicazioni inoltrate alla Banca dai dirigenti e/o dai dipendenti di avvio di procedimenti giudiziari a loro carico;
- riceve i rapporti predisposti nell'ambito delle attività di controllo da funzioni interne e/o da soggetti esterni;
- riceve i verbali delle Autorità Giudiziaria e di Vigilanza di settore dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle norme del Decreto 231.

Al fine di consentire la segnalazione da parte dei destinatari del presente Modello 231 di eventuali notizie relative alla commissione o al tentativo di commissione dei reati oltre che di violazione delle regole previste dal Modello 231 stesso, la Banca si impegna a garantire idonei canali di comunicazione nei confronti dell'Organismo di Vigilanza, anche tramite uno specifico indirizzo di posta elettronica.

In generale, la gestione dei c.d. "flussi informativi", deve avvenire nel rispetto delle seguenti indicazioni:

- le segnalazioni devono essere inviate all'ODV dal Responsabile dell'Unità Organizzativa o dalla Funzione di riferimento (tra cui possono rientrare anche il CdA o il Collegio Sindacale), con la frequenza o al verificarsi degli eventi individuata nel Modello per ciascuna categoria di Reati;
- è data comunque facoltà a chiunque di inviare una segnalazione all'ODV, non anonima, anche senza il coinvolgimento del superiore gerarchico. Tali segnalazioni dovranno rivestire la forma scritta, sebbene senza alcuna necessità di formule sacramentali;
- l'ODV sarà libero di compiere tutte le attività di indagine ed istruttorie ritenute a sua discrezione utili e/o opportune per verificare la fondatezza della segnalazione, avendo preliminarmente ricevuto dalla Banca garanzia di massima collaborazione nelle indagini;
- l'ODV, nei casi in cui particolari esigenze lo richiedano, garantirà la riservatezza dell'identità del segnalante, fatta eccezione per i casi in cui ciò non sia possibile per rispettare un obbligo di legge o per consentire il diritto di difesa alla Banca o alle persone eventualmente menzionate nella segnalazione.

L'invio e la ricezione dei flussi informativi avverrà attraverso messaggi di posta elettronica che coinvolgeranno l'ODV, il CdA, il Collegio Sindacale e gli Uffici interni. Questi ultimi godranno di ampia autonomia in merito all'invio dei c.d. "flussi ad evento" e potranno essere chiamati a rispondere a specifici quesiti dell'ODV in risposta a specifiche richieste.

A tal proposito si osserva che la qualità dei flussi informativi si declina però non solo in termini di idoneità a rappresentare effettivamente il fenomeno monitorato (capacità segnaletica) e di attendibilità, nel senso che il dato riportato deve essere veritiero e corretto, ma anche in termini di tempestività ed aggiornamento, nel senso che le informazioni devono essere il più possibile attuali rispetto al periodo di osservazione.

Per questo motivi la Banca, consapevole dell'opportunità che l'OdV riceva con tempestività flussi informativi su una molteplicità di materie (ad esempio: (a) controlli inerenti la gestione delle risorse finanziarie; (b) formazione; (c) provvedimenti disciplinari; (d) profili legati alla sicurezza informatica ed ai reati cd. informatici; (e) sicurezza sui luoghi di lavoro; (f) antiriciclaggio e rischi connessi (autoriciclaggio, ricettazione); g) rapporti con la Pubblica Amministrazione etc.), ha introdotto un Sistema di flussi che, superando la tradizionale dicotomia tra "flussi periodici" e "flussi ad evento", prevede che la maggior parte delle informazioni sia inviata all'OdV al verificarsi di fatti più o meno significativi (e quindi sia "ad evento"). Tale scelta consente, a parere della Banca, la massima tempestività nella trasmissione delle informazioni rilevanti, non dovendosi mai attendere una scadenza temporale predefinita (qualunque ne sia la periodicità).

Tale Sistema, per calmierare il rischio che alcune informazioni, ancorché rilevanti, non siano state comunque portate a conoscenza dell'OdV, prevede inoltre un doppio meccanismo di salvaguardia, in forza del quale l'Organismo:

- almeno una volta l'anno, riceve da parte di tutte le Unità coinvolte nell'invio dei Flussi una "attestazione del rispetto delle norme di comportamento prescritte nel MOG", così che le suddette Unità possano colmare eventuali inosservanze/ritardi/lacune informative che, per negligenza o altro, hanno impedito all'OdV di conoscere di un fatto;
- può richiedere il rilascio di tale attestazione da qualunque Unità Operativa ogni qual volta lo ritenga opportuno, senza vincoli di periodicità.

ATTENZIONE: l'identificazione di coloro che saranno tenuti all'invio dei flussi è di fondamentale importanza. I soggetti che potrebbero venire a conoscenza del fatto-reato (o comunque dell'evento che l'ODV chiede di conoscere) potrebbero infatti essere molti, con conseguente rischio che ciascuno di essi, confidando nell'altrui segnalazione (in realtà mai avvenuta) omettano di farla, bloccando il flusso informativo.

11. Il sistema disciplinare

Elemento essenziale per il funzionamento del Modello 231 è l'introduzione di un sistema disciplinare idoneo a sanzionare gli eventuali comportamenti ed attività contrastanti con le misure indicate.

Al riguardo, l'art. 6 comma 2 lett. e) prevede che i modelli di organizzazione e gestione devono "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello". Il mancato rispetto delle misure, previste dal Modello 231, viene valutato sotto il profilo disciplinare seguendo modalità differenti a seconda che si tratti di "soggetti sottoposti a direzione o vigilanza" (art. 5, comma 1, lett. b) ovvero di "soggetti apicali" (art. 5, comma 1, lett. a).

11.1 Principi generali in tema di sanzioni disciplinari

L'avvio di un procedimento disciplinare e l'eventuale emanazione delle sanzioni disciplinari, che non potrà trascurare il rispetto della legislazione vigente (ed in particolare dall'art. 2106 del Codice Civile e dell'art. 7 dello Statuto dei Lavoratori), prescinde sia dalla rilevanza penale della condotta sia dalla conclusione dell'eventuale procedimento penale avviato dall'Autorità Giudiziaria nel caso in cui il comportamento da censurare integri una fattispecie di reato. Pertanto, l'applicazione delle sanzioni potrà avere luogo anche se il destinatario abbia posto in essere esclusivamente una violazione dei principi sanciti dal Modello organizzativo o dal Codice Etico.

Saranno ad esempio applicabili sanzioni disciplinari alle seguenti condotte:

- l'inoltro con dolo o colpa grave di segnalazioni all'ODV che si rivelano infondate;
- l'omissione fraudolenta di fatti che, ai sensi del Modello, devono essere portati a conoscenza dell'ODV, al fine di impedire/evitare/ritardare i controlli;
- il compimento di atti ritorsivi o discriminatori nei confronti dei soggetti segnalanti per motivi collegati, direttamente o indirettamente, alla segnalazione, con particolare riferimento alle violazioni delle misure poste a tutela della riservatezza del segnalante.

11.2 Misure nei confronti del personale dipendente

Entrando più nel dettaglio delle singole sanzioni, quando la violazione delle regole comportamentali previste nel Modello sarà commessa da dipendenti destinatari del Contratto Collettivo Nazionale del Lavoro, troveranno applicazione i provvedimenti disciplinari previsti nel suddetto CCNL, che allo stato attuale della normativa sono rappresentate, in ordine di gravità, da: (1) rimprovero verbale; (2) biasimo scritto; (3) sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni; (4) licenziamento per giustificato motivo; (5) licenziamento per giusta causa.

Senza pretesa di completezza ed a titolo esemplificativo, fermo restando che l'individuazione della sanzione applicabile al caso concreto spetterà al datore di lavoro, qui di seguito vengono elencate alcune condotte integranti la violazione del Modello 231 che dovranno essere valutate sotto il profilo disciplinare:

- condotte non conformi alle prescrizioni indicate nel Modello e nei diversi presidi documentali aziendali che ne costituiscono il fondamento (statuto, regolamenti, processi, ordini di servizio, note operative etc.);
- violazioni agli obblighi di informativa nei confronti dell'Organismo di Vigilanza, sia mediante comportamenti omissivi (ad es. mancato o ritardato invio, con colpa grave o dolo, di un Flusso in presenza delle circostanze individuate dal sistema dei Flussi) che commissivi (ad es. invio di un Flusso con dati incompleti o non veritieri);
- condotte che, oltre a essere non conformi alle prescrizioni del Modello, hanno arrecato un danno alla Banca (economico, all'integrità dei suoi beni o reputazionale) od abbiamo esposto il suo personale ad una situazione di pericolo;
- condotte che sono state adottate allo scopo precipuo di compiere una condotta illecita rilevante ai sensi del Decreto 231 o che abbiano determinato il rischio – se non addirittura l'irrogazione - di sanzioni previste dal Decreto 231 a carico della Banca.

11.3 Misure nei confronti dei soggetti apicali

Si premette che le sanzioni previste a carico dei soggetti apicali per le violazioni del Modello 231 costituiscono sanzioni "convenzionali", irrogabili solo laddove tali soggetti si siano impegnati contrattualmente, all'atto della nomina o con successiva adesione, a rispettare le previsioni del Modello e a soggiacere alle sanzioni ivi stabilite.

In tali ipotesi, potranno essere applicate le sanzioni della ammonizione (sia verbale che scritta), la sanzione pecuniaria (fino alla misura massima deliberata dal Consiglio di Amministrazione o, in mancanza di delibera, fino ad un massimo di 10.000 Euro), la revoca da una o più deleghe e, nei casi più gravi, la destituzione dalla carica. Potranno trovare inoltre applicazione le sanzioni previste dal Codice Civile, per la cui individuazione ed irrogazione si rimanda alla normativa vigente.

In tutti i casi dovrà essere rispettato il principio della proporzionalità della sanzione rispetto alla gravità dell'infrazione commessa.

12. Formazione e Informazione.

Il Modello 231 è portato a conoscenza di tutti i destinatari mediante appositi interventi di comunicazione e formazione al fine di garantire la massima diffusione dei principi ispiratori e delle regole di condotta.

La divulgazione del Modello organizzativo non è infatti sufficiente ai fini dell'efficace attuazione del modello organizzativo. Il suo corretto funzionamento presuppone che i soggetti interessati – siano essi apicali o subordinati – ne siano adeguatamente informati e che questi siano messi in condizione, attraverso specifici interventi formativi, di usufruire correttamente dei sistemi, informatici o di altra natura, volti alla segnalazione dei reati o delle irregolarità.

La formazione dovrà essere appropriatamente tarata in funzione dei ruoli/livelli dei destinatari e dovrà riguardare sia la disciplina sulla responsabilità amministrativa degli enti in generale che l'analisi e l'illustrazione del Modello organizzativo specifico della propria realtà di lavoro.

13. Il Whistleblowing

Il "whistleblowing" è la segnalazione compiuta da un lavoratore che, nello svolgimento delle proprie mansioni, si accorge di una frode, un rischio o una situazione di pericolo che possa arrecare danno all'azienda per cui lavora, nonché a clienti, colleghi o qualunque altra categoria di soggetti.

Il 14 dicembre 2017 è stata pubblicata nella Gazzetta Ufficiale n. 291 la Legge 30.11.2017 n. 179, recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", allo scopo di riformare la materia del whistleblowing estendendola dal settore pubblico (nella quale era stata introdotta con la legge 190/2012) a quello privato (che fino a quel momento la prevedeva in via obbligatoria solo per determinate categorie di soggetti - sostanzialmente le sole banche, ex art. 52 Tub).

La Legge 179 ha integrato dell'art. 6 del Decreto 231/2001, inserendo 4 nuovi commi all'articolo 6 del Decreto. La disciplina prevede ora l'obbligo (comma 2-bis), per ogni Ente che si sia munito di un Modello di Organizzazione, di prevedere adeguati canali informativi che consentano ai segnalanti di "presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti".

13.1 Whistleblowing e contenuto del Modello

Per rispondere alle caratteristiche di idoneità previste dalla legge, il Modello adottato dalla Banca recepisce la normativa sul whistleblowing.

In questo contesto l'Organismo di Vigilanza, unitamente al Responsabile delle Segnalazioni, ha il compito di:

- verificare che il Modello contenga, nella Parte Generale, una specifica sezione dedicata alla normativa in oggetto e, nella Regolamentazione interna, la previsione espressa di sanzioni connesse alla violazione del divieto di atti di ritorsione nei confronti dei segnalanti e all'utilizzo abusivo dei canali di segnalazione;
- dare indicazioni affinché sia predisposta una specifica procedura che disciplini le modalità di segnalazione, mediante la predisposizione di almeno due canali, di cui uno informatico;

- verificare il buon funzionamento dei canali informativi predisposti in applicazione della disciplina, sia in termini di possibilità di inoltrare correttamente le segnalazioni che in termini di garanzia di riservatezza (se non di anonimato, se espressamente consentito) nell'intero processo di gestione della segnalazione.

L'ODV dovrà inoltre vigilare nel continuo sul rispetto dei divieti di ritorsione o di compimento di atti discriminatori nei confronti dei segnalanti per motivi collegati, direttamente o indirettamente, alle segnalazioni" (art. 6 comma 2-bis lett. c del Decreto), come ad es. demansionamenti e trasferimenti, accertandosi che la violazione di tali divieti sia espressamente prevista nel sistema disciplinare aziendale e che sia parimenti sanzionato chi "effettui con dolo o colpa grave segnalazioni che si rivelano infondate".

14. La privacy

Tra i reati presupposto del Decreto figurano alcune condotte attinenti alla normativa sulla privacy, la cui disciplina è contenuta nel Regolamento UE 2016/679 (c.d. GDPR - General Data Protection Regulation), in vigore dal 25.05.2018.

In particolare, l'art. 24-bis, rubricato "Delitti informatici e trattamento illecito dei dati", punisce con sanzioni pecuniarie e talvolta interdittive numerose condotte: accesso abusivo ad un sistema informatico; detenzione e diffusione abusiva di codici di accesso a sistemi informatici; diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche; frode informatica del soggetto che presta servizi di certificazione di firma elettronica; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblica utilità.

Alcune delle ipotesi delittuose sopra richiamate, alla luce della nuova normativa privacy, richiedono da parte dell'Organismo di Vigilanza un costante monitoraggio del processo di adeguamento alla normativa, tenuto conto del fatto che, nonostante la Banca non sia assoggettata agli obblighi di nomina di un DPO (Data Protection Officer) e di tenuta del c.d. Registro dei trattamenti, tratta comunque dati relativi a prestazioni sanitarie, come tali rientranti nel concetto di "particolari di dati personali" (art. 9 GDPR).

PARTE SPECIALE

Metodologia di calcolo

La Parte Speciale riporta la mappatura specifica dei rischi cui l'Ente potrebbe essere maggiormente esposto, elaborata con le modalità qui di seguito descritte.

Si premette che tale mappatura è suscettibile di continuo adeguamento in relazione sia a modifiche normative che a variazioni organizzative interne dell'Ente. Sarà compito dell'Organismo di Vigilanza, con l'ausilio degli Organi direttivi e del personale dell'Associazione, garantire che essa sia costantemente aggiornata, anche attraverso l'ausilio di un'apposita procedura software utile a valutare il grado di rischio.

Nella Sezione I il Modello contiene la mappatura del c.d. Rischio Iniziale (o Inerente), ovvero la rischiosità intrinseca di un reato 231 indipendentemente dalla sua rilevanza per l'Ente (che potrebbe essere inesistente), dalla probabilità che esso si realizzi o dagli accorgimenti che sono stati posti in essere per fare in modo che esso non si verifichi. Tale valutazione tiene conto della misura delle sanzioni pecuniarie ed interdittive previste dal Decreto 231 per ciascun reato presupposto.

Nella Sezione II viene invece individuato, attraverso la compilazione di Schede, il c.d. "Rischio residuo". Tali Schede talvolta riportano alcuni esempi operativi, da non considerarsi in alcun caso esaustivi ed unicamente funzionali a guidare l'operatore nell'aggiornamento del Modello. Il calcolo del Rischio residuo terrà conto, partendo dal Rischio Inerente, dei fattori di calmieramento presenti nell'organizzazione aziendale.

Sezione I

Individuazione del Rischio Inerente

Nella valutazione del Rischio Inerente è stato convenzionalmente assegnato al reato un valore:

- in base all'entità delle sanzioni pecuniarie, calcolato sulle relative quote;
- in base alle altre eventuali tipologie di sanzioni presenti ed in particolare:

DESCRIZIONE DELLA SANZIONE	GRAVITA'
Esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi	1
Divieto di pubblicizzare beni o servizi	2
Divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio	3
Sospensione / revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito	4
Interdizione dall'esercizio dell'attività	5

La somma dei valori è stata quindi riportata in un intervallo compreso tra 1 e 5, così determinando il livello complessivo del fattore di gravità:

VALORE	GRAVITA'	DESCRIZIONE
1	Bassissima	La Società subisce una lieve e simbolica sanzione
2	Bassa	La Società viene sanzionata in modo sensibile
3	Media	La Società subisce una sanzione di media entità in grado di danneggiare gli <i>stakeholder</i>
4	Alta	La Società subisce una sanzione di grave entità che ostacola sensibilmente l'ottenimento dei risultati che si era prefissata
5	Altissima	La Società vede interrotta la propria attività a causa di una sanzione 231

Tenuto conto dei criteri di cui sopra, il Rischio Inerente dei reati considerati più significativi ai fini 231 per l'attività dell'Ente è indicato nella seguente Tabella.

Articolo	Descrizione	Gravità	Valore
(Articolo 24 D.lgs. 231/2001) Art. 316-bis Codice Penale	Malversazione a danno dello Stato	Alta	4
(Articolo 24 D.lgs. 231/2001) Art. 316-ter Codice Penale	Indebita percezione di erogazioni a danno dello Stato	Alta	4
(Articolo 24 D.lgs. 231/2001) Art. 640-bis Codice Penale	Truffa aggravata per il conseguimento di erogazioni pubbliche	Alta	4
(Articolo 24 D.lgs. 231/2001) Art. 640-ter Codice Penale	Frode informatica	Alta	4
(Articolo 24 D.lgs. 231/2001) Art. 640 (comma 2, n.1) Codice Penale	Truffa	Alta	4
(Articolo 24-bis D.lgs. 231/2001) Art. 615-ter Codice Penale	Accesso abusivo ad un sistema informatico o telematico	Alta	4
(Articolo 24-bis D.lgs. 231/2001) Art. 615-quater Codice Penale	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	Media	3
(Articolo 24-bis D.lgs. 231/2001) Art. 615-quinquies Codice Penale	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	Media	3
(Articolo 24-bis D.lgs. 231/2001) Art. 617-quater Codice Penale	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	Alta	4
(Articolo 24-bis D.lgs. 231/2001) Art. 617-quinquies Codice Penale	Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche	Alta	4
(Articolo 24-bis D.lgs. 231/2001) Art. 640-quinquies Codice Penale	Frode informatica di soggetto che presta servizi di certificazione di firma elettronica	Alta	4

(Articolo 24-bis D.lgs. 231/2001) Art. 635-bis Codice Penale	Danneggiamento di informazioni, dati e programmi informatici	Media	3
(Articolo 24-bis D.lgs. 231/2001) Art. 635-ter Codice Penale	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità	Alta	4
(Articolo 24-bis D.lgs. 231/2001) Art. 635-quater Codice Penale	Danneggiamento di sistemi informatici e telematici	Alta	4
(Articolo 24-bis D.lgs. 231/2001) Art. 635-quinquies Codice Penale	Danneggiamento di sistemi informatici o telematici di pubblica utilità	Alta	4
(Articolo 24-bis D.lgs. 231/2001) Art. 491-bis Codice Penale	Falsità nei documenti informatici	Alta	4
(Articolo 24-ter D.lgs. 231/2001) Art. 416 Codice Penale	Associazione per delinquere	Altissima	5
(Articolo 24-ter D.lgs. 231/2001) Art. 416-bis Codice Penale	Associazioni di tipo mafioso anche straniere (anche transnazionale)	Altissima	5
(Articolo 24-ter D.lgs. 231/2001) Art. 630 Codice Penale	Sequestro di persona a scopo di estorsione	Altissima	5
(Articolo 24-ter D.Lgs.231/2001) Art. 74 DPR 309/1990	Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope	Altissima	5
(Articolo 24-ter D.lgs. 231/2001) Art. 407, c.2, lett a), n. 5 Codice di procedura penale	Delitti in materia di armi (termini di durata massima delle indagini preliminari)	Altissima	5
(Articolo 24-ter D.lgs. 231/2001) Art. 416-ter Codice Penale	Scambio elettorale politico-mafioso	Altissima	5
(Articolo 25 D.lgs. 231/2001) Art. 319 Codice Penale	Corruzione per un atto contrario ai doveri d'ufficio	Alta	4
(Articolo 25 D.lgs. 231/2001) Art. 322 Codice Penale	Istigazione alla corruzione	Alta	4
(Articolo 25 D.lgs. 231/2001) Art. 319-ter Codice Penale	Corruzione in atti giudiziari	Altissima	5
(Articolo 25 D.lgs. 231/2001) Art. 322-bis Codice Penale	Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri	Altissima	5
(Articolo 25 D.lgs. 231/2001) Art. 317 Codice Penale	Concussione	Altissima	5

(Articolo 25 D.lgs. 231/2001) Art. 319-quater Codice Penale	Induzione indebita a dare o promettere utilità	Altissima	5
(Articolo 25 D.lgs. 231/2001) Art. 318 Codice Penale	Corruzione per l'esercizio della funzione	Bassissima	1
(Articolo 25 D.lgs. 231/2001) Art. 320 Codice Penale	Corruzione di persona incaricata di un pubblico servizio	Altissima	5
(Articolo 25 D.lgs. 231/2001) Art. 346-bis Codice Penale	Traffico di influenze illecite	Bassissima	1
(Articolo 25-bis D.lgs. 231/2001) Art. 454 Codice Penale	Alterazione di monete	Alta	4
(Articolo 25-bis D.lgs. 231/2001) Art. 455 Codice Penale	Spendita e introduzione nello Stato, senza concerto, di monete falsificate	Alta	4
(Articolo 25-bis D.lgs. 231/2001) Art. 457 Codice Penale	Spendita di monete falsificate ricevute in buona fede	Bassissima	1
(Articolo 25-bis D.lgs. 231/2001) Art. 459 Codice Penale	Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati	Alta	4
(Articolo 25-bis D.lgs. 231/2001) Art. 460 Codice Penale	Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo	Alta	4
(Articolo 25-bis D.lgs. 231/2001) Art. 464 Codice Penale	Uso di valori di bollo contraffatti o alterati	Bassissima	1
(Articolo 25-bis D.lgs. 231/2001) Art. 473 Codice Penale	Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali	Alta	4
(Articolo 25-bis D.lgs. 231/2001) Art. 474 Codice Penale	Introduzione nello Stato e commercio di prodotti con segni falsi	Alta	4
(Articolo 25-bis D.lgs. 231/2001) Art. 453 Codice Penale	Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate	Altissima	5
(Articolo 25-bis D.lgs. 231/2001) Art. 461 Codice Penale	Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata	Alta	4
(Articolo 25-bis1 D.lgs. 231/2001) Art. 513 Codice Penale	Turbata libertà dell'industria o del commercio	Bassissima	1
(Articolo 25-bis1 D.lgs. 231/2001) Art. 513-bis Codice Penale	Illecita concorrenza con minaccia o violenza	Altissima	5
(Articolo 25-bis1 D.lgs. 231/2001) Art. 514 Codice Penale	Frodi contro le industrie nazionali	Altissima	5

(Articolo 25-bis1 D.lgs. 231/2001) Art. 515 Codice Penale	Frode nell'esercizio del commercio	Bassa	2
(Articolo 25-bis1 D.lgs. 231/2001) Art. 516 Codice Penale	Vendita di sostanze alimentari non genuine come se fossero tali	Bassa	2
(Articolo 25-bis1 D.lgs. 231/2001) Art. 517 Codice Penale	Vendita di prodotti industriali con segni mendaci	Bassa	2
(Articolo 25-bis1 D.lgs. 231/2001) Art. 517-ter Codice Penale	Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale	Bassa	2
(Articolo 25-bis1 D.lgs. 231/2001) Art. 517-quater Codice Penale	Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2622 Codice Civile	False comunicazioni sociali delle società quotate	Media	3
(Articolo 25-ter D.lgs. 231/2001) Art. 2621 Codice Civile	False comunicazioni sociali	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2635 (c. 3) Codice Civile	Corruzione tra privati	Media	3
(Articolo 25-ter D.lgs. 231/2001) Art. 2625, comma 2 Codice Civile	Impedito controllo	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2626 Codice Civile	Indebita restituzione dei conferimenti	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2627 Codice Civile	Illegale ripartizione degli utili e delle riserve	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2628 Codice Civile	Illecite operazioni sulle azioni o quote sociali e della società controllante	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2629 Codice Civile	Operazioni in pregiudizio dei creditori	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2632 Codice Civile	Formazione fittizia del capitale	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2633 Codice Civile	Indebita ripartizione dei beni sociali da parte dei liquidatori	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2636 Codice Civile	Illecita influenza sull'assemblea	Media	3
(Articolo 25-ter D.lgs. 231/2001) Art. 2637 Codice Civile	Aggiotaggio	Media	3

(Articolo 25-ter D.lgs. 231/2001) Art. 2638 Codice Civile	Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza	Media	3
(Articolo 25-ter D.lgs. 231/2001) Art. 2629-bis Codice Civile	Omessa comunicazione del conflitto di interessi	Media	3
(Articolo 25-ter D.lgs. 231/2001) Art. 2635-bis (c. 1) Codice Civile	Istigazione alla corruzione tra privati	Bassa	2
(Articolo 25-ter D.lgs. 231/2001) Art. 2623 Codice Civile	Falso in prospetto	Bassissima	1
(Articolo 25-ter D.lgs. 231/2001) Art. 2624 Codice Civile	Falsità nelle relazioni o nelle comunicazioni delle società di revisione	Bassissima	1
(Articolo 25-quater D.lgs. 231/2001) Art. 270-bis Codice Penale	Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 270-ter Codice Penale	Assistenza agli associati in terrorismo	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 270-quater Codice Penale	Arruolamento con finalità di terrorismo anche internazionale	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 270-quinquies Codice Penale	Addestramento ad attività con finalità di terrorismo anche internazionale	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 270-sexies Codice Penale	Condotte con finalità di terrorismo	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 280 Codice Penale	Attentato per finalità terroristiche o di eversione	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 280-bis Codice Penale	Atto di terrorismo con ordigni micidiali o esplosivi	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 270-quater1 Codice Penale	Organizzazione di trasferimenti per finalità di terrorismo	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 289-bis Codice Penale	Sequestro di persona a scopo di terrorismo o eversione	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 302 Codice Penale	Istigazione a commettere alcuno dei delitti previsti dai capi primo e secondo	Altissima	5
(Articolo 25-quater D.lgs. 231/2001) Art. 2 Convenzione internaz. New York 9.12.1999	Reati previsti convenzione per la repressione del finanziamento del terrorismo	Altissima	5

(Articolo 25-quater D.lgs. 231/2001) Art. 270-bis1 Codice Penale	Circostanze aggravanti e attenuanti	Altissima	5
(Art. 10, L. 16 marzo 2006, n.146) Art. 378 Codice Penale	Favoreggiamento personale (transnazionale)	Bassa	2
(Art. 10, L. 16 marzo 2006, n.146) Art. 291-quater D.P.R. 43/1973	Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (transnazionale)	Altissima	5
(Articolo 25-quater1 D.lgs. 231/2001) 583-bis Codice Penale	Pratiche di mutilazione degli organi genitali femminili	Altissima	5
(Art. 10, L. 16 marzo 2006, n.146) Art. 74 D.P.R. 309/1990	Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (transnazionale)	Altissima	5
(Articolo 25-quinquies D.lgs. 231/2001) Art. 600 Codice Penale	Riduzione o mantenimento in schiavitù o in servitù	Altissima	5
(Articolo 25-quinquies D.lgs. 231/2001) Art. 600-bis Codice Penale	Prostituzione minorile	Altissima	5
(Articolo 25-quinquies D.lgs. 231/2001) Art. 600-ter Codice Penale	Pornografia minorile	Altissima	5
(Articolo 25-quinquies D.lgs. 231/2001) Art. 600-quater Codice Penale	Detenzione di materiale pornografico	Media	3
(Articolo 25-quinquies D.lgs. 231/2001) Art. 600-quater1 Codice Penale	Pornografia virtuale	Altissima	5
(Articolo 25-quinquies D.lgs. 231/2001) Art. 600-quinquies Codice Penale	Iniziative turistiche volte allo sfruttamento della prostituzione minorile	Altissima	5
(Articolo 25-quinquies D.lgs. 231/2001) Art. 601 Codice Penale	Tratta di persone	Altissima	5
(Articolo 25-quinquies D.lgs. 231/2001) Art. 602 Codice Penale	Acquisto e alienazione di schiavi	Altissima	5
(Articolo 25-quinquies D.lgs. 231/2001) Art. 609-undecies Codice Penale	Adescamento di minorenni	Bassa	2
(Articolo 25-quinquies D.lgs. 231/2001) Art. 603-bis Codice Penale	Intermediazione illecita e sfruttamento del lavoro	Altissima	5
(Articolo 25-sexies D.lgs. 231/2001) Art. Parte V, titolo I bis, capo II - 184 D.Lgs. 58/1998	Abuso di informazioni privilegiate	Media	3

(Articolo 25-sexies D.lgs. 231/2001) Art. Parte V, titolo I bis, capo II - 185 D.Lgs. 58/1998	Manipolazione del mercato	Media	3
(Articolo 25-sexies D.lgs. 231/2001) Art. 14 Reg. UE 596/2014	Divieto di comunicazione illecita di informazioni privilegiate	Media	3
(Articolo 25-sexies D.lgs. 231/2001) Art. 15 Reg. UE 596/2014	Divieto di manipolazione del mercato	Media	3
(Articolo 25-septies D.lgs. 231/2001) Art. 589 Codice Penale	Omicidio colposo	Altissima	5
(Articolo 25-septies D.lgs. 231/2001) Art. 590 (terzo comma) Codice Penale	Lesioni personali colpose	Media	3
(Articolo 25-octies D.lgs. 231/2001) Art. 648 Codice Penale	Ricettazione	Altissima	5
(Articolo 25-octies D.lgs. 231/2001) Art. 648-bis Codice Penale	Riciclaggio	Altissima	5
(Articolo 25-octies D.lgs. 231/2001) Art. 648-ter Codice Penale	Impiego di denaro, beni o utilità di provenienza illecita	Altissima	5
(Articolo 25-octies D.lgs. 231/2001) Art. 648-ter1 Codice Penale	Autoriciclaggio	Altissima	5
(Articolo 25-novies D.lgs. 231/2001) Art. 171 (c. 1, lett. a-bis e c. 3) L. 633/1941	Divulgazione opere ingegno attraverso rete telematica	Alta	4
(Articolo 25-novies D.lgs. 231/2001) Art. 171-bis L. 633/1941	Reati in materia di software e banche dati (abusiva duplicazione di software per trarne profitto)	Alta	4
(Articolo 25-novies D.lgs. 231/2001) Art. 171-ter L. 633/1941	Reati opere dell'ingegno destinate a circuiti radiotelevisivi e cinematografico oppure letterarie, scientifiche e didattiche	Alta	4
(Articolo 25-novies D.lgs. 231/2001) Art. Art. 171-septies L. 633/1941	Violazioni nei confronti della SIAE	Alta	4
(Articolo 25-novies D.lgs. 231/2001) Art. Art. 171-octies L. 633/1941	Manomissione di apparati per la decodificazione di segnali audiovisivi ad accesso condizionato	Alta	4
(Articolo 25-decies D.lgs. 231/2001 + Art. 10, L. 16 marzo 2006, n.146) Art. 377-bis Codice Penale	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (anche transnazionale)	Bassa	2
(Articolo 25-undecies D.lgs. 231/2001) Art. 452-bis Codice Penale	Inquinamento ambientale	Alta	4

(Articolo 25-undecies D.lgs. 231/2001) Art. 452-quater Codice Penale	Disastro ambientale	Altissima	5
(Articolo 25-undecies D.lgs. 231/2001) Art. 452-quinquies Codice Penale	Delitti colposi contro l'ambiente	Bassa	2
(Articolo 25-undecies D.lgs. 231/2001) Art. 452-sexies Codice Penale	Traffico e abbandono di materiale ad alta radioattività	Bassa	2
(Articolo 25-undecies (Reati ambientali)) Art. 727-bis Codice Penale	Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette	Bassissima	1
(Articolo 25-undecies (Reati ambientali)) Art. 733-bis Codice Penale	Distruzione o deterioramento di habitat all'interno di un sito protetto	Bassissima	1
(Articolo 25-undecies D.lgs. 231/2001) Art. 137 D.Lgs. 152/2006	Sanzioni penali in materia di scarichi di acque reflue	Media	3
(Articolo 25-undecies D.lgs. 231/2001) Art. 256 D.Lgs. 152/2006	Attività di gestione di rifiuti non autorizzata	Media	3
(Articolo 25-undecies D.lgs. 231/2001) Art. 257 comma 1 e 2 D.Lgs. 152/2006	Mancata bonifica dei siti	Bassissima	1
(Articolo 25-undecies D.lgs. 231/2001) Art. 258 D.Lgs. 152/2006	Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari	Bassissima	1
(Articolo 25-undecies D.lgs. 231/2001) Art. 259 comma 1 D.Lgs. 152/2006	Traffico illecito di rifiuti	Bassissima	1
(Articolo 25-undecies D.lgs. 231/2001) Art. 279 comma 5 D.Lgs. 152/2006	Violazione limiti di emissioni atmosferiche	Bassissima	1
(Articolo 25-undecies D.lgs. 231/2001) Art. 1 o 2 L. 150/1992	Commercio di esemplari di specie dell'allegato A, appendice I, ed allegato C, parte 1 o appendice I e III, ed allegato C, parte 2	Bassissima	1
(Articolo 25-undecies D.lgs. 231/2001) Art. 3-bis (comma 1) L. 150/1992	Violazioni al regolamento di protezione di specie della flora e della fauna selvatiche	Bassa	2
(Articolo 25-undecies D.lgs. 231/2001) Art. 6 L. 150/1992	Divieto di detenzione di esemplari costituenti pericolo per la salute e l'incolumità pubblica	Bassissima	1
(Articolo 25-undecies D.lgs. 231/2001) Art. 8 comma 1 e 2 D.Lgs. 202/2007	Inquinamento doloso (navi)	Media	3
(Articolo 25-undecies D.lgs. 231/2001) Art. 9 comma 1 e 2 D.Lgs. 202/2007	Inquinamento colposo (navi)	Media	3
(Articolo 25-undecies D.lgs. 231/2001) Art. 452-quaterdecies c.p.	Attività organizzate per il traffico illecito di rifiuti	Altissima	5

(Articolo 25-undecies D.lgs. 231/2001) Art. 260-bis D.Lgs. 152/2006	Sistema informatico di controllo della tracciabilità dei rifiuti	Bassissima	1
(Articolo 25-duodecies D.lgs. 231/2001) Art. 22, comma 12-bis D.Lgs. 286/1998	Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	Bassissima	1
(Articolo 25-duodecies D.lgs. 231/2001 + Art. 10, L. 16 marzo 2006, n.146) Art. 12 D.Lgs. 286/1998	Disposizioni contro le immigrazioni clandestine (anche transnazionale)	Altissima	5
(Articolo 25-terdecies D.lgs. 231/2001) Art. 604-bis Codice Penale	Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa	Altissima	5
(Articolo 25-quaterdecies D.lgs. 231/2001) L. 39/2019	Frodi in competizioni sportive e gioco d'azzardo	Alta	4
(Art. 25 quinquiesdecies D.Lgs 231/2001) Art. 2 comma 1 e 2-bis D.L.74/2000	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti	Alta	4
(Art. 25 quinquiesdecies D.Lgs 231/2001) Art. 3 D.L.74/2000	Dichiarazione fraudolenta mediante altri artifici	Alta	4
(Art. 25 quinquiesdecies D.Lgs 231/2001) Art. 8 comma 1 e 2-bis D.L.74/2000	Emissione di fatture o altri documenti per operazioni inesistenti	Alta	4
(Art. 25 quinquiesdecies D.Lgs 231/2001) Art. 10 D.L.74/2000	Occultamento o distruzione di documenti contabili	Alta	4
(Art. 25 quinquiesdecies D.Lgs 231/2001) Art. 11 comma 2-bis D.L.74/2000	Sottrazione fraudolenta al pagamento di imposte	Alta	4

L'esito di tale valutazione, tenuto conto che i reati sono inseriti in categorie omogenee, è stato quindi ricondotto ad una seconda Tabella al fine di identificare il Rischio Inerente per Categoria, che l'Ente ritiene costituisca il riferimento più corretto per condurre una analisi sui rischi aziendali.

I parametri di riferimento sono stati i seguenti:

Valore (Numero reati/Somma valori rischio inerente)	Gravità
Inferiore a 2	Irrilevante
Da 2 a 2,9	Lieve
Da 3 a 3,9	Medio
Da 4 a 4,9	Grave
5	Gravissimo

L'esito di questa ulteriore valutazione è stato il seguente:

Articolo	Categoria reati	Gravità	Valore
24	Reati contro la Pubblica Amministrazione	Grave	4,0
24-bis	Delitti informatici e trattamento illecito di dati	Medio	3,7
24-ter	Delitti di criminalità organizzata	Gravissimo	5,0
25	Concussione, induzione indebita a dare o promettere utilità e corruzione	Medio	3,9
25-bis	Falsità in monete, carte di pubblico credito, valori di bollo e segni di riconoscimento	Medio	3,5
25-bis-1	Delitti contro l'industria e il commercio	Lieve	2,6
25-ter	Reati societari	Lieve	2,2
25-quater	Delitti con finalità di terrorismo o di eversione dell'ordine democratico	Gravissimo	5,0
25-quater-1	Pratiche di mutilazione degli organi genitali femminili	Gravissimo	5,0
25-quinquies	Delitti contro la personalità individuale	Grave	4,5
25-sexies	Abusi di mercato	Medio	3,0
25-septies	Reati commessi con violazione delle norme a tutela della salute e sicurezza sul lavoro	Grave	4,0
25-octies	Ricettazione, riciclaggio e autoriciclaggio	Gravissimo	5,0
25-novies	Delitti in materia di violazione del diritto d'autore	Grave	4,0
25-decies	Induzione a non rendere o a rendere dichiarazioni mendaci all'autorità giudiziaria	Lieve	2,0
25-undecies	Reati ambientali	Lieve	2,2
25-duodecies	Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare	Medio	3,0
25-terdecies	Razzismo e xenofobia	Gravissimo	5,0
25-quaterdecies	Frodi sportive e gioco d'azzardo	Grave	4,0
Legge 146/2006	Reati transnazionali	Gravissimo	5,0
25-quinquiesdecies	Frodi fiscali	Grave	4,0

Questa voce comparirà, in ciascuna Scheda, come "Rischio Inerente", e non sarà modificabile in quanto calcolata prescindendo, come sopra spiegato, da valutazioni di carattere soggettivo.

Sezione II

Calcolo del Rischio residuo

Come precisato in premessa, qui di seguito viene descritta la procedura di calcolo del c.d. "Rischio residuo", ottenuto decurtando dal valore di Rischio inerente i fattori di calmieramento presenti nell'organizzazione aziendale.

Per ciascuna categoria di reati è stata redatta un'apposita Scheda che riporta le seguenti informazioni:

- la rilevanza del rischio all'interno dell'organizzazione aziendale (se è irrilevante non si procede ad ulteriori valutazioni);
- la probabilità di verifica dell'illecito;
- l'entità ipotetica del danno (riferita al Rischio Inerente);
- i processi aziendali posti a presidio del rischio;
- le Unità organizzative coinvolte;
- i controlli (per tipo e frequenza) svolti dall'Ente;
- il Costo residuo di adozione.

La Scheda potrà anche riportare alcune criticità (con relativi suggerimenti) individuate dall'ODV e cenni alle misure adottate dalla Struttura per presidiare il rischio.

Voce	Note
RILEVANZA	
Rilevanza concreta (in IPOTESI DELITTUOSE)	Delimita l'ambito di intervento dell'ODV, individuando i reati che hanno possibilità di essere commessi nel contesto aziendale da quelli che, al contrario, non hanno alcuna possibilità di verifica. In quest'ultimo caso, il Rischio Residuo è sempre irrilevante
RISCHIO INERENTE	
Rischio Inerente (DATO NON MODIFICABILE)	Viene calcolato in modo oggettivo, sulla base dell'entità delle sanzioni pecuniarie, calcolato sulle relative quote e delle altre eventuali tipologie di sanzioni presenti (ad es. interdittive).
MISURAZIONE	
Probabilità di accadimento	Individua la probabilità di verifica dell'evento, da IMPROBABILE a MOLTO PROBABILE
U.O. coinvolta	Individua le Unità Operative potenzialmente coinvolte nella realizzazione delle condotte illecite, sia in veste esecutiva che decisionale. È possibile inserire fino a 3 Unità (ognuna delle quali eredita, come informazione aggiuntiva, la propria autonomia di spesa)
Doc. processo	Individua i presidi documentali (processi, regolamenti, ordini di servizio etc.) destinati a regolare le condotte prodromiche ad ogni fattispecie criminosa. È possibile inserire fino a 3 riferimenti (ognuno dei quali eredita, come informazione aggiuntiva, l'eventuale segregazione, ovvero l'affidamento a più soggetti diversi della esecuzione del processo)

U.O. controllo	Individua l'Unità Operativa coinvolta in fase di controllo, con il relativo Tipo (1°, 2° o 3° livello) e la frequenza con cui questo viene eseguito (da AD EVENTO a IN CONTINUITA'). E' possibile inserire fino a 3 Unità
Costo residuo	Indica il costo (economico o organizzativo) occorrente per adottare le misure necessarie per eliminare/ridurre il rischio reato. Costituisce un fattore di rischio in quanto, più è alto il costo residuo, più l'Ente potrebbe essere portato a non adottare tali misure
Calmieramento generico	Indica, in percentuale, l'incidenza che alcuni fattori di calmieramento hanno sull'organizzazione dell'Ente e la loro relativa attitudine ad evitare/gestire i rischi aziendali. I fattori attualmente sono 7 ed ognuno può incidere in misura diversa, da "irrilevante" a "molto" (comportando una diminuzione massima complessiva del rischio residuo)

Controllo (per Tipo)

I^ livello	<u>controlli di linea</u> , effettuati dalle stesse strutture produttive che hanno posto in essere le operazioni o incorporati nelle procedure e diretti ad assicurare il corretto svolgimento delle operazioni
II^ livello	<p><u>controlli sulla gestione dei rischi</u>, condotti a cura di una struttura interna (Funzione di Risk Controlling/ Management), contraddistinta dalla piena separatezza dalle funzioni operative, avente il compito di definire le metodologie di misurazione dei rischi, verificare il rispetto dei limiti assegnati alle varie funzioni operative e controllare la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio/rendimento, quantificare il grado di esposizione ai rischi e gli eventuali impatti economici;</p> <p><u>controlli di conformità normativa</u>, svolti dalla Funzione indipendente all'uopo costituita con il compito specifico di promuovere il rispetto delle leggi, delle norme, dei codici interni di comportamento per minimizzare il rischio di non conformità normativa e i rischi reputazionali a questo collegati contribuendo, per gli aspetti di competenza, alla realizzazione del modello aziendale di monitoraggio e gestione dei rischi.</p>
III^ livello	<u>attività di revisione interna</u> (Internal Auditing, Collegio Sindacale, Società di Revisione), volta a valutare l'adeguatezza e la funzionalità del complessivo Sistema dei Controlli Interni e ad individuare andamenti anomali delle procedure e della regolamentazione.

Grazie all'inserimento del valore "Fattore di calmieramento generico" l'ODV sarà libero di valutare – ed apprezzare numericamente - la presenza di quegli elementi di riduzione del rischio che possono agire in modo trasversale per tutti i reati. In particolare, rientrano tra i suddetti fattori i seguenti 5, menzionati nelle linee guida delle maggiori associazioni di categoria:

1. Definizione delle autonomie di spesa e dei poteri di firma
2. Formalizzazione dell'organigramma aziendale
3. Segregazione di compiti e funzioni
4. Definizione delle procedure per lo svolgimento delle attività sensibili (presidi)
5. Tracciabilità delle attività svolte e dei controlli effettuati (controlli)

Grado di probabilità

Voce	Definizione
Improbabile	<ul style="list-style-type: none"> - Non sono noti episodi già verificati - L'evento si può verificare solo per una concatenazione di eventi improbabili e tra loro indipendenti - Il verificarsi dell'evento susciterebbe incredulità in azienda - rischi a livello di assenza di probabilità (Improbabile – Trascurabile – Irrilevante) e perciò accettabili anche in assenza di azioni correttive - la mancanza rilevata può provocare un danno per la concomitanza di più eventi poco probabili e indipendenti - non sono noti eventi o episodi già verificatisi.
Poco probabile	<ul style="list-style-type: none"> - Sono noti rari episodi già verificati - l'evento può verificarsi solo in circostanze particolari - il verificarsi dell'evento susciterebbe sorpresa in azienda - rischi con probabilità trascurabile (Poco Probabile - Tollerabile – Basso) - il pericolo può provocare un danno solo in circostanze sfortunate
Probabile	<ul style="list-style-type: none"> - È noto qualche episodio in cui il pericolo ha causato danno - il pericolo può trasformarsi in danno anche se non in modo automatico - il verificarsi dell'evento susciterebbe scarsa sorpresa in azienda - rischi con probabilità di esposizione media (Probabile - Moderato – Medio) che l'impresa deve gestire e governare - il pericolo può provocare un danno anche se in modo automatico o diretto - è noto qualche episodio in cui la mancanza ha fatto seguire un danno
Molto probabile	<ul style="list-style-type: none"> - sono noti episodi in cui la commissione ha causato danno - il pericolo esiste e può trasformarsi in danno - il verificarsi dell'evento non susciterebbe sorpresa/incredulità in azienda - rischi con elevato livello di probabilità di impatto che rappresentano un rischio NON accettabile (Molto Probabile – Intollerabile - Alto) che l'impresa deve assolutamente eliminare - esiste una correlazione diretta tra il pericolo ed il verificarsi del danno ipotizzato - si sono già verificati danni per la stessa mancanza rilevata nella stessa azienda o in aziende simili

Valutazione del Rischio residuo

Al termine della misurazione, le categorie di reato sono state suddivise nei seguenti livelli di Rischio residuo.

Voce	Definizione
Irrelevante	Il rischio-reato è molto al di sotto della soglia di accettabilità (sia per la non riferibilità concreta del reato alla attività dell'Ente che per la sua assoluta improbabilità di verificazione, anche alla luce dei presidi e controlli esistenti) e quindi, a meno di modificazioni nell'organizzazione dell'Ente o nella sua operatività, non sono richiesti interventi.
Basso	Il rischio-reato è entro la soglia di accettabilità. I presidi ed i controlli esistenti consentono di arginarne la verificabilità entro margini di tranquillità per l'Ente, che potrà omettere o comunque rinviare interventi correttivi salvo verificare nel continuo la perdurante adeguatezza di quelli esistenti
Medio	Il rischio-reato è al limite della soglia di accettabilità e l'Ente dovrà programmare interventi correttivi, sia in termini di presidi che di controlli, per ricondurlo rapidamente entro tale soglia.
Alto	Il rischio-reato è al di sopra della soglia di accettabilità e pertanto richiede un rapido intervento degli organi decisionali dell'Ente per la introduzione di presidi e controlli che evitino la commissione dell'illecito e la verificazione del danno, onde ridurre l'attuale elevato livello di probabilità di una sua verificazione.
Altissimo	Il rischio-reato è ad un livello inaccettabile. Il pericolo esiste e può trasformarsi in danno con un alto grado di probabilità. Gli organi decisionali dell'Ente sono chiamati ad intervenire immediatamente per ricondurre il grado di rischio ad un livello accettabile, attraverso interventi sostanziali (ad es. segregazione) e formali (processi, controlli) nell'organizzazione dell'Ente.

L'appartenenza ad un livello costituisce per l'Ente un elemento per valutare la propria organizzazione interna e per indirizzare e pianificare l'attività di calmiamento del rischio, mentre per l'Organismo di Vigilanza rappresenta un indice utile per orientare e programmare i controlli.

L'ODV, indipendentemente dalle risultanze informatiche, sarà comunque libero di considerare con maggiore severità quei reati che, per il particolare ambito di attività dell'Ente, potrebbero risultare particolarmente gravi in termini di danno di immagine e reputazione.

ATTENZIONE

SEBBENE LE SCHEDE CONTENGANO ALCUNE NOTE ESPLICATIVE DEI SINGOLI REATI E ALCUNE IPOTESI DI COMMISSIONE DELL'ILLECITO, TALI INFORMAZIONI NON POSSONO CONSIDERARSI ASSOLUTAMENTE ESAUSTIVE. LE NOTE SONO UTILI ALL'OPERATORE ESCLUSIVAMENTE PER L'INQUADRAMENTO GENERALE DELLA NORMATIVA, SENZA ALCUNA PRETESA DI COMPLETEZZA E SENZA POTER SOSTITUIRE IL PARERE LEGALE DELL'ODV O DI UN PROFESSIONISTA.

ALLO STESSO MODO, LE IPOTESI DI COMMISSIONE DELL'ILLECITO SERVONO SOLO PER INDICARE, SENZA PRETESE DI COMPLETEZZA, IN QUALI SITUAZIONI O CON QUALI MODALITA' POTREBBE COMMITTERSI L'ILLECITO NELLA OPERATIVITA' DELL'ENTE, FERMO RESTANDO CHE LA LORO RILEVANZA AI FINI 231 DOVRA' ESSERE VALUTATA DALL'ODV O DA UN PROFESSIONISTA ESPERTO DELLA MATERIA, ANCHE PER VERIFICARE LA NECESSARIA SUSSISTENZA DI UN INTERESSE O DI VANTAGGIO PER L'ENTE.

REPORT RILEVANZA E FATTORI DI RISCHIO PER CATEGORIA

N.	Articolo	Categoria reati	Rilevanza	Rischio inerente	Rischio residuo	Valutazione ODV
1	24	Reati contro la Pubblica Amministrazione	SI	ALTO	BASSO	BASSO
2	24-bis	Delitti informatici e trattamento illecito di dati	SI	MEDIO	BASSO	BASSO
3	24-ter	Delitti di criminalità organizzata	SI	ALTISSIMO	IRRILEVANTE	IRRILEVANTE
4	25	Concussione e corruzione	SI	MEDIO	BASSO	BAS (PRUDENZA)
5	25-bis	Falsità in monete, carte di credito e valori di bollo	SI	MEDIO	BASSO	BASSO
6	25-bis-1	Delitti contro l'industria e il commercio	NO	BASSO	BASSO	ASSENTE
7	25-ter	Reati societari	SI	BASSO	IRRILEVANTE	IRR (PRUDENZA)
8	25-quater	Delitti con finalità di terrorismo o di eversione	SI	ALTISSIMO	IRRILEVANTE	IRRILEVANTE
9	25-quater-1	Pratiche di mutilazione degli organi genitali femminili	NO	ALTISSIMO	MEDIO	ASSENTE
10	25-quinquies	Delitti contro la personalità individuale	SI	ALTO	BASSO	BASSO
11	25-sexies	Abusi di mercato	SI	MEDIO	IRRILEVANTE	IRRILEVANTE
12	25-septies	Reati sulla salute e sicurezza sul lavoro	SI	ALTO	MEDIO	MEDIO
13	25-octies	Ricettazione, riciclaggio e autoriciclaggio	SI	ALTISSIMO	MEDIO	MEDIO
14	25-novies	Delitti in materia di violazione del diritto d'autore	SI	ALTO	IRRILEVANTE	MEDIO
15	25-decies	Induzione a rendere dichiarazioni mendaci all'A.G.	SI	BASSO	IRRILEVANTE	BASSO
16	25-undecies	Reati ambientali	SI	BASSO	BASSO	BASSO
17	25-duodecies	Impiego di cittadini extracomunitari irregolari	SI	MEDIO	BASSO	BASSO
18	25-terdecies	Razzismo e xenofobia	NO	ALTO	MEDIO	ASSENTE
19	25-quaterdecies	Frodi sportive e gioco d'azzardo	NO	BASSO	BASSO	ASSENTE
20	Legge 146/2006	Reati transnazionali	NO	ALTO	MEDIO	ASSENTE
21	25-quinquiesdecies	Reati fiscali	SI	ALTO	IRRILEVANTE	IRRILEVANTE

PROCESSI

Processo	Tipo documentazione	Segregaz.	Adozione	Note
Tesoreria Enti	Processo	SI		
Contabilità Bilancio e Segnalazioni	Processo	SI		
Risorse Umane	Processo	SI		
Infrastruttura e Spese	Processo	SI		
Incassi e Pagamenti	Regolamento	SI		
Auto aziendali	Nota operativa	SI		
Gestione Reclami	Processo	SI		
Privacy	Processo	SI		
Salute e Sicurezza	Processo	SI		
Antiriciclaggio	Processo	SI		
Contante e valori	Processo	SI		
Trasparenza	Processo	SI		
Sicurezza informatica	Regolamento	SI		
Bancassicurazione	Processo	SI		
Finanza e Market Abuse	Processo	SI		
Credito	Processo	SI		
Risparmio	Processo	SI		
Whistleblowing	Regolamento	SI		
Codice Etico	Codice	SI		
Regolamento Disciplinare	Regolamento	SI		
Eestero	Processo	SI		
Regolamento Interno	Regolamento	SI		
Single Customer View	Policy	SI		
Conflitti di interesse	Processo	SI		
OMR Operazioni Maggior Rilievo	Regolamento	SI		
RAF Risk Appetite Framework	Processo	SI		
Funzionamento Organi e Flussi Informativi	Regolamento	SI		
Esternalizzazioni	Policy	SI		
Politiche remunerazione	Policy	SI		
ICAAP	Processo	SI		
Anagrafe	Processo	SI		
Soci	Processo	SI		
Statuto	Codice	SI		
Regolamento elettorale	Regolamento	SI		
Contributi e Sponsorizzazioni	Regolamento	SI		
Continuità Operativa	Processo	SI		
Internet Banking	Processo	SI		
Fiscale	Processo	SI		
Information and Communication Tecnology	Processo	SI		

RIEPILOGO SISTEMA DEI FLUSSI

N.	Flusso	Frequenza
1	Programmazione formazione in ambito 231, Whistleblowing ed altre materie rilevanti (ad es. antiriciclaggio, sicurezza sul lavoro)	Annuale
2	Attestazione del rispetto, da parte dei responsabili delle U.O., delle norme di comportamento prescritte nel MOG	Annuale
3	Contratti con fornitori che per modalità di conclusione (ad es. urgenza o fuori procedure standard) o per condizioni (ad es. sottocosto) pres	Ad evento
4	Segnalazione di criticità o violazioni del Modello 231 (anche verbali di CdA o CS sull'argomento)	Ad evento
5	Segnalazioni Whistleblowing (rese anonime) e Privacy che rilevano ai fini 231	Ad evento
6	Richieste di chiarimenti in merito alla disciplina 231 (compreso il Modello ed i Flussi) e Whistleblowing	Ad evento
7	Richieste di assistenza legale da parte di dipendenti	Ad evento
8	Verifiche sull'utilizzo di materiali coperti da diritto d'autore (manifestazioni/pubblicità/organi di stampa/licenze software)	Ad evento
9	Verbali di accertamento, a posteriori, delle cause che hanno condotto al verificarsi - o al rischio di commissione - di un reato	Ad evento
10	Verbali e rapporti di certificazione dei sistemi tecnici ed informatici (impianti, strumentazioni, reti) che hanno evidenziato criticità	Ad evento
11	Relazioni intrattenute con A.G., GG.FF. o P.A. e sogg. collegati diverse da accertamento e verifica (ad es. Convenzioni, Sponsorizzazioni,	Ad evento
12	Contestazioni/indagini/provedimenti delle Autorità (A.G., polizia giud., vigilanza, fiscale, lavoro, privacy etc.)	Ad evento
13	Assunzione da parte del personale (compresi coniugi e familiari) di incarichi in enti pubblici	Ad evento
14	Procedimenti/provedimenti sanzionatori a carico di dipendenti o esponenti aziendali	Ad evento
15	Finanziamenti ottenuti da PA per finalità della Banca o mutui di scopo concessi a clienti col contributo di un Ente pubblico per finalità di pu	Ad evento
16	Eventi infortunistici (lesioni gravi e gravissime), relazioni e verbali di verifica in materia di sicurezza sul lavoro	Ad evento
17	Testimonianze rese alle Autorità Competenti	Ad evento
18	Verbali di verifica e controllo, relazioni periodiche, verbali e autovalutazioni in materia di Antiriciclaggio (se con criticità)	Ad evento
19	Verbali di verifica e controllo, relazioni periodiche, verbali e autovalutazioni in materia di Compliance (se con criticità)	Ad evento
20	Verbali di verifica e controllo, relazioni periodiche, verbali e autovalutazioni in materia di Risk Management (se con criticità)	Ad evento
21	Verbali di verifica e controllo, relazioni periodiche, verbali e autovalutazioni in materia di Audit (se con criticità)	Ad evento

REATO

N.	Articolo	Categoria reati
1	<u>24</u>	<u>Reati contro la Pubblica Amministrazione</u>
2	<u>24-bis</u>	<u>Delitti informatici e trattamento illecito di dati</u>
3	<u>24-ter</u>	<u>Delitti di criminalità organizzata</u>
4	<u>25</u>	<u>Concussione e corruzione</u>
5	<u>25-bis</u>	<u>Falsità in monete, carte di credito e valori di bollo</u>
6	<u>25-bis-1</u>	<u>Delitti contro l'industria e il commercio</u>
7	<u>25-ter</u>	<u>Reati societari</u>
8	<u>25-quater</u>	<u>Delitti con finalità di terrorismo o di eversione</u>
9	<u>25-quater-1</u>	<u>Pratiche di mutilazione degli organi genitali femminili</u>
10	<u>25-quinquies</u>	<u>Delitti contro la personalità individuale</u>
11	<u>25-sexies</u>	<u>Abusi di mercato</u>
12	<u>25-septies</u>	<u>Reati sulla salute e sicurezza sul lavoro</u>
13	<u>25-octies</u>	<u>Ricettazione, riciclaggio e autoriciclaggio</u>
14	<u>25-novies</u>	<u>Delitti in materia di violazione del diritto d'autore</u>
15	<u>25-decies</u>	<u>Induzione a rendere dichiarazioni mendaci all'A.G.</u>
16	<u>25-undecies</u>	<u>Reati ambientali</u>
17	<u>25-duodecies</u>	<u>Impiego di cittadini extracomunitari irregolari</u>
18	<u>25-terdecies</u>	<u>Razzismo e xenofobia</u>
19	<u>25-quaterdecies</u>	<u>Frodi sportive e gioco d'azzardo</u>
20	<u>Legge 146/2006</u>	<u>Reati transnazionali</u>
21	<u>25-quinquiesdecies</u>	<u>Reati fiscali</u>

FLUSSI

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Red	Yellow	Red	Yellow	Red	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Red	Yellow	Yellow	Red	Yellow	Red	White	Yellow	White	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Red	Yellow	White	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	Red	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Red	Yellow	White	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	Red	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey	Grey
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red
Yellow	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	Yellow	White	Yellow	Yellow	Yellow	Yellow	White	White	White	White	Red	Red	Red

ORGANIZZAZIONE INTERNA (U.O., UFFICI, FUNZIONI)

Nome Unità	ABBR.	Autonom. spesa
REFERENTE ODV	RODV	NO
Consiglio di Amministrazione	CDA	SI
Collegio Sindacale	CS	NO
Comitato Esecutivo	CE	SI
Società di revisione	REV	NO
Direzione Generale	DIR	SI
Segreteria Generale	SEG	NO
Comunicazione	COM	SI
Supporto gestionale	SUP	NO
Risorse Umane	RU	NO
Soci	SOC	NO
Organizzazione	ORG	SI
Direzione Amministrativa	DA	SI
Servizio Finanza	FIN	NO
Economato e Logistica	ECO	SI
Servizio Crediti	CRED	SI
Area PNP	PNP	SI
Antiriciclaggio	AML	NO
Compliance	COM	NO
Risk Management	RM	NO
DPO	DPO	NO
Dirigente Sicurezza	DS	SI
Responsabile Servizio Prevenzione e Protezione	RSPP	NO
Federazione Toscana BCC	FTBCC	NO
Audit	AUD	NO
BCCSI	BCCSI	NO
Sinergia	SIN	NO
Società Portavalori	VAL	NO
Direzione Mercato	MKT	SI
Unità di Supporto	UDS	NO