



**SPARKASSE
CASSA DI RISPARMIO**

Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001 della Cassa di Risparmio di Bolzano S.p.A.

Versione approvata dal Consiglio di Amministrazione del 22-09-2009



1. Parte Generale	5
1.1. Il Decreto Legislativo 231/2001	5
1.1.1 Premessa	5
1.1.2 Normativa	5
1.2. Adozione del Modello organizzativo da parte della Banca	9
1.2.1 Struttura del Modello di organizzazione, gestione e controllo	9
1.2.2 Modifiche e integrazioni del Modello	10
1.3. Metodologia per l'individuazione delle attività sensibili e dei processi di supporto	10
1.4. Individuazione delle attività a rischio reato	10
1.5. Destinatari del modello	12
1.6. Organismo di Vigilanza	13
1.6.1 Composizione, nomina e revoca dell'Organismo di vigilanza	13
1.7. Ruolo dell'Organismo di vigilanza	15
1.8. Coordinamento dell'Organismo di vigilanza con altri Organi e funzioni aziendali	16
1.9. Poteri dell'Organismo di vigilanza	16
1.10. Flussi informativi delle singole funzioni diretti all'Organismo di vigilanza	16
1.11. Flussi informativi dell'Organismo di Vigilanza diretti agli Organi aziendali	18
1.12. Responsabilità dell'Organismo di Vigilanza	18
1.13. La formazione delle risorse e la diffusione del Modello	19
1.13.1 Formazione ed informazione dei Dipendenti	19
1.13.2 Consulenti, collaboratori e fornitori	19
1.14. Sistema disciplinare	20
1.15. Aggiornamento ed adeguamento del Modello	20
2. Parte Speciale	21
2.1. Norme emanate ai fini del D.Lgs. 231/01	21
2.1.1 Fonti normative	21
2.1.2 Principi generali di comportamento	21
2.2. Approccio metodologico	21
2.3. I potenziali reati	22
2.4. Rapporti con la Pubblica Amministrazione	26



2.4.1	I principi di comportamento da tenere nell'ambito dei rapporti con la Pubblica Amministrazione	27
2.4.2	Compiti specifici dell'Organismo di Vigilanza	27
2.5.	Prevenzione dei reati societari	28
2.5.1	I principi di comportamento da tenere per la prevenzione di reati societari	28
2.5.2	Compiti dell'Organismo di Vigilanza	28
2.6.	Prevenzione dei reati in materia di abusi di mercato	29
2.6.1	Le informazioni privilegiate	29
2.6.2	I principi di comportamento da tenere per la prevenzione dei reati in materia di abusi di mercato	30
2.6.3	Compiti dell'Organismo di Vigilanza	30
2.7.	Prevenzione dei reati in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	30
2.7.1	I principi di comportamento da tenere nell'ambito del rispetto delle norme antinfortunistiche e della tutela dell'igiene e della salute del lavoro.	31
2.7.2	Compiti dell'Organismo di Vigilanza	32
2.8.	Prevenzione dei reati in violazione delle norme anti-riciclaggio	32
2.8.1	I principi di comportamento da tenere nell'ambito del rispetto delle norme anti-riciclaggio	33
2.8.2	Compiti dell'Organismo di Vigilanza	33
2.9.	Prevenzione reati connessi alla criminalità organizzata nazionale e transnazionale	34
2.9.1	Compiti dell'Organismo di Vigilanza	34
2.10.	Prevenzione dei Reati in violazione delle norme in materia di delitti informatici e trattamento illecito di dati	34
2.10.1	I principi di comportamento da tenere per la prevenzione dei reati in violazione delle norme in materia di delitti informativi e trattamento illecito dei dati	35
2.10.2	Compiti dell'Organismo di Vigilanza	36
2.11.	Reati in materia di falsità di monete, in carte di pubblico credito, in valori in bollo e in strumenti o segni di riconoscimento	36
2.12.	Delitti in materia di terrorismo o di eversione dell'ordine democratico	36
2.13.	Delitti contro l'industria ed il commercio ed in materia di violazione del diritto d'autore	37
2.14.	Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	37
3.	Glossario	38



1. Parte Generale

1.1. Il Decreto Legislativo 231/2001

1.1.1 Premessa

Il Gruppo Cassa di Risparmio di Bolzano (di seguito il "Gruppo") è sensibile all'esigenza di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività bancarie, a tutela della propria posizione ed immagine nonché del lavoro dei propri dipendenti.

La Cassa di Risparmio di Bolzano S.p.A. (di seguito la "Capogruppo" o la "Banca") ha ritenuto conforme alla propria politica procedere alla formalizzazione del Modello Organizzativo previsto dal Decreto Legislativo 231/2001 (di seguito anche il "Decreto" o "D.Lgs. 231/01").

A tal fine, la Banca ha avviato un progetto di analisi dei propri strumenti organizzativi, di gestione e di controllo, volto a verificare la corrispondenza dei principi comportamentali e delle procedure già adottate alle finalità previste dal Decreto.

Il presente Modello ed i principi in esso contenuti disciplinano i comportamenti degli Organi societari, dei dipendenti, dei collaboratori, dei consulenti, dei fornitori e, più in generale, di tutti coloro che, a qualunque titolo, operano nell'ambito delle attività "sensibili" per conto o nell'interesse della Banca (di seguito "Destinatari").

1.1.2 Normativa

Il Decreto Legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300" ha affiancato alla responsabilità penale della persona fisica colpevole del reato, una nuova forma di responsabilità per l'ente nell'ambito del procedimento penale.

L'ampliamento della responsabilità mira a coinvolgere nella sanzione di taluni illeciti penali il patrimonio degli enti e, in definitiva, gli interessi economici dei soci, i quali, fino all'entrata in vigore della legge in esame, non pativano conseguenze dalla realizzazione di reati commessi, con vantaggio della società, da amministratori e/o dipendenti. Il principio costituzionale di personalità della responsabilità penale lasciava indenne l'ente da conseguenze sanzionatorie, diverse dall'eventuale risarcimento del danno, se ed in quanto esistente.

1.1.2.1 I reati

In origine, il legislatore delegato aveva operato una scelta minimalista rispetto alle indicazioni contenute nella legge delega (l. n. 300/2000). Infatti, delle quattro categorie di reati indicate nella legge n. 300/2000, il Governo aveva preso in considerazione soltanto i maggiori reati contro la pubblica amministrazione, evidenziando, nella relazione di accompagnamento al D. Lgs. n. 231/2001, la prevedibile estensione della disciplina in questione anche ad altre categorie di reati.

Infatti, successivi interventi normativi hanno esteso il catalogo dei reati per cui si applica la disciplina del decreto n. 231/2001.

L'art. 4 della legge 23 novembre 2001, n. 409 ha introdotto l'art. 25-bis nel Decreto relativo alle falsità in monete, carte di pubblico credito e in valori di bollo.

L'intervento più importante è stato attuato dal D. Lgs. n. 61/2002 che ha riformato la materia dei reati societari, aggiungendo al decreto n. 231 l'art. 25-ter, ed estendendo la responsabilità ad alcune fattispecie di reati societari commessi nell'interesse (ma non anche a vantaggio, come invece previsto dal Decreto) della società da amministratori, direttori generali, liquidatori o da



persone sottoposte alla loro vigilanza, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità agli obblighi inerenti la loro carica.

L'art. 25-ter disciplina, in particolare, i reati di: falsità in bilancio, nelle relazioni e nelle altre comunicazioni sociali, falso in prospetto, falsità nelle relazioni o comunicazioni della società di revisione, impedito controllo, formazione fittizia del capitale, indebita restituzione dei conferimenti, illegale ripartizione degli utili e delle riserve, illecite operazioni sulle azioni o quote sociali o della società controllante, operazioni in pregiudizio dei creditori, indebita ripartizione dei beni sociali da parte dei liquidatori, indebita influenza sull'assemblea, aggio, ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.

Successivamente, la legge di "Ratifica ed esecuzione della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999", ha inserito l'art. 25-quater al decreto 231, che stabilisce la responsabilità amministrativa dell'ente anche in relazione alla commissione dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico. La legge trova inoltre applicazione (art. 25-quater, ult. co.) con riferimento alla commissione di delitti, diversi da quelli espressamente richiamati, "che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999".

La legge contenente "Misure contro la tratta delle persone" ha, introdotto l'articolo 25-quinquies al decreto, che estende il regime della responsabilità dell'ente anche in relazione alla commissione dei delitti contro la personalità individuale disciplinati dalla sezione I del capo III del titolo XII del libro II del codice penale.

Successivi interventi diretti a modificare la disciplina della responsabilità amministrativa degli enti sono stati attuati con la Legge Comunitaria per il 2004 (art. 9) che, tra l'altro, ha recepito mediante norme di immediata applicazione la direttiva 2003/6/CE del Parlamento europeo e del Consiglio, del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (c.d. abusi di mercato), e con la c.d. "Legge sul Risparmio" che ha apportato alcune modifiche e inasprimenti al regime della responsabilità delle persone giuridiche riguardo, tra l'altro, ai reati societari.

La nuova normativa in materia di abusi di mercato ha ampliato l'ambito di applicazione del decreto 231, facendo rientrare nel novero degli illeciti "presupposto" della responsabilità amministrativa degli enti le fattispecie dell'abuso di informazioni privilegiate (c.d. insider trading) e della manipolazione del mercato.

La Legge Comunitaria 2004, in particolare, è intervenuta sia sul codice civile che sul Testo Unico della Finanza (TUF).

Quanto al codice civile, è stato modificato l'art. 2637, che sanzionava il reato di aggio commesso su strumenti finanziari sia quotati che non quotati. Ad oggi, la norma si applica ai soli casi di aggio posti in essere con riferimento a strumenti finanziari non quotati o per i quali non è stata presentata richiesta di ammissione alle negoziazioni in un mercato regolamentato, e non invece a quelli quotati, cui si applicano le norme del TUF in materia di manipolazione di mercato.

È invece riferita alle sole informazioni privilegiate relative a società emittenti disciplinate dal TUF la nuova fattispecie dell'insider trading (o abuso di informazioni privilegiate).

La legge n. 262/2005 sulla tutela del risparmio ha invece esteso la responsabilità degli enti alla nuova fattispecie di reato di omessa comunicazione del conflitto di interessi degli amministratori, riguardante esclusivamente le società quotate, e modificato le norme sulle false comunicazioni sociali e sul falso in prospetto.

Ulteriori modifiche legislative in materia di responsabilità degli enti sono state introdotte dalla legge n. 7/2006, che vieta e punisce le c.d. pratiche di infibulazione, dalla legge n. 38/2006, contenente "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la



pedopornografia anche a mezzo Internet” e, infine, dalla legge di ratifica ed esecuzione della Convenzione di Palermo sulla criminalità organizzata transnazionale del 15 novembre 2000.

La legge sulla prevenzione e divieto delle c.d. pratiche di infibulazione, ha poi esteso l'ambito di applicazione del D. Lgs. n. 231/2001 al nuovo reato di pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.).

La legge 6 febbraio 2006, n. 38, ha modificato l'ambito di applicazione dei delitti di pornografia minorile e detenzione di materiale pornografico (rispettivamente, artt. 600-ter e 600-quater c.p.), per i quali era già prevista la responsabilità dell'ente ex decreto 231, includendo anche le ipotesi in cui il materiale pornografico utilizzato rappresenti immagini virtuali di minori (c.d. “pedopornografia virtuale”).

La legge n. 146/2006 di ratifica ed esecuzione della Convenzione ONU contro il crimine organizzato transnazionale, ha stabilito l'applicazione del decreto 231 ai reati di criminalità organizzata transnazionale. Le nuove disposizioni hanno previsto la responsabilità degli enti per gli illeciti amministrativi dipendenti dai delitti di associazione a delinquere, riciclaggio e impiego di denaro e beni di provenienza illecita, traffico di migranti e intralcio alla giustizia.

Successivamente, la legge 3 agosto 2007, n. 123, con l'introduzione dell'art. 25-septies nell'impianto normativo del D. Lgs. n. 231/2001, ha ulteriormente esteso l'ambito applicativo della responsabilità degli enti ai reati di omicidio colposo e lesioni colpose gravi o gravissime che si verificano mediante la violazione delle norme per la prevenzione degli infortuni sul lavoro o relative alla tutela dell'igiene e della salute sul lavoro.

Inoltre, con decreto legislativo 21 novembre 2007, n. 231, il legislatore ha dato attuazione alla direttiva 2005/60/CE del Parlamento e del Consiglio, del 26 ottobre 2005, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (c.d. III Direttiva antiriciclaggio). Ne consegue che l'ente sarà ora punibile per i reati di ricettazione, riciclaggio e impiego di capitali illeciti, anche se compiuti in ambito prettamente “nazionale”, sempre che ne derivi un interesse o vantaggio per l'ente medesimo.

La Legge 18 marzo 2008 n. 48 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001) ha inserito l'art. 24-bis relativo ai delitti informatici e al trattamento illecito di dati.

Il Decreto Legislativo 9 aprile 2008 n. 81 (Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela di salute e sicurezza nei luoghi di lavoro) ha sostituito l'art. 25 septies del Decreto. In particolare le norme puniscono, con una pena aggravata rispetto all'ipotesi ordinaria di omicidio colposo e di lesioni personali colpose, chiunque cagioni per propria colpa rispettivamente la morte o lesioni personali gravi o gravissime, ad altri in conseguenza di un inadempimento agli obblighi di legge vigenti in materia di prevenzione di infortuni sul lavoro.

La Legge 15 luglio 2009, n. 94 recante disposizioni in materia di sicurezza pubblica ha previsto l'inserimento dell'articolo 24-ter riguardante la responsabilità amministrativa degli enti per i delitti di criminalità organizzata.

La Legge 23 luglio 2009, n. 99 recante disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, ha introdotto la lettera f-bis all'articolo 25-bis, introducendo tra i reati presupposto quelli di cui agli articoli 473 e 474 del codice penale (i.e., contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali nonché introduzione nello Stato e commercio di prodotti con segni falsi).

La summenzionata legge, inoltre, introduce l'articolo 25-bis.1, in materia di delitti contro l'industria e il commercio, di cui agli articoli 513 (Turbata libertà dell'industria o del commercio), 515 (Frode nell'esercizio del commercio), 516 (Vendita di sostanze alimentari non genuine come genuine), 517 (Validità di prodotti industriali con segni mendaci), 517-ter (Fabbricazione e commercio di



beni realizzati usurpando titoli di proprietà industriale), 517-quater (Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari), 513 bis (Illecita concorrenza con minaccia o violenza) e 514 (Frodi contro le industrie nazionali) del codice penale. Inoltre, si introduce l'articolo 25-nonies (Delitti in materia di violazione del diritto d'autore), ampliando l'ambito dei reati presupposto ai reati di cui alla legge n. 633 del 1941.

La Legge 3 agosto 2009 n. 116 (Ratifica ed esecuzione della Convenzione delle Nazioni Unite contro la corruzione, adottata dall'assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n.58/4) ha introdotto l'articolo 25-decies relativo al reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, di cui all'articolo 377-bis del codice penale.

1.1.2.2 I soggetti destinatari del Decreto

La legge individua quali soggetti destinatari "gli enti forniti di personalità giuridica, le società fornite di personalità giuridica e le società e le associazioni anche prive di personalità giuridica" (art. 1, co. 2). Il quadro descrittivo non si applica a "lo Stato, gli enti pubblici territoriali nonché gli enti che svolgono funzioni di rilievo costituzionale" (art. 1, co. 3).

Tra i soggetti destinatari del Decreto rientrano pertanto la Banca e le società del Gruppo.

1.1.2.3 Soggetti apicali e soggetti sottoposti

L'ente non avrà alcuna responsabilità se gli autori del reato, siano essi soggetti apicali o sottoposti alla altrui vigilanza, hanno agito nell'interesse esclusivo proprio o di terzi.

Sotto altro profilo invece la norma distingue due differenti ipotesi.

1. Per i reati commessi da soggetti apicali (art. 5 comma 1 lett. a), l'ente è onerato della dimostrazione della c.d. prova liberatoria. Ovverosia rimane sempre responsabile se non prova che:
 - a) 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;
 - b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento e' stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
 - c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
 - d) non vi e' stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

2. Se il reato è commesso da soggetti sottoposti all'altrui direzione (art. 5, comma 1, lettera b), l'ente è responsabile nell'ipotesi in cui la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. Pertanto la prova circa la responsabilità dell'ente graverà sulla pubblica accusa.

L'inosservanza degli obblighi di direzione o vigilanza è esclusa, ai sensi dell'art. 7 comma 2 del Decreto, qualora "l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi".



1.1.2.4 La condizione esimente

L'art. 6 del provvedimento in esame contempla tuttavia una forma di "esonero" da responsabilità dell'ente se si dimostra, in occasione di un procedimento penale per uno dei reati considerati, di aver adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti penali considerati. Il sistema prevede l'istituzione di un organo di controllo interno all'ente con il compito di vigilare sull'efficacia reale del Modello.

Di conseguenza una forma specifica di esonero della responsabilità si ottiene qualora la società dimostri che:

- a) l'Organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di organizzazione, gestione e controllo idoneo a prevenire i reati e gli illeciti della specie di quello verificatosi;
- b) il compito di vigilare sul funzionamento e sull'osservanza del Modello nonché di curare il suo aggiornamento è stato affidato ad un organismo della società dotato di autonomi poteri di iniziativa e controllo;
- c) le persone che hanno commesso i reati e gli illeciti hanno agito eludendo fraudolentemente, quindi in violazione del suddetto Modello;
- d) non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

L'"esonero" dalle responsabilità della società passa attraverso il giudizio d'idoneità e di tenuta preventiva del Modello, che il giudice penale è chiamato a formulare in occasione del procedimento penale a carico dell'autore materiale del reato.

Dunque, la formulazione del Modello e l'organizzazione dell'attività dell'organo di controllo devono porsi come obiettivo l'esito positivo di tale giudizio d'idoneità. Questa particolare prospettiva finalistica impone agli enti di valutare l'adeguatezza delle proprie procedure. Pertanto l'adozione del Modello diviene obbligatoria e risponde ad esigenze di prudenza e buona gestione dell'impresa, laddove si voglia beneficiare dell'esimente.

Allo scopo di offrire un aiuto concreto alle società ed associazioni nella elaborazione dei modelli e nella individuazione di un organo di controllo, le Linee Guida predisposte da ABI contengono una serie di indicazioni e misure ritenute in astratto idonee a rispondere alle esigenze delineate dal D. Lgs. n. 231/2001, e quindi tali da rivestire un importante ruolo ispiratore nella costruzione del Modello e dell'organismo di controllo..

1.2. Adozione del Modello organizzativo da parte della Banca

1.2.1 Struttura del Modello di organizzazione, gestione e controllo

Il presente Modello è costituito da una "Parte Generale" e da una "Parte Speciale" predisposta per le diverse categorie di reato contemplate nel D. Lgs. 231/2001 e considerate a rischio per la Banca e le società del Gruppo.

La Parte Generale ha la funzione di definire i principi di carattere generale, che ciascuna società pone come riferimento per la gestione dei propri affari e che sono, quindi, validi per la realtà bancaria in senso lato e non soltanto per il compimento delle attività rischiose. Illustra inoltre i principali aspetti della normativa, l'approccio metodologico utilizzato dalla Banca per la definizione e l'adozione del Modello, l'individuazione delle attività a rischio reato e le principali caratteristiche / compiti dell'Organismo di Vigilanza.

La Parte Speciale ha la funzione di:



- stabilire le fonti normative interne a cui si devono attenere i Destinatari;
- individuare i principi comportamentali da porre in essere;
- ripercorrere l'approccio metodologico utilizzato per la predisposizione del Modello;
- individuare i singoli reati concretamente e potenzialmente attuabili in Banca e le relative misure preventive;
- definire i compiti dell'Organismo di Vigilanza.

Il presente Modello ,adottato dalla Capogruppo, deve essere personalizzato dalle società del Gruppo in base alle loro peculiarità e successivamente da esse adottato, previa approvazione delle funzioni omologhe della Capogruppo.

1.2.2 Modifiche e integrazioni del Modello

Essendo il presente Modello un "atto di emanazione dell'Organo dirigente" (in conformità alle prescrizioni dell'art. 6, primo comma, lettera a) del decreto legislativo) le successive modifiche e integrazioni di carattere sostanziale del Modello stesso sono rimesse alla competenza del Consiglio di Amministrazione delle società del Gruppo, previo parere favorevole della Capogruppo.

1.3. Metodologia per l'individuazione delle attività sensibili e dei processi di supporto

L'art. 6 comma 2 lett. a) del D.Lgs. 231/01 prescrive l'individuazione delle cosiddette "aree sensibili" o "a rischio", cioè di quei processi e di quelle aree di attività della Banca in cui si potrebbe verificare la commissione di uno dei reati espressamente richiamati dal D.Lgs. 231/01.

E' necessario pertanto, analizzare la realtà operativa di ciascuna società nelle aree/settori in cui risulta apprezzabile il rischio della commissione dei reati previsti dal D.Lgs. 231/01, evidenziando i momenti ed i processi maggiormente rilevanti e parallelamente, condurre un'indagine sugli elementi costitutivi dei reati in questione, allo scopo di identificare le condotte concrete che, nel contesto delle singole società, potrebbero realizzare le fattispecie delittuose.

Tali attività si realizzano attraverso le seguenti fasi:

- Fase di Scoping: definizione dettagliata del perimetro oggetto di valutazione nonché individuazione, attraverso interviste rivolte ai soggetti apicali, dei corretti processi bancari e dei relativi referenti.
- Fase di Analisi: valutazione del sistema di controllo interno in essere, raccolta, mediante interviste ed analisi documentale, delle informazioni necessarie a costruire la mappa delle principali attività a rischio reato, l'elenco delle possibili modalità di realizzazione dei comportamenti configurati come reati e per i quali sia prevista una responsabilità della Banca ai sensi del Decreto Legislativo, l'analisi e valutazione dei punti di debolezza individuati e la determinazione dei possibili rimedi.

Tale metodologia deve essere applicata nel continuo.

1.4. Individuazione delle attività a rischio reato

Identificazione delle aree, delle attività e dei Processi Sensibili (c.d. "as-is analysis")

Al fine di individuare i settori di attività astrattamente idonei a suscitare comportamenti riconducibili ai Reati è stato analizzato il contesto aziendale della Banca, in base alla metodologia descritta nel paragrafo precedente, ottenendo una rappresentazione (cosiddetta "mappatura") dei



Processi Sensibili, delle aree/funzioni critiche per il rischio di commissione di Reati, del sistema dei controlli esistenti e dei relativi aspetti migliorabili.

Comparazione della situazione attuale rispetto al modello a tendere (c.d. “gap analysis”)

Sulla base della rilevazione della situazione esistente nella Banca in relazione alle singole area/attività “sensibili”, alle aree/funzioni aziendali coinvolte ed ai controlli e procedure esistenti circa i Processi Sensibili, è stata effettuata un’analisi comparativa con il modello “a tendere” evincibile in generale dal Decreto, necessaria a valutare:

- a) l’adeguatezza dei protocolli esistenti, ossia la loro attitudine a prevenire comportamenti illeciti (o comunque a ridurre il rischio ad un livello accettabile) e ad evidenziarne l’eventuale commissione;
- b) l’effettività dei protocolli esistenti, ossia l’idoneità degli stessi a ricomprendere e disciplinare tutti i comportamenti potenzialmente illeciti, previsti dal Decreto.

In particolare, tutti i Processi Sensibili devono rispettare i seguenti principi generali:

- separazione dei compiti attraverso una corretta distribuzione delle responsabilità e la previsione di adeguati livelli autorizzativi, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto;
- chiara e formalizzata assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell’ambito della struttura organizzativa;
- esistenza di regole comportamentali idonee a garantire l’esercizio delle attività aziendali nel rispetto delle leggi e dei regolamenti e dell’integrità del patrimonio aziendale;
- “proceduralizzazione” delle attività aziendali “a rischio reato”, al fine di:
 - definire e regolamentare le modalità e tempistiche di svolgimento delle attività medesime;
 - garantire la tracciabilità degli atti, delle operazioni e delle transazioni attraverso adeguati supporti documentali che attestino le caratteristiche e le motivazioni dell’operazione ed individuino i soggetti a vario titolo coinvolti nell’operazione (autorizzazione, effettuazione, registrazione, verifica dell’operazione);
 - garantire, ove necessario, l’“oggettivazione” dei processi decisionali e limitare decisioni aziendali basate su scelte soggettive non legate a predefiniti criteri oggettivi (es.: esistenza di albi fornitori, esistenza di criteri oggettivi di valutazione e selezione del personale, ecc.);
- esistenza e documentazione di attività di controllo e supervisione, compiute sulle transazioni aziendali; esistenza di meccanismi di sicurezza che garantiscano un’adeguata protezione/accesso fisico-logico ai dati e ai beni aziendali.

Le aree di rischio sono state raffrontate con il sistema dei presidi/controlli esistenti presso la Banca, per evidenziare eventuali disallineamenti rispetto al modello a tendere e fornire suggerimenti utili a porvi rimedio.

Più in dettaglio, per ogni area sensibile (processo) sono stati definiti i seguenti elementi:

1. i rischi associati;
2. le strutture organizzative coinvolte nel processo;
3. il sistema dei presidi e controlli (protocolli) esistente;
4. gli eventuali ulteriori presidi (protocolli) ritenuti utili per il rafforzamento dei controlli.



In esito alla fase di indagine e ricognizione delle aree di attività a rischio di commissione di Reati, sono stati individuati i Processi Sensibili della Banca con riguardo alle seguenti categorie di reato:

- a) reati contro la P.A.;
- b) reati societari;
- c) reati di abuso di informazione privilegiata e manipolazione del mercato;
- d) reati relativi all'antiriciclaggio e terrorismo;
- e) reati contro la salute e sicurezza sul lavoro;
- f) reati relativi ai delitti informatici ed al trattamento illecito dei dati.

L'analisi è stata condotta:

- quanto ai reati nei rapporti con P.A., sulle attività che prevedono rapporti, contatti e/o interazioni tra soggetti esponenziali della Banca e soggetti esterni qualificabili come "pubblici ufficiali" o "incaricati di pubblico servizio" e sulle attività per le quali tali risorse operano in qualità di "incaricati di pubblico servizio" nei rapporti con terzi;
- quanto ai reati societari, di abuso di informazioni privilegiate e manipolazione del mercato, sulle attività sociali che possono avere una qualche rilevanza per la commissione dei reati di cui all'art. 25-ter e sexies del Decreto;
- quanto ai reati di antiriciclaggio e terrorismo, sulle attività che prevedono rapporti, contatti e/o interazioni con l'esterno che possono fornire, direttamente o indirettamente, ma comunque volontariamente, fondi a favore di soggetti che intendano porre in essere reati di terrorismo; in tale ambito sicuramente assumono una rilevanza centrale i settori finanziario ed amministrativo;
- quanto ai reati relativi alla salute e sicurezza sul lavoro, sulle attività che evidenziano un maggior rischio di possibili incidenti o lesioni a danno di dipendenti o terzi;
- quanto ai reati relativi ai delitti informatici ed al trattamento illecito dei dati, sulle attività che possono avere una qualche rilevanza per la commissione dei reati di cui all'art. 24 bis del Decreto.

Non è stato invece ritenuto particolarmente significativo, al momento, il rischio relativo ad altre categorie di Reato, pur ritenendo la Banca tutte le aree di rischio meritevoli di idonei presidi.

I risultati di quanto sopra hanno consentito la mappatura dei rischi descritta nella Parte Speciale del documento.

Il modello organizzativo esposto nella Parte Speciale evidenzia dunque, per ciascun processo, i protocolli ritenuti utili ai fini del Decreto.

1.5. Destinatari del modello

Destinatari del presente Modello sono i soggetti in posizione apicale, quali Amministratori o soggetti con funzione di direzione dell'intera Banca, i soggetti che di fatto gestiscono o controllano la Banca e le persone sottoposte alla direzione o al controllo dei soggetti in posizione apicale (dipendenti o collaboratori), così come individuati dall'art. 5, comma 1, del D. Lgs. n. 231/01.

Le disposizioni del presente Modello si applicano anche a tutti gli altri dipendenti, collaboratori, fornitori e consulenti esterni che agiscono in nome e per conto o nell'interesse della Banca,



nonché ai dipendenti, collaboratori, fornitori e consulenti esterni delle società del Gruppo Cassa di Risparmio.

Tutti i soggetti identificati nel presente paragrafo sono di seguito denominati “i Destinatari”.

1.6. Organismo di Vigilanza

Affinché ciascuna società possa usufruire dell’esonero dalla responsabilità, il D.Lgs. 231/01 (art. 6) prevede che l’Organo dirigente abbia, tra l’altro:

- adottato un Modello di organizzazione, gestione e controllo idoneo a prevenire il compimento dei c.d. “reati presupposto” (il Modello della Banca già adottato con delibera del 11 novembre 2003 è stato aggiornato nel continuo e formalizzato nel presente documento, adottato con delibera del 22 settembre 2009);
- affidato il compito di vigilare sul funzionamento e l’osservanza del Modello e di curarne l’aggiornamento ad un organismo dell’ente dotato di autonomi poteri di iniziativa e controllo (di seguito l’Organismo di Vigilanza o OdV). La Banca ha ridefinito la composizione in data 22 settembre 2009.

L’affidamento di detti compiti all’OdV ed il corretto, continuo ed efficace svolgimento degli stessi sono presupposti indispensabili per l’esonero dalla responsabilità, sia che il reato sia stato commesso dai soggetti “apicali” (espressamente contemplati dall’art. 6), che dai soggetti sottoposti all’altrui direzione (di cui all’art. 7).

L’art. 7, co. 4, ribadisce, infine, che l’efficace attuazione del Modello richiede, oltre all’istituzione di un sistema disciplinare, una sua verifica periodica da parte dell’organismo a ciò deputato.

Il massimo vertice societario (es. Consiglio di Amministrazione o Amministratore Delegato), pur con l’istituzione dell’Organismo ex D. Lgs. n. 231/2001, mantiene invariate tutte le attribuzioni e le responsabilità previste dal Codice Civile, alle quali si aggiunge oggi quella relativa all’adozione ed all’efficacia del Modello, nonché all’istituzione dell’Organismo (art. 6, co. 1, lett. a) e b)).

1.6.1 Composizione, nomina e revoca dell’Organismo di vigilanza

L’Organismo di vigilanza è definito a livello di Gruppo ed è composto da tre membri, di cui almeno uno esterno. Gli eventuali membri scelti tra gli Amministratori devono possedere i requisiti di indipendenza.

I componenti dell’Organismo di vigilanza sono nominati dal Consiglio di Amministrazione della banca, sentito il Collegio sindacale.

All’atto della nomina dei membri dell’Organismo di vigilanza, il Consiglio di Amministrazione della banca, sentito il Collegio Sindacale, fissa il compenso spettante al Presidente ed agli altri membri per l’espletamento dei propri compiti, nonché il budget assegnato all’Organismo di Vigilanza per eventuali consulenze esterne, formazione dei membri dell’OdV stesso ed eventuale struttura a supporto.

La durata dell’incarico dei membri dell’Organismo di vigilanza è di regola di tre esercizi sociali, in corrispondenza della durata del CdA e la scadenza è fissata dopo l’approvazione da parte dell’Assemblea del bilancio relativo al terzo esercizio. I membri dell’Organismo di vigilanza sono rieleggibili e l’incarico di ciascun membro non può essere rinnovato per più di due volte.

Nella dichiarazione formale di incarico devono essere obbligatoriamente indicati:



- il soggetto / i soggetti chiamato/i ad assumere il ruolo di OdV e le relative responsabilità;
- la durata in carica, se è previsto un termine, e in ogni caso le modalità di revoca dell'incarico;
- i principali compiti cui l'OdV è chiamato nell'ambito dell'espletamento delle attività di controllo sull'efficienza ed efficacia del Modello di organizzazione, gestione e controllo (l'indicazione della modalità operative è rimessa all'Organismo stesso tramite l'adozione di un regolamento interno delle proprie attività – pianificazione dei controlli, individuazione dei criteri e delle procedure di analisi, disciplina dei flussi informativi, etc.);
- i poteri di cui l'Organismo deve necessariamente essere dotato per assicurare una puntuale ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello;
- le tempistiche e gli organi destinatari dell'attività di reporting dell'Organismo di Vigilanza.

L'Organismo di Vigilanza si riunisce di massima in via ordinaria ogni semestre o in qualsiasi momento su convocazione del Presidente nei casi di accertamento di violazioni del Modello 231/2001.

Per la validità delle sedute dell'Organismo di Vigilanza è necessaria la presenza della maggioranza dei suoi membri in carica. Delle attività svolte nelle predette sedute viene redatto apposito verbale.

I membri dell'Organismo di vigilanza devono possedere conoscenze specialistiche in merito alla valutazione ed alla gestione dei rischi nonché conoscenze organizzative, di revisione e giuridico-penalistiche. Oltre alle competenze professionali, i componenti dell'Organismo di vigilanza devono possedere, inoltre, i requisiti di onorabilità e di indipendenza previsti per gli Esponenti della banca. Pertanto, l'Organismo di vigilanza deve:

- garantire l'autonomia dell'iniziativa di controllo da interferenze e/o condizionamenti da parte di altri Organi. L'Organismo di vigilanza non è titolare di compiti operativi e riporta direttamente al Consiglio di Amministrazione;
- garantire l'efficace attuazione del modello organizzativo, del modello gestionale e del modello di controllo predisposti dalla banca, anche su proposta dell'Organismo stesso, al fine di prevenire la commissione dei reati previsti nel d. lgs. 231/2001. A tale riguardo, all'Organismo di vigilanza vengono attribuiti poteri in materia di spese per adeguare le risorse necessarie per lo svolgimento del ruolo assegnato al medesimo Organismo che può avvalersi di consulenti esterni.

La revoca dell'Organismo di vigilanza è ammessa solo nei seguenti casi:

- per giusta causa, in caso di negligenza, inefficienza o infedeltà dei membri dell'Organismo di vigilanza (mancata presentazione, senza giustificato motivo, al Consiglio di Amministrazione delle relazioni dell'Organismo di vigilanza; assenza non giustificata a più di due riunioni, anche non consecutive, dell'Organismo di vigilanza; mancata esecuzione del piano di formazione o del piano di controllo interno; rivelazione di informazioni riservate all'esterno della banca, senza che sussista un giustificato motivo);
- al verificarsi di eventi che facciano venire meno i requisiti di professionalità, onorabilità ed indipendenza previsti dalle disposizioni di legge e di vigilanza per gli Esponenti della banca.

La delibera di revoca dell'Organismo di vigilanza da parte del Consiglio di Amministrazione della Società deve essere espressamente approvata dal Collegio Sindacale e deve contenere adeguata motivazione delle cause di revoca.

Qualora, nel corso dell'incarico, dovesse sopraggiungere una causa di decadenza da riconnettere ai requisiti di professionalità, onorabilità ed indipendenza, il membro interessato è tenuto ad informare immediatamente gli altri componenti dell'Organismo di vigilanza ed il Consiglio di Amministrazione.

Altre cause di cessazione dall'incarico sono:



- la rinuncia da parte del membro dell'Organismo di vigilanza, mediante comunicazione scritta e motivata al Consiglio di Amministrazione, da inviarsi almeno un mese prima della data in cui la rinuncia avrà effetto;
- la morte o la sopravvenuta incapacità mentale o fisica o impossibilità ad esercitare l'incarico;
- la cessazione, per qualsiasi ragione o causa, dalla carica di Consigliere di Amministrazione della banca.

Il Presidente dell'Organismo di vigilanza, o un altro componente nel caso di cessazione del Presidente, dovrà comunicare senza indugio al Consiglio di Amministrazione il verificarsi di una delle predette cause dalle quali derivi la necessità di sostituire un membro dell'Organismo di vigilanza ed il Consiglio di Amministrazione dovrà provvedere tempestivamente alla sostituzione del membro cessato.

1.7. Ruolo dell'Organismo di vigilanza

Il ruolo dell'Organismo di vigilanza è volto a:

1. promuovere le iniziative, ivi inclusi i corsi di formazione e le comunicazioni, dirette a favorire un'adeguata conoscenza dei regolamenti nonché la diffusione degli stessi alla struttura organizzativa della banca;
2. verificare la conformità normativa ed operativa dei controlli svolti dalle funzioni aziendali sui processi di competenza delle stesse funzioni per la prevenzione dei reati. Tale verifica può essere effettuata dall'Organismo di vigilanza direttamente e/o sulla base delle informazioni fornite dalla Revisione Interna e/o dalla funzione di compliance;
3. valutare le segnalazioni a lui pervenute con riferimento a possibili reati previsti nel D. Lgs. 231/2001 e violazioni del codice etico;
4. esaminare le carenze significative che ostacolano la prevenzione dei reati segnalate dal Responsabile della Revisione Interna, dai responsabili della funzione di compliance o direttamente dai responsabili dei processi relativi alla prevenzione dei reati o in generale da qualsiasi dipendente. In tale contesto, l'Organismo di vigilanza deve:
 - garantire la riservatezza dell'identità dei soggetti segnalanti allo scopo di tutelare gli stessi da eventuali ritorsioni e/o discriminazioni di qualsiasi genere o natura;
 - tenere traccia delle segnalazioni di cui sopra, nonché documenti di compendio dei controlli svolti, corredati degli eventuali rilievi e dalle risposte dei responsabili dei processi aziendali coinvolti;
5. informare gli Organi aziendali in merito ai risultati delle predette verifiche e/o alle segnalazioni di carenze pervenute dalle funzioni aziendali, unitamente agli interventi da assumere dai medesimi Organi per adeguare il modello organizzativo, il modello gestionale ed il modello di controllo all'evoluzione delle disposizioni di legge e di vigilanza e/o per eliminare le carenze e le disfunzioni emerse dalla verifica di cui al precedente punto;
6. verificare e valutare l'idoneità del sistema disciplinare, ai sensi e per gli effetti del D. Lgs. 231/2001 in collaborazione con il Direttore Generale ed il Responsabile del Personale.



1.8. Coordinamento dell'Organismo di vigilanza con altri Organi e funzioni aziendali

L'Organismo di Vigilanza svolge il predetto ruolo coordinandosi con gli altri Organi o funzioni di controllo della banca. In particolare:

- si coordina con la funzione deputata alla gestione delle risorse umane per gli aspetti relativi alla formazione del Personale, all'adozione dei provvedimenti disciplinari in vigore ed all'elaborazione delle clausole contrattuali che regolano l'applicazione del modello 231/2001 ai destinatari;
- si coordina con le funzioni previste dal Regolamento del processo organizzativo e di compliance per la prevenzione dei reati per l'adeguamento degli stessi processi alle disposizioni di legge e di vigilanza nonché per eliminare eventuali carenze e/o disfunzioni che ostacolano la predetta prevenzione.

1.9. Poteri dell'Organismo di vigilanza

L'Organismo di vigilanza gode di ampi poteri ispettivi e di accesso ai documenti aziendali nonché dispone di risorse finanziarie, che vengono stanziare annualmente a suo favore dal Consiglio di Amministrazione e modificate anche dietro sua proposta.

Inoltre l'Organismo di vigilanza si avvale del supporto e della collaborazione delle varie strutture aziendali, che possano essere interessate o comunque coinvolte nelle attività di controllo nonché può avvalersi della consulenza di terzi, dotati delle competenze necessarie. Pertanto, l'Organismo di Vigilanza, ha facoltà di:

- effettuare tutte le verifiche e le ispezioni ritenute opportune ai fini del corretto espletamento dei propri compiti;
- libero accesso presso tutte le funzioni, gli archivi ed i documenti della banca, senza alcun consenso preventivo o necessità di autorizzazione, al fine di ottenere ogni informazione, dato o documento ritenuto necessario;
- disporre, ove occorra, l'audizione dei soggetti aziendali che possano fornire indicazioni o informazioni utili in merito allo svolgimento dell'attività aziendale o ad eventuali disfunzioni o violazioni del modello 231;
- avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di tutte le funzioni della banca ovvero di consulenti esterni;
- disporre, per ogni esigenza necessaria al corretto svolgimento dei suoi compiti, delle risorse finanziarie stanziare dal Consiglio di Amministrazione.

1.10. Flussi informativi delle singole funzioni diretti all'Organismo di vigilanza

L'Organismo di Vigilanza deve essere tempestivamente informato, tramite la Revisione Interna, dai responsabili dei singoli processi per la prevenzione dei reati o dai responsabili delle complessive funzioni di controllo o, in generale, da qualsiasi dipendente di ogni informazione, di qualsiasi tipo, derivante da risultati di propri accertamenti e/o segnalazioni ricevute attinente al mancato svolgimento e/o alla violazione dei processi stessi che costituiscono il modello organizzativo, il modello gestionale, il modello di controllo, del codice etico e del codice di comportamento. In particolare, devono essere obbligatoriamente e immediatamente segnalate al responsabile della Revisione Interna che provvede all'invio all'Organismo di vigilanza:



1. le violazioni o la commissione di Reati, quali, a titolo esemplificativo ma non esaustivo:
 - le richieste di assistenza legale inoltrate dai dipendenti nei confronti dei quali la Magistratura o altra Autorità procede per i reati di cui al Decreto;
 - i provvedimenti e/o le notizie comunicati alla banca e provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità dai quali si evinca lo svolgimento di indagini che interessano, anche indirettamente, la banca stessa e/o i suoi dipendenti;
 - le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per i reati;
 - le notizie relative ai procedimenti disciplinari in corso e alle eventuali sanzioni irrogate ovvero la motivazione della loro archiviazione, relative ai reati;
 - eventuali ordini ricevuti dal superiore e ritenuti in contrasto con la legge, la normativa interna, o il modello 231;
 - eventuali richieste od offerte di doni (eccedenti il valore modico) o di altre utilità provenienti da pubblici ufficiali o incaricati di pubblico servizio
 - eventuali scostamenti significativi fra costi sostenuti e relativo budget aziendale o anomalie di spesa e cioè di costo non connesso, in genere, alla specifica attività aziendale;
 - eventuali omissioni, trascuratezze o falsificazioni nella tenuta della contabilità o nella conservazione della documentazione su cui si fondano le registrazioni contabili;

2. le informazioni relative all'attività della banca che possono assumere rilevanza quanto all'espletamento da parte dell'Organismo di vigilanza dei compiti ad esso assegnati, incluse, senza che ciò costituisca limitazione:
 - le notizie relative ai cambiamenti organizzativi;
 - gli aggiornamenti del sistema dei poteri e delle deleghe;
 - le eventuali comunicazioni della società di revisione riguardanti aspetti che possono indicare una carenza dei controlli interni;
 - le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
 - ogni informazione propedeutica alle proposte di modifica del modello 231.

L'Organismo di vigilanza, nel corso dell'attività di indagine che segua alle segnalazioni, agirà in modo da garantire che i soggetti coinvolti non siano oggetto di ritorsioni, discriminazioni o, comunque, penalizzazioni, assicurando, quindi, la riservatezza del soggetto che effettua la segnalazione e della normativa sulla tutela dei dati personali, fatti salvi la ricorrenza di eventuali obblighi di legge che impongano diversamente e la tutela dei diritti della banca.

I membri dell'Organismo di vigilanza non potranno riferire in alcun caso al di fuori della banca, salvo gli obblighi di legge, quanto appreso nell'esercizio delle proprie funzioni.

Nel caso in cui le segnalazioni abbiano ad oggetto l'operato dell'Organismo di vigilanza, la stessa dovrà essere inviata al Presidente del Collegio Sindacale ed al Presidente del Consiglio di Amministrazione.

L'Organismo di vigilanza, in presenza di una segnalazione effettua le necessarie indagini, utilizzando gli ampi poteri di cui dispone, per appurare la fondatezza e la veridicità delle segnalazioni ricevute. Nel caso di segnalazione di una possibile violazione, verifica l'esistenza di prove o di presunzioni chiare, precise e concordanti.

Nel caso in cui l'Organismo di vigilanza ritenga non fondata la segnalazione, la stessa verrà archiviata. Nel caso di segnalazioni false, improprie o caluniose, l'Organismo di vigilanza provvederà ad informare le funzioni aziendali competenti per l'irrogazione delle sanzioni previste nel sistema disciplinare.



Nel caso di accertamento della commissione di una Violazione, l'Organismo di vigilanza dovrà individuare i provvedimenti da adottare, sulla base del sistema disciplinare.

A tal fine, l'Organismo di vigilanza, non potendo irrogare direttamente le sanzioni, si coordinerà con la funzione aziendale e/o con l'Organo Sociale competente affinché siano irrogate le relative sanzioni.

L'Organismo di vigilanza provvede alla raccolta delle segnalazioni ricevute, dei report inviati e delle risultanze dell'attività di indagine e di verifica svolta in un apposito archivio. Di tale archivio cura l'aggiornamento e definisce, con propria disposizione, i criteri, le modalità di accesso ed i soggetti legittimati ad accedervi.

1.11. Flussi informativi dell'Organismo di Vigilanza diretti agli Organi aziendali

L'Organismo di vigilanza riferisce periodicamente agli Organi Sociali in merito all'attuazione del Modello 231/2001 ed alle risultanze della propria attività di verifica e controllo svolto. In particolare, l'Organismo di vigilanza:

1. si coordina su base continuativa con il Consiglio di Amministrazione. Al riguardo, il Presidente dell'Organismo di vigilanza può, a sua volta, presentare richiesta di audizione agli Organi Sociali, per riferire in merito al modello 231 o a tematiche connesse con lo stesso.
2. relaziona per iscritto, con cadenza almeno semestrale, al Consiglio di Amministrazione ed al Collegio Sindacale sull'attività compiuta. A tal fine fornisce ai predetti Organi una relazione contenente una sintesi delle attività svolte nei precedenti sei mesi, dei controlli e delle verifiche eseguite, nonché le eventuali proposte di aggiornamento del modello 231;
3. riferisce tempestivamente al Consiglio di Amministrazione nel caso di violazioni gravi commesse dai responsabili dei processi. In particolare, in caso di violazione grave commessa da un membro del Consiglio di Amministrazione, l'Organismo di vigilanza riferirà al Consiglio e al Collegio Sindacale. Nel caso di violazione commessa da un membro del Collegio Sindacale, l'Organismo di vigilanza riferirà al Collegio Sindacale ed al Consiglio di Amministrazione. In entrambi i casi l'Organismo di vigilanza proporrà le sanzioni che riterrà più adeguate per le violazioni.

In ogni caso, l'Organismo di vigilanza fornirà al Consiglio di Amministrazione qualsiasi informazione ritenuta utile ai fini dell'assunzione di determinazioni urgenti da parte degli Organi deputati.

1.12. Responsabilità dell'Organismo di Vigilanza

L'Organismo di vigilanza è responsabile:

1. del proprio processo di verifica dei predetti modelli e dei relativi processi. Il processo di verifica di pertinenza dell'Organismo di vigilanza, articolato in fasi, deve essere svolto secondo quanto disciplinato nel Regolamento dell'Organismo di Vigilanza in termini di criteri da seguire ed attività da svolgere nei singoli aspetti delle fasi del processo stesso;
2. della verifica dell'attuazione della proposta di modifica al modello organizzativo, del modello gestionale e del modello di controllo e dei relativi processi. Al riguardo, la predisposizione dei predetti modelli deve essere effettuata secondo quanto previsto nel regolamento del processo organizzativo e di conformità deliberato dal Consiglio di Amministrazione.



1.13. La formazione delle risorse e la diffusione del Modello

1.13.1 Formazione ed informazione dei Dipendenti

Ai fini dell'attuazione del presente Modello, ciascuna società del Gruppo garantisce una corretta conoscenza delle regole di condotta ivi contenute, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nei processi sensibili.

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'Organismo di Vigilanza in collaborazione con il responsabile della Funzione Risorse Umane e con i responsabili delle altre funzioni di volta in volta coinvolte nell'applicazione dei processi.

- *La comunicazione iniziale*

L'adozione del presente Modello è comunicata a tutte le risorse presenti in Banca al momento dell'adozione stessa, tramite i canali informativi adottati dal Gruppo. Tutte le modifiche intervenute successivamente e le informazioni concernenti il Modello verranno comunicate attraverso i medesimi canali informativi.

Ai nuovi assunti, invece, viene consegnato un set informativo comprendente tra gli altri il Codice Etico, il codice di comportamento ed il Modello 231/2001, con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza.

- *La formazione*

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D. Lgs. 231/2001 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della società.

In particolare, la Banca prevede livelli diversi di informazione e formazione.

1.13.2 Consulenti, collaboratori e fornitori

Ai soggetti esterni alla Banca (consulenti, collaboratori e fornitori) devono essere fornite apposite informative sulle politiche e le procedure adottate dal Gruppo sulla base del presente Modello, nonché i testi delle clausole contrattuali abitualmente utilizzate al riguardo.

I soggetti esterni devono essere informati del contenuto del Modello e dell'esigenza della Banca che il loro comportamento sia conforme ai disposti del D.Lgs. 231/2001.

Nei confronti di terze parti contraenti (es.: collaboratori, consulenti, agenti, fornitori, ecc.) che operano con la Pubblica Amministrazione o coinvolte nello svolgimento di attività a rischio reato per conto o nell'interesse della Banca, i relativi contratti devono:

- essere definiti per iscritto, in tutte le loro condizioni e termini;
- contenere clausole standard al fine del rispetto del D.Lgs. 231/2001;
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D.Lgs. 231/2001 e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse, penali).

1.14. Sistema disciplinare

La predisposizione di un efficace sistema sanzionatorio costituisce, ai sensi dell'art. 6 primo comma lettera e) del D.Lgs. 231/2001, un requisito essenziale del Modello ai fini dell'esimente rispetto alla responsabilità della società.

I comportamenti dei dipendenti non conformi ai principi e alle regole di condotta prescritti nel presente Modello - ivi ricomprendendo il Codice Etico, il Codice di comportamento e le disposizioni interne, che fanno parte integrante del Modello - costituiscono illecito contrattuale.

I comportamenti dei soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, gli agenti, i fornitori, i partner commerciali, ecc.) non conformi ai principi e alle regole di condotta prescritti nel presente Modello, nel Codice etico e nel Codice di comportamento, costituiscono illecito contrattuale e motivo per la risoluzione anticipata del rapporto.

La verifica dell'adeguatezza del sistema sanzionatorio, il costante monitoraggio dei procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché degli interventi nei confronti dei soggetti esterni sono affidati all'Organismo di Vigilanza, il quale procede anche alla segnalazione delle infrazioni di cui venisse a conoscenza nello svolgimento delle funzioni che gli sono proprie.

La Capogruppo ha adottato un Regolamento del Sistema disciplinare parte integrante del presente modello, volto a definire le sanzioni da applicare ad ogni violazione di norme di legge, disposizioni interne e regole comportamentali.

1.15. Aggiornamento ed adeguamento del Modello

Il presente Modello è soggetto a due tipi di verifiche:

- verifiche sugli atti: annualmente si procede a una verifica dei principali atti societari e dei contratti di maggior rilevanza conclusi dalla società in aree di attività a rischio;
- verifiche delle procedure: periodicamente viene verificato l'effettivo funzionamento del presente Modello con le modalità stabilite dal OdV.

La Funzione di Revisione interna, di concerto con l'OdV, pone in essere un controllo annuale tramite interviste dirette ai responsabili delle funzioni a rischio reato, al fine di accertare l'effettiva applicazione delle disposizioni contenute nel presente documento, oltre a verificarne l'efficacia nella propria attività di controllo.

Inoltre, viene intrapresa da parte dell'Organismo di Vigilanza una review di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dal OdV stesso e dagli altri soggetti interessati, degli eventi considerati rischiosi, della consapevolezza del personale rispetto alle ipotesi di reato previste dal Decreto, con interviste a campione.

Come esito delle verifiche, viene stipulato un rapporto da sottoporre all'attenzione dell' Organo Dirigente della Banca (in concomitanza con il rapporto annuale predisposto dall'OdV) che evidenzia le possibili manchevolezze e suggerisca le azioni da intraprendere.

2. Parte Speciale

2.1. Norme emanate ai fini del D.Lgs. 231/01

La presente Parte Speciale fornisce ai Destinatari come definiti nella Parte Generale, le indicazioni affinché vengano adottate regole di comportamento conformi a quanto prescritto nel Decreto Legislativo 231/01, al fine di prevenire il verificarsi dei reati ivi considerati, e di qualunque comportamento illecito.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare le disposizioni interne che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza, e ai responsabili delle funzioni aziendali che cooperano con lo stesso, le indicazioni per esercitare le attività di controllo, monitoraggio e verifica necessarie.

2.1.1 Fonti normative

I Destinatari, nello svolgimento delle rispettive attività, si attengono:

- a) alle disposizioni legislative e regolamentari, italiane o straniere, applicabili alla fattispecie;
- b) alle deliberazioni del Consiglio di Amministrazione
- c) alle previsioni dello Statuto sociale;
- d) al Codice etico
- e) al Codice di comportamento;
- f) al presente Modello.
- g) alle disposizioni interne emanate dalle unità organizzative competenti.

2.1.2 Principi generali di comportamento

Tutti i Destinatari si astengono dal:

- a) porre in essere comportamenti tali da integrare, favorire o istigare qualunque comportamento delittuoso, con particolare riguardo ai reati considerati dal D.Lgs. 231/01;
- b) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato, in particolare rientranti tra quelle sopra considerate, possano potenzialmente porre in essere qualsiasi situazione di conflitto di interessi nei confronti della P.A. o di ogni altra autorità pubblica in relazione a quanto previsto dalle differenti ipotesi di reato.

2.2. Approccio metodologico

Il processo che ha consentito di pervenire ad una mappa documentata delle potenziali modalità attuative degli illeciti di cui al D. Lgs. 231/01 e dei relativi presidi di controllo, al fine della valutazione del rischio potenziale di compimento di "reati rilevanti", della corretta progettazione delle misure preventive e della valutazione del rischio residuo, che deve presentare un livello accettabile, è descritta nella Parte Generale.



Tale metodologia è stata applicata per la valutazione dei rischi relativamente alle aree di attività a rischio reato che fanno capo alla Capogruppo.

Il lavoro è iniziato con l'analisi della struttura organizzativa della Capogruppo acquisendo la seguente documentazione:

- Poteri e procure;
- Disposizioni interne ed organigramma.

Per ognuna delle aree di attività a rischio reato si è provveduto ad identificare gli ambiti di rischio e le conseguenti attività in cui si estrinseca ciascun processo aziendale.

La fase di analisi è stata sviluppata attraverso l'esecuzione di interviste svolte con i responsabili dei processi ed eventuali referenti individuati per ciascuna area di attività a rischio e/o ambito del rischio.

Le interviste hanno permesso di:

- approfondire gli ambiti in cui i reati previsti dal D.Lgs.231/01 possono essere commessi considerando le attività di controllo e di monitoraggio svolte;
- approfondire la struttura del sistema delle deleghe, individuando in maniera appropriata in particolare i poteri di firma e di spesa, in modo da valutare il livello di autonomia e responsabilità di ciascuno nonché il grado di supervisione e le correlate attività di rendicontazione;
- individuare i rapporti di coordinamento con altre funzioni e le relative responsabilità;
- indagare l'esistenza di eventuali prassi operative di fatto seguite ma non formalizzate e richiedere la formalizzazione di tali regole;
- dare una valutazione sull'idoneità delle procedure operative a presidiare l'insorgere dei rischi di compimento di "reati rilevanti";
- dare una valutazione sull'idoneità del flusso informativo e del sistema di archiviazione e tracciabilità della documentazione.

Per quanto attiene la partecipazione dei collaboratori e consulenti, ai fini della mappatura delle attività a rischio, la responsabilità delle stesse è ascritta ai responsabili delle strutture organizzative deputate al coordinamento e controllo dei processi. L'efficacia nel tempo del Modello 231 è così svincolata dalla variabilità delle prestazioni dei collaboratori / consulenti.

2.3. I potenziali reati

Reati commessi nei rapporti con la pubblica amministrazione ex art. 24, d.lgs. 231/01:

- Malversazione a danno dello Stato o di altro ente pubblico (art. 316 bis c.p.);
- Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico o delle Comunità Europee (art. 316 ter c.p.);
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità Europee (art. 640 comma 2 n. 1 c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.);

Reati introdotti dalla legge n. °48 del 18 Marzo 2008 (art. 24 bis d.lgs. 231/01):

- Falsità in un documento informatico pubblico o privato (art. 491-bis c.p.);



- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quarter);
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quarter c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- Truffa del certificatore di firma elettronica (art. 640-quinquies c.p.).

Delitti di criminalità organizzata ex art. 24-ter d. lgs. 231/01

- Associazione per delinquere dirette a commettere delitti di riduzione o mantenimento in schiavitù o in servitù, tratta di persone o acquisto e alienazione di schiavi (art. 416 c.p.)
- Associazioni per delinquere (art. 416 c.p.)
- Associazioni di tipo mafioso anche straniere e delitti commessi avvalendosi delle condizioni previste dall'art. 416-bis o al fine di agevolare l'attività delle associazioni previste dallo stesso articolo (art. 416 c.p.)
- Scambio elettorale politico – mafioso (art. 416 ter c.p.)
- Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.)
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope;
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo.

Reati commessi nei rapporti con la pubblica amministrazione ex art. 25 d.lgs. 231/01:

- Corruzione per un atto d'ufficio (art. 318 c.p.);
- Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.);
- Pene per il corruttore (art. 321 c.p.);
- Circostanze aggravanti (art. 319 bis c.p.);
- Corruzione in atti giudiziari (art. 319 ter c.p.);
- Istigazione alla corruzione (art. 322 c.p.);
- Concussione (art. 317 c.p.);
- Corruzione di persona incaricata di pubblico servizio (art. 320 c.p.);
- Peculato, concussione, corruzione e istigazione alla corruzione di membri degli Organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.).

Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (25-bis d.lgs. 231/01)

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.)



- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.)
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

Delitti contro l'industria e il commercio (art.25-bis.1)

- Turbata libertà dell'industria o del commercio (art. 513 c.p.)
- Frode nell'esercizio del commercio (art. 515 c.p.)
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)
- Illecita concorrenza con minaccia o violenza (art. 513 bis c.p.)
- Frodi contro le industrie nazionali (art. 514 c.p.)
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà intellettuale (art. 517 ter c.p.)
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 quater c.p.)

Reati societari (art. 25-ter d.lgs. 231/01):

- False comunicazioni sociali (art. 2621 c.c.);
- False comunicazioni sociali in danno delle società, dei soci o dei creditori (art. 2622 c.c.);
- Falsità nelle relazioni o nelle comunicazioni delle società di revisione (art. 2624 comma 1 e 2 c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Indebita restituzione dei conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Falso in prospetto (art. 173 bis D. Lgs. 58/1998 TUF)
- Impedito controllo (art. 2625 c.c.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
- Omessa comunicazione del conflitto di interesse (art. 2629 c.c.)
- Ostacolo all'esercizio delle autorità pubbliche di vigilanza (art. 2638 c.c.)

Delitti con finalità di terrorismo o di eversione dall'ordine democratico (art. 25-quater d.lgs. 231/01)

- associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.).
- arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.).
- addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies c.p.)
- attentato per finalità terroristiche o di eversione (art. 280 c.p.).
- atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis c.p.).
- sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.).
- delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti da leggi penali speciali.
- delitti con finalità di terrorismo previsti dalla Convenzione di New York del 1999



Pratiche di mutilazione degli organi genitali femminili (art. 25-quater.1 d.lgs. 231/01)

Delitti contro la personalità individuale (art. 25-quinquies d.lgs. 231/01)

- Riduzione o mantenimento in schiavitù o servitù (art. 600 c.p.)
- Prostituzione minorile (art. 600 bis c.p.)
- Pornografia minorile (art. 600 ter c.p.)
- Detenzione di materiale pornografico (art. 600 quater c.p.)
- Pornografia virtuale (art. 600 quater.1 c.p.)
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies c.p.)
- Tratta di persone (art. 601 c.p.)
- Acquisto e alienazione di schiavitù (art. 602 c.p.)

Abusi di mercato (art. 25-sexies c.p.)

- abuso di informazioni privilegiate (art. 184 D.lgs. 58/1998 - Testo Unico dell'Intermediazione Finanziaria).
- manipolazione del mercato (art. 185 D.lgs. 58/1998).
- abuso di informazioni privilegiate (art. 187 bis D.lgs. 58/1998).
- manipolazione del mercato (art. 187 ter D.lgs. 58/1998).

Reati introdotti dall'art. 9 della legge 123/2007 (art. 25-septies d.lgs. 231/01):

- Omicidio colposo (art. 589 c.p.);
- Lesioni colpose gravi o gravissime (art. 590 comma 3 c.p.).

Ricettazione, riciclaggio e impiego di denaro, bene o utilità di provenienza illecita (art. 25-octies d.lgs. 231/01):

- Ricettazione (art.648 c.p.);
- Riciclaggio (art.648 bis);
- Impiego di denaro, beni o utilità di provenienza illecita (art.648 ter).

Delitti in materia di violazione del diritto d'autore (art. 25-novies d.lgs. 231/01)

- Immissione su sistemi di rete telematiche a disposizione del pubblico, mediante connessioni di qualsiasi genere, di opere di ingegno protette o parte di esse
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione dell'autore
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla Siae; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di un programma per elaboratori
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca dati; estrazione o reimpiego della banca di dati; distribuzione, vendita o concessione in locazione di banca di dati;
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere di ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi o ogni altro supporto contenenti fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, anche se inserite in opere collettive o composite o banche dati
- Riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita, cessione o importazione abusiva di oltre 50 copie o esemplari di opere tutelate dal diritto di autore e da diritti connessi; immissione in un sistema di rete telematiche, mediante connessioni di qualsiasi genere, di opere dell'ingegno protette



- Mancata comunicazione alla Siae dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzazione per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies d.lgs. 231/01)

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)

Reati transnazionali introdotti dagli artt. 3 e 10 della legge 146/2006:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416-bis c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quarter del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del D.P.R. 309/1990);
- Disposizioni contro le immigrazioni clandestine (art. 12 commi 3, 3-bis, 3-ter, 5, del testo unico di cui al D.lgs. 25 Luglio 1998, n. 286);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.);
- Favoreggiamento personale (art. 378 c.p.);
- riciclaggio (art. 648 bis c.p.);
- impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.).

2.4. Rapporti con la Pubblica Amministrazione

I reati contro la Pubblica Amministrazione (artt. 24 e 25, d.lgs. 231/01) sopra considerati trovano come presupposto l'instaurazione di rapporti con la P.A. (intesa in senso lato).

In relazione a tali reati e alle condotte criminose sopra esplicitate, le aree di attività a rischio che presentano profili di maggiore criticità risultano essere, ai fini della presente Parte Speciale del Modello, le seguenti:

1. Acquisizione di contratti con enti pubblici il cui ambito di rischio è:

- la gestione dei rapporti con funzionari pubblici per l'acquisizione di incarichi;
- nell'ipotesi di acquisizione di incarichi a mezzo di procedure ad evidenza pubblica, predisposizione della documentazione di offerta;
- la negoziazione con gli Enti pubblici del contratto e/o delle relative condizioni di vendita o consulenza.

2. Gestione dei rapporti con funzionari pubblici per adempimenti normativi / operativi ed in occasione di verifiche e ispezioni sul rispetto della normativa medesima il cui ambito di rischio è:

- la gestione amministrativa (es: adempimenti fiscali, rapporti con Banca d'Italia, rapporti con uffici tributari, rapporti con CCIAA, ufficio del Registro, Guardia di Finanza, ecc);
- la gestione delle verifiche ispettive da parte delle Autorità competenti;
- la gestione del personale (es: rapporti con gli enti previdenziali ed assistenziali, INPS, INAIL), gestione convenzione enti pubblici (es: disabili, ecc) e relative verifiche ispettive;



- la gestione dei rapporti con funzionari pubblici (A.S.L., VVFF, Ispettorato del Lavoro, medico competente, etc.) per gli adempimenti prescritti dal TU sulla sicurezza, anche in occasione di ispezioni/ verifiche;
- la gestione degli immobili di proprietà e non (A.S.L., rinnovo certificati, ecc);
- la gestione degli adempimenti relativi ai diritti di proprietà industriale o intellettuale (es: brevetti, marchi, diritto d'autore).

3. Gestione dei rapporti con le Autorità di Pubblica Vigilanza il cui ambito di rischio è:

- la gestione degli adempimenti e dei rapporti con il Garante per la Protezione dei Dati Personali ai sensi della L. 196/03;
- la gestione dei rapporti con la Banca di Italia, Isvap e con la Consob;

4. Gestione dei contenziosi il cui ambito di rischio è:

- la gestione dei rapporti con la Banca di Italia e con la Consob;
- la gestione dei rapporti con i magistrati competenti, con i loro consulenti tecnici ed ausiliari, nell'ambito di procedimenti amministrativi, civili o penali;
- la gestione dei rapporti con i magistrati competenti, con i loro consulenti tecnici ed ausiliari, nell'ambito delle cause di lavoro.

5. Richiesta, percezione e gestione di contributi e/o finanziamenti pubblici agevolati, il cui ambito del rischio è:

- la gestione dei contatti preliminari con gli Enti Pubblici finanziatori, nazionali e sovranazionali, per l'ottenimento di finanziamenti a fondo perduto e/o a tasso agevolato, contributi o erogazioni pubbliche;
- la realizzazione dei progetti agevolati e predisposizione/trasmissione all'Ente erogante di prospetti, relazioni, documenti di rendicontazione per l'ottenimento dell'erogazione;
- la gestione dei rapporti con i delegati dell'Ente Pubblico erogante in sede di verifiche ed accertamenti circa il corretto conseguimento e utilizzo del finanziamento, il rispetto delle modalità previste per la realizzazione del progetto e la veridicità di quanto dichiarato in fase di rendicontazione.

2.4.1 I principi di comportamento da tenere nell'ambito dei rapporti con la Pubblica Amministrazione

Al fine di evitare la commissione dei reati negli ambiti sopra descritti, la Banca ha definito specifiche disposizioni volte a regolamentare la gestione dei rapporti tra i Destinatari e la Pubblica Amministrazione, contenute nel Codice di Comportamento e nel Regolamento della Disciplina delle deleghe di potere (05A003), cui si rimanda.

2.4.2 Compiti specifici dell'Organismo di Vigilanza

I compiti dell'Organismo di Vigilanza concernenti la valutazione sull'efficacia delle procedure e l'osservanza delle prescrizioni del Modello in materia di prevenzione dei reati contro la Pubblica Amministrazione sono i seguenti:

- verifica periodica, del sistema di deleghe vigente e del rispetto della procedura di comunicazione alle unità organizzative interessate;
- verifica della regolarità dei comportamenti da tenere nei rapporti con la Pubblica Amministrazione, così come definiti nelle disposizioni interne.



2.5. Prevenzione dei reati societari

Una delle aree di attività che presenta i profili di maggiore criticità risulta essere la gestione della contabilità generale e la predisposizione dei progetti di bilancio civilistico nonché di (eventuali) situazioni patrimoniali in occasione dell'effettuazione di operazioni straordinarie. Medesime considerazioni, valgono per ogni altro adempimento in materia societaria il cui ambito di rischio è:

- la gestione della contabilità generale e rilevazione, raccolta, aggregazione e valutazione dei dati contabili necessari per la predisposizione della proposta di bilancio e delle situazioni patrimoniali da sottoporre alla delibera del Consiglio di Amministrazione;
- predisposizione dei progetti di bilancio da sottoporre ad approvazione del Consiglio di Amministrazione;
- custodia delle scritture contabili e dei Libri Sociali e predisposizione relazioni, comunicazioni sociali e di mercato;
- predisposizione delle situazioni economiche e patrimoniali relative alla gestione dei conferimenti, destinazione dell'utile, operazioni sul capitale e operazioni straordinarie;
- attività strumentali propedeutiche a convocazioni/delibere assembleari e gestione dei rapporti con tale organo sociale;
- rapporti con il Collegio Sindacale, revisori e soci relativamente alle verifiche sulla gestione amministrativa/contabile e sul bilancio di esercizio e consolidato;
- relazioni infragruppo o con parti correlate.

2.5.1 I principi di comportamento da tenere per la prevenzione di reati societari

Con riferimento alle summenzionate aree a rischio di commissione reati, la Banca, oltre ad aver definito specifiche disposizioni finalizzate alla prevenzione dei reati societari, raccolte nel Codice di Comportamento (cui si rimanda), rileva che la delibera di approvazione del bilancio d'esercizio indica e descrive analiticamente i criteri redazionali del bilancio medesimo e che vi è un controllo periodico da parte del Collegio Sindacale, che assiste a tutte le sedute del Consiglio di Amministrazione e del Comitato Esecutivo, sull'effettivo rispetto dei criteri redazionali del bilancio sulla base delle risultanze della società di revisione.

2.5.2 Compiti dell'Organismo di Vigilanza

All'Organismo di Vigilanza vengono assegnati i seguenti compiti:

- Assicurare l'emanazione e l'aggiornamento delle istruzioni emanate relative ai comportamenti da seguire nell'ambito delle aree a rischio. Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;
- con riferimento al bilancio, alle relazioni ed alle altre comunicazioni sociali previste dalla legge, in ragione della circostanza che il bilancio di esercizio è sottoposto a verifica di una società di revisione, provvedere all'espletamento dei seguenti compiti:
 - monitoraggio sull'efficacia delle procedure interne per la prevenzione del reato di false comunicazioni sociali;



- vigilanza sull'effettiva sussistenza delle condizioni per garantire alla società di revisione una concreta autonomia nelle sue funzioni di controllo delle attività aziendali.
- con riferimento alle altre attività a rischio:
 - svolgere verifiche periodiche sull'efficacia e il rispetto delle procedure interne inerenti alla gestione della contabilità, predisposizione dei bilanci e altre attività amministrative connesse volte a prevenire la commissione dei reati;
 - svolgere verifiche periodiche circa il rispetto degli adempimenti fiscali e contabili rispetto alla normativa italiana;
 - svolgere verifiche periodiche al fine di accertare la corretta registrazione delle operazioni infragruppo;
 - svolgere verifiche periodiche sull'effettuazione delle comunicazioni alle Autorità pubbliche di Vigilanza e sull'osservanza delle procedure adottate nel corso di eventuali ispezioni compiute dai funzionari di queste ultime;

2.6. Prevenzione dei reati in materia di abusi di mercato

L'area di attività a rischio che presenta profili di maggiore criticità risulta essere la seguente:

Gestione delle informazioni privilegiate e "price sensitive", il cui ambito di rischio è:

- la gestione delle informazioni "price sensitive", atta a provocare una sensibile alterazione del prezzo degli strumenti finanziari emessi;
- l'utilizzo delle informazioni "price sensitive" nello svolgimento dell'attività

2.6.1 Le informazioni privilegiate

La nozione di informazione privilegiata rappresenta il fulcro attorno al quale ruota l'intera disciplina dell'insider trading.

Secondo l'art. 181 TUF, per "informazione privilegiata" si intende una informazione:

- di carattere preciso, nel senso che deve riferirsi ad un complesso di circostanze esistenti o che si possa ragionevolmente prevedere che verrà ad esistenza o ad un evento verificatosi o che si possa ragionevolmente prevedere che si verificherà, e sufficientemente specificata in modo da consentire di trarre conclusioni sul possibile effetto del complesso di circostanze o dell'evento di cui sopra sui prezzi degli strumenti finanziari;
- che non è stata ancora resa pubblica;
- che concerne, direttamente (corporate information, fatti generati o provenienti dalla società emittente) o indirettamente (market information, fatti generati al di fuori della sfera dell'emittente e che abbiano un significativo riflesso sulla market position dell'emittente), uno o più emittenti strumenti finanziari o uno o più strumenti finanziari.

Relativamente alla nozione di strumenti finanziari, si segnala che, ai sensi dell'art. 180 TUF, si intendono per strumenti finanziari: gli strumenti finanziari di cui all'art. 1, comma 2 dello stesso TUF – ovvero:

- le azioni o altri titoli rappresentativi di capitale di rischio negoziabili sul mercato dei capitali;
- le obbligazioni, i titoli di Stato e gli altri titoli di debito negoziabili sul mercato dei capitali;
- bis) gli strumenti finanziari, negoziabili sul mercato dei capitali, previsti dal Codice civile;
- le quote di fondi comuni di investimento;
- i titoli normalmente negoziati sul mercato monetario;
- qualsiasi altro titolo normalmente negoziato che permetta di acquisire gli strumenti indicati nelle precedenti lettere e i relativi indici;



- i contratti “futures” su strumenti finanziari, su tassi di interesse, su valute, su merci e sui relativi indici, anche quando l’esecuzione avvenga attraverso il pagamento di differenziali in contanti;
- i contratti di scambio a pronti e a termine (swaps) su tassi di interesse, su valute, su merci nonché su indici azionari (equity swaps), anche quando l’esecuzione avvenga attraverso il pagamento di differenziali in contanti;
- i contratti a termine collegati a strumenti finanziari, a tassi di interesse, a valute, a merci e ai relativi indici, anche quando l’esecuzione avvenga attraverso il pagamento di differenziali in contanti;
- i contratti di opzione per acquistare o vendere gli strumenti indicati nelle precedenti lettere e i relativi indici, nonché i contratti di opzione su valute, su tassi d’interesse, su merci e sui relativi indici, anche quando l’esecuzione avvenga attraverso il pagamento di differenziali in contanti;
- le combinazioni di contratti o titoli indicati nelle precedenti lettere, ammessi alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell’Unione Europea, nonché qualsiasi altro strumento ammesso o per il quale è stata presentata domanda di ammissione alle negoziazioni in un mercato regolamentato di un Paese dell’Unione Europea.

2.6.2 I principi di comportamento da tenere per la prevenzione dei reati in materia di abusi di mercato

Al fine di evitare la commissione dei reati negli ambiti sopra descritti, la Banca ha definito specifiche disposizioni, contenute nella Norma Operativa “Market Abuse” a cui si rimanda (08C002).

2.6.3 Compiti dell’Organismo di Vigilanza

I compiti di vigilanza dell’Organismo per quanto concerne i reati e gli illeciti di abuso di mercato sono i seguenti:

- con riferimento al trattamento delle Informazioni Privilegiate, l’OdV provvede all’espletamento dei seguenti compiti:
 - monitoraggio sull’efficacia delle procedure interne per la prevenzione degli illeciti di abuso di mercato,
 - esame di eventuali segnalazioni specifiche provenienti dagli organi di controllo o da qualsiasi dipendente ed effettuazione degli accertamenti ritenuti necessari od opportuni in consegna delle segnalazioni ricevute.
- con riferimento alle altre attività a rischio l’OdV provvede all’espletamento dei seguenti compiti:
 - svolgimento delle verifiche periodiche sull’effettuazione delle eventuali comunicazioni di operazioni sospette alla Consob.

2.7. Prevenzione dei reati in violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro

L’art. 9 della Legge n. 123/2007 ha introdotto nel D. Lgs. n. 231/2001 l’art. 25-septies, che estende la responsabilità amministrativa delle società ai reati di omicidio colposo e lesioni personali colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro.

Nelle ipotesi di commissione dei reati contemplati dall’art. 25-septies, la responsabilità prevista dal D. Lgs. n. 231/2001 è configurabile solo se dal fatto illecito ne sia derivato un vantaggio per la società, che, nel caso di specie, potrebbe essere rinvenuto in un risparmio di costi o di tempi.



I presupposti per definire il fatto colposo sono:

- le condotte penalmente rilevanti consistono nel fatto, da chiunque commesso, di cagionare la morte o lesioni gravi/gravissime al lavoratore, per effetto dell'inosservanza di norme antinfortunistiche;
- soggetto attivo dei reati può essere chiunque sia tenuto ad osservare o far osservare la norme di prevenzione e protezione Tale soggetto può quindi individuarsi nei datori di lavoro, nei dirigenti, nei preposti, nei soggetti destinatari di deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro, nonché nei medesimi lavoratori;
- nella previsione del codice penale, le fattispecie delittuose contemplate dagli artt. 589 e 590 sono caratterizzate dall'aggravante della negligente inosservanza delle norme antinfortunistiche. L'elemento soggettivo, dunque, consiste nella c.d. colpa specifica, ossia nella volontaria inosservanza di norme precauzionali volte a impedire gli eventi dannosi previsti dalla norma incriminatrice;
- il concetto di colpa specifica rimanda all'art. 43 c.p., nella parte in cui si prevede che il delitto è colposo quando l'evento, anche se preveduto ma in ogni caso non voluto dall'agente, si verifica a causa dell'inosservanza di norme di leggi, regolamenti, ordini o discipline;
- le norme antinfortunistiche di cui agli artt. 589, co. 2, e 590, co. 3, c.p., ricomprendono anche l'art. 2087 c.c., che impone al datore di lavoro di adottare tutte quelle misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica dei lavoratori.

La Banca si impegna ad assolvere agli obblighi giuridici relativi:

- a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- d) alle attività di sorveglianza sanitaria;
- e) alle attività di informazione e formazione dei lavoratori;
- f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

2.7.1 I principi di comportamento da tenere nell'ambito del rispetto delle norme antinfortunistiche e della tutela dell'igiene e della salute del lavoro.

È fatto obbligo per tutti i Destinatari del Modello di rispettare ogni cautela possibile (anche non espressamente nominata) volta ad evitare qualsivoglia danno. La Banca ha implementato tutti gli opportuni standard di sicurezza e ha, inoltre, predisposto un apposito Regolamento in materia di sicurezza sul lavoro con Allegati (Regolamento del processo della Salute e Sicurezza sul



Lavoro e relativo Sistema di Gestione - SGSL) (09A006), cui si fa rimando per i relativi profili di interesse.

L'obbligo di sicurezza in capo al datore di lavoro non può intendersi in maniera esclusivamente statica quale obbligo di adottare le misure di prevenzione e sicurezza (forme di protezione oggettiva) ma deve intendersi anche in maniera dinamica implicando l'obbligo di informare e formare i lavoratori sui rischi propri dell'attività lavorativa e sulle misure idonee per evitare i rischi o ridurli al minimo (forme di protezione soggettiva).

2.7.2 Compiti dell'Organismo di Vigilanza

L'estensione dell'applicazione del decreto 231 ai delitti colposi non pone un problema di rapporti tra il piano della sicurezza e quello del Modello organizzativo, nonché tra le attività dei soggetti responsabili dei controlli in materia di salute e sicurezza sul lavoro e l'Organismo di Vigilanza. L'autonomia di funzioni proprie di questi organi non consente di ravvisare una sovrapposizione dei compiti di controllo: i diversi soggetti deputati al controllo svolgono i propri compiti su piani differenti.

Per quanto concerne le tematiche di tutela della salute e sicurezza sul lavoro, l'OdV si avvale di tutte le risorse attivate per la gestione dei relativi aspetti (RSPP - Responsabile del Servizio di Prevenzione e Protezione, ASPP – Addetti al Servizio di Prevenzione e Protezione, RLS – Rappresentante dei Lavoratori per la Sicurezza, MC - Medico Competente, addetti primo soccorso, addetto emergenze in caso d'incendio).

L'Organismo di Vigilanza prevede un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico, in particolare attraverso le verifiche svolte dall'Organismo di Monitoraggio previsto dalle norme sulla salute e sicurezza sul lavoro.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante e dovrà ricevere copia della reportistica periodica in materia di salute e sicurezza sul lavoro.

2.8. Prevenzione dei reati in violazione delle norme anti-riciclaggio

Ai sensi dell'art. 25-octies, D. Lgs. n. 231/2001, recentemente inserito dal d.lgs. 231/2007, l'ente è punibile per i reati di ricettazione, riciclaggio e impiego di capitali illeciti, anche se compiuti in ambito prettamente "nazionale", sempre che ne derivi un interesse o vantaggio per l'ente medesimo.

La finalità del decreto n. 231/2007 consiste nella protezione del sistema finanziario dal suo utilizzo a fini di riciclaggio o di finanziamento del terrorismo. Tale tutela viene attuata con la tecnica della prevenzione per mezzo di apposite misure e obblighi di comportamento per una vasta platea di soggetti - individuati agli artt. 10, co. 2, 11, 12, 13 e 14 del decreto - che comprende, oltre alle banche e agli intermediari finanziari, anche gli altri soggetti a cui erano già stati estesi gli obblighi antiriciclaggio dal D. Lgs. n. 56/04: professionisti; revisori contabili; altri soggetti.

I reati presupposto sono i seguenti:

1. Ricettazione (art. 648 c.p.)
2. Riciclaggio (art. 648-bis c.p.)
3. Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)



La responsabilità amministrativa dell'ente per i reati previsti dagli art. 648, 648-bis e 648 ter, c.p. è limitata alle ipotesi in cui il reato sia commesso nell'interesse o a vantaggio dell'ente medesimo.

Considerato che le fattispecie delittuose in questione possono essere realizzate da chiunque (c.d. reati comuni), si ritiene che la ricorrenza del requisito oggettivo dell'interesse o vantaggio vada escluso ogni qual volta non vi sia attinenza tra la condotta incriminata e l'attività d'impresa esercitata dall'ente.

Al fine di prevenire i citati reati, la Banca pone in essere le seguenti misure:

- Identifica ed effettua l'adeguata verifica della clientela, nonché verifica dell'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari.
- Verifica della regolarità con riferimento alla limitazione dell'uso del contante e dei titoli al portatore.
- Controlli formali e sostanziali della movimentazione, con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni infragruppo.
- Determinazione dei requisiti minimi in possesso dei fornitori e fissazione dei criteri di valutazione delle offerte, nonché del responsabile dell'esecuzione del contratto di fornitura di beni e servizi, con indicazione di compiti, ruoli e responsabilità.
- Adozione di adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio.

2.8.1 I principi di comportamento da tenere nell'ambito del rispetto delle norme anti-riciclaggio

I Destinatari del Modello devono agire in ottemperanza alle politiche interne poste in essere dalla Banca. In particolare, per quanto concerne la prevenzione dei reati di riciclaggio, essi non devono interfacciarsi con clienti, venditori od altre parti che vogliano intrattenere relazioni d'affari con la Banca senza aver previamente soddisfatto tutti i requisiti necessari per l'identificazione della parte e del denaro o dei beni oggetto della contrattazione.

In materia di anti-riciclaggio, la Banca ha predisposto un apposito Regolamento Antiriciclaggio (08A001) nonché due norme operative (Segnalazione di operazioni sospette - 07C001 e Identificazione, adeguata verifica e censimento della clientela - 08C010) e lettere circolari in tema di gestione di assegni e libretti, cui si rimanda per i profili di specifico interesse.

2.8.2 Compiti dell'Organismo di Vigilanza

L'art. 52 del decreto 231/2007 obbliga i diversi organi di controllo di gestione, tra cui l'OdV, esistenti negli enti destinatari della disciplina a vigilare sull'osservanza della normativa antiriciclaggio e a comunicare le violazioni delle relative disposizioni di cui vengano a conoscenza nell'esercizio dei propri compiti o di cui abbiano altrimenti notizia.

Tali obblighi di comunicazione riguardano in particolar modo le possibili infrazioni relative alle operazioni di registrazione, segnalazione e ai limiti all'uso di strumenti di pagamento e di deposito (contante, titoli al portatore, conti e libretti di risparmio anonimi o con intestazioni fittizie) e sono destinati ad avere effetto sia verso l'interno dell'ente (titolare dell'attività o legale rappresentante) che verso l'esterno (autorità di vigilanza di settore, Ministero Economia e Finanze, Unità di Informazione Finanziaria presso la Banca d'Italia).



Il dovere di informativa dell'OdV deve essere parametrato alla funzione, prevista dall'art. 6, co. 1, lett. b) del decreto 231, di vigilare sul funzionamento e sull'osservanza dei modelli e, con specifico riferimento all'antiriciclaggio, di comunicare quelle violazioni di cui venga a conoscenza nell'esercizio delle proprie funzioni o nelle ipotesi in cui ne abbia comunque notizia (es. su segnalazione di dipendenti o altri organi dell'ente).

Tale chiave di lettura, senza riconoscere una posizione di garanzia, in assenza di effettivi poteri impeditivi dell'OdV rispetto alle fattispecie di reato in esame, viene completata dalla sanzione penale della reclusione fino a 1 anno e della multa da 100 a 1000 euro in caso di mancato adempimento dei suddetti obblighi informativi (art. 55, co. 5).

Vale la pena sottolineare che quello in esame è l'unico caso in cui il legislatore abbia espressamente disciplinato una specifica fattispecie di reato a carico dell'OdV (reato omissivo proprio), peraltro a seguito del riconoscimento di una atipica attività a rilevanza esterna dello stesso.

2.9. Prevenzione reati connessi alla criminalità organizzata nazionale e transnazionale

La Legge n. 146 del 2006 di ratifica ed esecuzione della Convenzione ONU contro il crimine organizzato transnazionale, ha stabilito l'applicazione del Decreto 231/2001 ai reati di criminalità organizzata transnazionale.

La Legge 15 luglio 2009, n. 94 recante disposizioni in materia di sicurezza pubblica ha previsto l'inserimento dell'articolo 24-ter riguardante la responsabilità amministrativa degli enti per i delitti di criminalità organizzata.

In linea generale, nell'ambito della più ampia definizione di reati di criminalità transnazionale e con riferimento ai reati presupposto della responsabilità amministrativa dell'ente ex D.Lgs. n. 231/2001, vengono in considerazione le fattispecie delittuose concernenti i reati di associazione, i reati di traffico di migranti e di intralcio alla giustizia, a condizione che tali condotte delittuose siano state commesse, nell'interesse o a vantaggio dell'ente, da soggetti che rivestono al suo interno un ruolo apicale o subordinato.

Per una disamina delle disposizioni volte a prevenire la commissione di tali reati, si rinvia a quanto descritto nel contesto del Codice di Comportamento della Banca.

2.9.1 Compiti dell'Organismo di Vigilanza

I compiti di vigilanza dell'Organismo per quanto concerne i reati a carattere transnazionale sono i seguenti:

- Assicurare che venga effettuata l'identificazione e l'adeguata verifica della clientela, in particolare per quanto riguarda l'appartenenza della clientela a liste di soggetti segnalate dalle Autorità (anagrafe negativa).

2.10. Prevenzione dei Reati in violazione delle norme in materia di delitti informatici e trattamento illecito di dati

Mediante la promulgazione della legge n. ° 48 del 18 Marzo 2008, nel cui art. 7 il legislatore ha previsto l'introduzione dell'art. 24-bis nell'impianto normativo del D.lgs. n. 231/01, il legislatore ha ratificato e dato esecuzione alla Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001.



L'introduzione dell'articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231, risponde all'esigenza di introdurre forme di responsabilità penale per le persone giuridiche anche con riferimento ai reati informatici più gravi.

Occorre subito specificare che nonostante nel titolo dell'art.24-bis si faccia riferimento anche al "trattamento illecito dei dati", il corpo dell'articolo in questione non fa alcun riferimento alla disciplina relativa al trattamento illecito dei dati personali. Pertanto, il risk assessment svolto non ha avuto in oggetto la verifica della corretta attuazione della normativa nazionale in tema di privacy ed, in particolare, dell'art. 167 del Codice della privacy (D.lgs. 196/03).

In relazione alle fattispecie di reato previsto dall'articolo 24-bis, è stata attuata una analisi delle procedure di accesso e di utilizzo dei sistemi informatici aziendali (modalità di utilizzo di strumenti informatici o telematici dell'ente dal dipendente o dal soggetto posto in posizione apicale, security policies per filtri di traffico di rete, ecc.) in merito alle principali aree a rischio.

L'area di Attività a Rischio che presenta profili di maggiore criticità risulta essere, ai fini della presente Parte Speciale del Modello, la gestione dei sistemi informativi e dei documenti informatici ed in particolare le seguenti attività:

- Predisposizione dell'assetto organizzativo a presidio dell'IT;
- Definizione Piano Strategico IT;
- Analisi e valutazione dei rischi IT;
- Individuazione e gestione degli indirizzi, delle politiche e del piano della sicurezza IT;
- Gestione del piano di comunicazione e della formazione inerente la gestione dei sistemi informativi e dei relativi strumenti di sicurezza;
- Gestione dell'inventario dell'hardware e del software aziendale;
- Definizione delle autorizzazioni di accesso ai Sistemi Informatici e Controllo Accessi;
- Acquisizione/ Sviluppo e manutenzione di Software Applicativo;
- Gestione modifiche ai software (Change management);
- Gestione dei sistemi e della rete;
- Monitoraggio della Sicurezza;
- Incident & Problem Management (registrazione dei malfunzionamenti, analisi e individuazione delle soluzioni);
- Verifica della conformità alle politiche e alle procedure di IT governance e sicurezza ICT (IT Audit);
- Gestione degli adempimenti e degli obblighi previsti dalla legge per il rilascio di certificazioni di firma elettronica qualificate.

2.10.1 I principi di comportamento da tenere per la prevenzione dei reati in violazione delle norme in materia di delitti informativi e trattamento illecito dei dati

La Banca ha implementato un processo in materia di gestione dei sistemi informativi e dei documenti informatici, definiti a livello locale, a tutela dei rischi di commissione dei reati informatici di cui all'art. 24 bis del D.lgs. 231/01, che definisce:

- ruolo e responsabilità dei soggetti coinvolti nelle singole fasi del processo;
- flussi informativi e documentali;
- flussi autorizzativi;
- attività di controllo e monitoraggio;
- modalità di gestione delle eccezioni;
- modalità di archiviazione della documentazione.

È stato inoltre istituito un Comitato Sicurezza con funzione deliberante, per l'individuazione delle misure di sicurezza e per la definizione delle norme strategiche ed operative in materia di sicurezza fisica, logica ed amministrativa della banca con riferimento alle disposizioni di legge ed



amministrative tempo per tempo vigenti. Le deliberazioni vengono assunte sulla base delle proposte formulate dalla Direzione Commerciale e di Sviluppo.

La Banca richiede che ogni proprio dipendente e/o collaboratore sottoscriva la qualifica di incaricato ai fini del trattamento dei dati personali dei propri clienti.

Per quanto concerne i profili procedurali specificamente predisposti dalla Banca al fine di prevenire la commissione dei menzionati delitti, si rimanda a quanto specificato nel Codice di Comportamento redatto dalla Banca medesima ed ai documenti di riferimento in materia.

La Banca ha predisposto e mantiene costantemente aggiornato un apposito Documento programmatico sulla sicurezza.

2.10.2 Compiti dell'Organismo di Vigilanza

I compiti di vigilanza dell'Organismo per quanto concerne i reati e gli illeciti in materia di delitti informatici e trattamento illecito dei dati sono i seguenti:

- svolgere verifiche periodiche sull'efficacia e il rispetto delle procedure interne inerenti alla gestione dei sistemi informatici e altre attività volte a prevenire la commissione dei reati.

2.11. Reati in materia di falsità di monete, in carte di pubblico credito, in valori in bollo e in strumenti o segni di riconoscimento

La legge 23 novembre 2001, n. 4092, di conversione del D.L. n. 350/2001 recante disposizioni urgenti in vista dell'euro, ha introdotto, all'art. 4, un nuovo articolo al decreto n. 231 (l'art. 25-bis) relativo alle falsità in monete, carte di pubblico credito e in valori di bollo. La Legge 23 luglio 2009, n. 99 ha esteso l'art. 25 bis ai segni di riconoscimento, introducendo tra i reati presupposto la contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni e l'introduzione nello Stato e commercio di prodotti con segni falsi.

Per una disamina delle disposizioni poste in essere dalla Banca al fine di prevenire la commissione di tali fattispecie di reato, si rimanda al Codice di Comportamento ed alla Norma operativa sulla gestione del contante.

2.12. Delitti in materia di terrorismo o di eversione dell'ordine democratico

La legge 14 gennaio 2003, n. 7, ha introdotto nel D.Lgs. 231/01 i "reati con finalità di terrorismo o di eversione dell'ordine democratico" (art. 25-quater).

Diversamente da quanto accade per gli altri reati previsti dal D.Lgs. 231/01, l'art. 25-quater [1] "reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali" opera un rinvio generale "aperto" a tutte le ipotesi attuali e future di reati per:

- delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale;
- delitti aventi finalità di terrorismo o di eversione dell'ordine democratico previsti dalle leggi speciali;
- delitti previsti dall'art. 2 della Convenzione Internazionale di New York del 9 dicembre 1999.



Per una disamina delle disposizioni poste in essere dalla Banca al fine di prevenire la commissione di tali fattispecie di reato, si rimanda al Codice di Comportamento.

2.13. Delitti contro l'industria ed il commercio ed in materia di violazione del diritto d'autore

In data 9 Luglio 2009 il Senato ha definitivamente approvato il disegno di legge 1195 B, che, tra l'altro, modifica l'art 25-bis del D. Lgs. 231/2001 ed inserisce nel medesimo Decreto l'art 25 bis. 1 (delitti contro l'industria e il commercio) e l'art 25 nonies (delitti in materia di violazioni del diritto d'autore).

Per una disamina delle disposizioni poste in essere dalla Banca al fine di prevenire la commissione di tali fattispecie di reato, si rimanda al Codice di Comportamento.

2.14. Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Per una disamina delle disposizioni poste in essere dalla Banca al fine di prevenire la commissione di tali fattispecie di reato, si rimanda al Codice di Comportamento.

3. Glossario

Termine/acronimo	Definizione
Attività/Area a Rischio Reato Attività a Rischio Attività Sensibili	Attività aziendali nel cui ambito potrebbero astrattamente crearsi le occasioni e/o le condizioni per la commissione di Reati.
Gruppo	Gruppo Cassa di Risparmio di Bolzano composto da: Cassa di Risparmio di Bolzano S.p.A. (Capogruppo) Sparim S.p.A. Millennium Sim S.p.A.
Collaboratori	Soggetti che intrattengono con la Banca rapporti di collaborazione senza vincolo di subordinazione, di rappresentanza commerciale ed altri rapporti che si concretino in una prestazione professionale non a carattere subordinato, sia continuativa sia occasionale nonché quanti, in forza di specifici mandati e procure, rappresentano la Banca verso terzi.
Consulenti	Coloro i quali forniscono informazioni e pareri ed assistono la Banca nello svolgimento di determinati atti, in forza di accertata esperienza e pratica in specifiche materie.
Dipendenti	Persone sottoposte alla direzione o alla vigilanza di soggetti che rivestono funzioni di rappresentanza, amministrazione o di direzione, ossia tutti i soggetti che intrattengono un rapporto di lavoro subordinato, di qualsivoglia natura con la Banca.
Fornitori	Coloro i quali forniscono beni o servizi in favore della Banca.
Destinatari	Gli Organi societari, i Dipendenti, i Collaboratori, i Consulenti, i Fornitori e, più in generale, tutti coloro che, a qualunque titolo, operano per conto o nell'interesse della Banca.
Modello 231/2001	Il Modello di organizzazione, gestione e controllo ritenuto dagli Organi Societari idoneo a prevenire i Reati e, pertanto, adottato dalla Banca, ai sensi degli articoli 6 e 7 del D.lgs. 231/01, al fine di prevenire la realizzazione dei Reati stessi da parte dei Soggetti Apicali o dei Dipendenti.
Organi Societari Organi Sociali	L'Organo Amministrativo e/o il Collegio Sindacale della Banca e i relativi componenti, in funzione del contesto di riferimento.
Organismo di Vigilanza	L'Organismo previsto dall'art. 6 del Decreto Legislativo, avente il compito di vigilare sul funzionamento e l'osservanza del modello di organizzazione, gestione e controllo, nonché sull'aggiornamento dello stesso.
Organo Amministrativo Organo Dirigente	L'Organo con idonei poteri di firma di rappresentanza e impegno della Banca, individuato nello Statuto e successive integrazioni
Protocolli	Le misure organizzative, fisiche e/o logiche previste dal Modello al fine di prevenire la realizzazione dei Reati.
Reati	L'insieme dei reati / il singolo reato, richiamati dal D.lgs. 231/01 e dalle successive modifiche e integrazioni.



Soggetti Apicali	Soggetti di cui all'articolo 5, comma 1, lett. a) del Decreto, ovvero i soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Banca o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale; in particolare, i membri dell'Organo Amministrativo, il Presidente, il Direttore Generale, gli eventuali institori, i procuratori.
Soggetti Esterni	I lavoratori autonomi o parasubordinati, i professionisti, i Consulenti, gli agenti, i Fornitori, i partner commerciali, ecc.
Pubblica Amministrazione	Le amministrazioni dello Stato, compresi gli istituti e scuole di ogni ordine e grado, le istituzioni educative, le aziende e le amministrazioni dello Stato ad ordinamento autonomo, le regioni, le province ed i comuni, le comunità montane e loro consorzi ed associazioni, le istituzioni universitarie, le amministrazioni ed aziende del servizio sanitario nazionale e le agenzie di cui al decreto legislativo 30/7/1999, n.300. Per Pubblica Amministrazione si deve intendere anche la persona, fisica che agisce in qualità di pubblico ufficiale o in qualità di incaricato di un pubblico servizio.