



**ELEMENTI DI SINTESI DEL
“DOCUMENTO DESCRITTIVO DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E
CONTROLLO *EX* D.LGS. 231/2001 DI UBI BANCA S.C.P.A.”**

INDICE

QUADRO NORMATIVO.....	4
<u>INTRODUZIONE.....</u>	4
<u>AUTORI DEL REATO.....</u>	4
<u>FATTISPECIE DI REATO.....</u>	4
<u>SANZIONI.....</u>	5
<u>DELITTI TENTATI.....</u>	5
<u>REATI COMMESSI ALL'ESTERO.....</u>	6
<u>MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO.....</u>	6
<u>SINDACATO DI IDONEITÀ.....</u>	8
IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 231/2001 DI UBI BANCA.8	
L'ORGANISMO DI VIGILANZA DI UBI BANCA.....	9
<u>PRINCIPI GENERALI IN TEMA DI ISTITUZIONE E NOMINA DELL'ORGANISMO DI VIGILANZA.....</u>	10
<u>FUNZIONI E POTERI DELL'ORGANISMO DI VIGILANZA.....</u>	10
<u>VERIFICHE E CONTROLLI SUL MODELLO.....</u>	12
<u>OBBLIGHI DI INFORMAZIONE NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA – FLUSSI INFORMATIVI.....</u>	12
<u>INVIO DELLE SEGNALAZIONI - RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI.....</u>	13
<u>REPORTING DELL'ORGANISMO DI VIGILANZA VERSO GLI ORGANI SOCIETARI.....</u>	13
SISTEMA DISCIPLINARE.....	13
<u>FUNZIONE DEL SISTEMA DISCIPLINARE.....</u>	13
<u>MISURE NEI CONFRONTI DI LAVORATORI SUBORDINATI.....</u>	13
<u>MISURE NEI CONFRONTI DEI COMPONENTI DEL CONSIGLIO DI GESTIONE E DEL CONSIGLIO DI SORVEGLIANZA.....</u>	14
<u>MISURE NEI CONFRONTI DI PARTNER COMMERCIALI, AGENTI, PROMOTORI FINANZIARI, CONSULENTI, COLLABORATORI.....</u>	14
FORMAZIONE E COMUNICAZIONE.....	14
<u>PREMESSA.....</u>	15
<u>DIPENDENTI E COMPONENTI DEGLI ORGANI SOCIALI.....</u>	15
<u>ALTRI DESTINATARI.....</u>	15
<u>ATTIVITÀ DI FORMAZIONE.....</u>	16
CRITERI DI AGGIORNAMENTO DEL MODELLO.....	16
<u>AGGIORNAMENTO DEL MODELLO.....</u>	16
LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA.....	17
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE.....</u>	17
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI REATI DI FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO, IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO.....</u>	18
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI REATI SOCIETARI.....</u>	18
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI DELITTI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO.....</u>	19
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI REATI CONTRO LA PERSONALITÀ INDIVIDUALE.....</u>	19
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AL REATO DI AGGIOTAGGIO E AI REATI (ED ILLECITI AMMINISTRATIVI) DI ABUSO DI INFORMAZIONI PRIVILEGIATE E DI MANIPOLAZIONE DEL MERCATO.....</u>	20
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI REATI TRANSNAZIONALI.....</u>	20
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI REATI IN MATERIA DI TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO.....</u>	21
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI DELITTI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA.....</u>	21

Elementi di Sintesi del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 di UBI Banca S.C.p.A. approvato dal Consiglio di Gestione e dal Consiglio di Sorveglianza rispettivamente in data 25 gennaio e 25 febbraio 2011

<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI.....</u>	<u>22</u>
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI DELITTI DI CRIMINALITÀ ORGANIZZATA.....</u>	<u>22</u>
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO.</u>	<u>23</u>
<u>LE ATTIVITÀ INDIVIDUATE COME SENSIBILI AI FINI DEL D.LGS. 231/2001 IN UBI BANCA CON RIFERIMENTO AI DELITTI IN MATERIA DI VIOLAZIONE DEI DIRITTI D'AUTORE.....</u>	<u>23</u>
IL SISTEMA DEI CONTROLLI.....	24

Quadro normativo.

Introduzione.

Con il decreto legislativo 8 giugno 2001 n. 231 (di seguito, il “d.lgs. 231/2001”) è stata disciplinata la “*responsabilità degli enti per gli illeciti amministrativi dipendenti da reato*”, concernente gli enti forniti di personalità giuridica e le società e associazioni anche prive di personalità giuridica.

La disciplina introdotta dal d.lgs. 231/2001 prevede che le società possano essere ritenute “responsabili” per alcuni reati commessi o tentati, nell’interesse o a vantaggio delle società stesse, da esponenti dei vertici aziendali (i c.d. soggetti “in posizione apicale” o semplicemente “apicali”) e da coloro che sono sottoposti alla direzione o vigilanza di questi ultimi.

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

Alle società sono quindi applicabili, in via diretta e autonoma, sanzioni di natura sia pecuniaria che interdittiva in relazione a reati ascritti a soggetti funzionalmente legati alle società stesse.

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

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

Autori del Reato.

In base al d.lgs. 231/2001, la società è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da “persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell’ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dell’ente stesso” (i sopra definiti soggetti “in posizione apicale” o “apicali”; art. 5, comma 1, lett. a), del d.lgs. 231/2001);
- da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali (i c.d. soggetti sottoposti all’altrui direzione o vigilanza; art. 5, comma 1, lett. b), del d.lgs. 231/2001).

Fattispecie di reato.

I reati per i quali l’ente può essere ritenuto responsabile ai sensi del d.lgs. 231/2001 – se commessi nel suo interesse o a suo vantaggio dai soggetti qualificati *ex art. 5, comma 1, del decreto stesso* – possono essere compresi, per comodità espositiva, nelle seguenti categorie:

- delitti contro la pubblica amministrazione (richiamati dagli artt. 24 e 25 d.lgs. 231/2001);
- delitti in materia di criminalità informatica (richiamati dall’art. 24-*bis* d.lgs. 231/2001);
- delitti di criminalità organizzata (richiamati dall’art. 24-*ter* d.lgs. 231/2001);
- delitti contro la fede pubblica (richiamati dall’art. 25-*bis* d.lgs. 231/2001);
- delitti contro l’industria e il commercio (richiamati dall’art. 25-*bis.1* d.lgs. 231/2001);
- reati societari (richiamati dall’art. 25-*ter* d.lgs. 231/2001);
- delitti in materia di terrorismo e di eversione dell’ordine democratico (richiamati dall’art. 25-*quater* d.lgs. 231/2001);
- delitti di pratiche di mutilazione degli organi genitali femminili (richiamati dall’art. 25-*quater.1* d.lgs. 231/2001);
- delitti contro la personalità individuale (richiamati dall’art. 25-*quinquies* d.lgs. 231/2001);

- reati in materia di abusi di mercato (richiamati dall'art. 25-*sexies* d.lgs. 231/2001);
- reati transnazionali (richiamati dall'art. 10 della legge 16 marzo 2006, n. 146, di “*ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 e il 31 maggio 2001*”);
- delitti commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (richiamati dall'art. 25-*septies* d.lgs. 231/2001);
- delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (richiamati dall'art. 25-*octies* d.lgs. 231/2001);
- delitti in materia di violazione del diritto d'autore (richiamati dall'art. 25-*novies* d.lgs. 231/2001);
- reato di “*induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*” (richiamato dall'art. 25-*novies* d.lgs. 231/2001).

In base all'art. 187-*quinquies* del d.lgs. 58/1998, l'ente può essere, altresì, ritenuto responsabile del pagamento di una somma pari all'importo della sanzione amministrativa pecuniaria irrogata per gli illeciti amministrativi di abuso di informazioni privilegiate (art. 187-*bis* d.lgs. 58/1998) e di manipolazione del mercato (187-*ter* d.lgs. 58/1998), se commessi, nel suo interesse o a suo vantaggio, da persone riconducibili alle categorie dei “soggetti apicali” e dei “soggetti sottoposti all'altrui direzione o vigilanza”. Per di più, l'ultimo comma del citato art. 187-*quinquies* dispone che agli illeciti amministrativi sopra richiamati si applichino talune norme del d.lgs. 231/2001, ivi espressamente richiamate, concernenti, fra l'altro, i modelli di organizzazione, gestione e controllo con efficacia esimente.

Sanzioni.

Le seguenti sanzioni sono previste dal d.lgs. 231/2001 a carico della società, in conseguenza della commissione o tentata commissione dei reati sopra menzionati:

- sanzione pecuniaria fino a un massimo di Euro 1.549.370,69 (e sequestro conservativo in sede cautelare);
- sanzioni interdittive (applicabili anche quale misura cautelare) di durata non inferiore a tre mesi e non superiore a due anni che, a loro volta, possono consistere in:
 - interdizione dall'esercizio dell'attività;
 - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
 - divieto di contrattare con la pubblica amministrazione;
 - esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli concessi;
 - divieto di pubblicizzare beni o servizi;
- confisca (e sequestro preventivo in sede cautelare);
- pubblicazione della sentenza (in caso di applicazione di una sanzione interdittiva).

Delitti tentati.

In caso di commissione, nelle forme del tentativo, dei delitti rilevanti ai fini della responsabilità amministrativa degli enti, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà. È invece esclusa l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento.

Reati commessi all'estero.

L'art. 4 del d.lgs. 231/2001 prevede che l'ente possa essere chiamato a rispondere in Italia in relazione a reati, rilevanti ai fini della responsabilità amministrativa degli enti, commessi all'estero. Scopo di tale previsione è, come sottolineato dalla Relazione illustrativa al d.lgs. 231/2001, quello di non lasciare sfornita di sanzione una situazione criminologica di frequente verifica, anche al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.

Modelli di organizzazione, gestione e controllo.

Aspetto fondamentale del d.lgs. 231/2001 è l'attribuzione di un valore esimente ai modelli di organizzazione, gestione e controllo della società. In caso di reato commesso da un soggetto in posizione apicale, infatti, la società non risponde se prova che (art. 6, comma 1, del d.lgs. 231/2001):

- 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 e di curare il loro aggiornamento è stato affidato a un organismo della società 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 è stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza.

Nell'ipotesi, invece, in cui il reato è commesso da soggetti sottoposti all'altrui direzione o vigilanza, la società risponde se la commissione del reato è stata resa possibile dalla violazione degli obblighi di direzione o vigilanza alla cui osservanza la società è tenuta (art. 7 del d.lgs. 231/2001).

La violazione degli obblighi di direzione o vigilanza è esclusa se la società, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello verificatosi.

L'art. 7, comma 4, del d.lgs. 231/2001 definisce i requisiti dell'efficace attuazione dei modelli organizzativi:

- la verifica periodica e l'eventuale modifica del modello quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione e nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Sarà l'autorità giudiziaria che dovrà, nell'ipotesi prevista dal citato art. 7, provare la mancata adozione ed efficace attuazione di un modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello verificatosi.

Il d.lgs. 231/2001 delinea il contenuto dei modelli di organizzazione e di gestione prevedendo che gli stessi, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, devono:

- a) individuare le attività nel cui ambito possono essere commessi reati;
- b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;
- c) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;

- d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Si rileva, inoltre, che ai sensi dell'art. 30 del d.lgs. 81/2008 (c.d. Testo Unico della sicurezza, di seguito anche "TUS") il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa ex d.lgs. 231/2001 deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli 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.

Il modello deve, altresì, prevedere:

- idonei sistemi di registrazione dell'avvenuta effettuazione delle attività sopra elencate;
- per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- 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 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.

Il comma 5 del citato art. 30 stabilisce, inoltre, che: *“In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti (...)”*.

Infine, di particolare rilevanza risulta la modifica dell'art. 51 TUS da parte dell'art. 30, comma 1, lettera a), del d.lgs. 3 agosto 2009, n. 106, recante *“Disposizioni integrative e correttive del decreto legislativo 9 aprile 2008, n. 81, in materia di tutela della salute e della sicurezza nei luoghi di lavoro”*, il quale, con l'introduzione del comma 3-bis, ha previsto la possibilità per le imprese di richiedere l'asseverazione dell'adozione e dell'efficace attuazione dei modelli di organizzazione e gestione della salute e sicurezza sul lavoro da parte di organismi paritetici costituiti a iniziativa di

una o più associazioni dei datori e dei prestatori di lavoro comparativamente più rappresentative sul piano nazionale.

Sindacato di idoneità.

Per accertare la responsabilità della società, il giudice penale verifica la sussistenza del reato presupposto per la responsabilità della società ed effettua un sindacato di idoneità sui modelli organizzativi adottati.

In sostanza, va giudicato “idoneo a prevenire i reati” il modello organizzativo che, prima della commissione del reato, potesse e dovesse essere ritenuto tale da azzerare o, almeno, minimizzare, con ragionevole certezza, il rischio della commissione del reato successivamente verificatosi.

Il Modello di organizzazione, gestione e controllo ex d.lgs. 231/2001 di UBI Banca.

Unione di Banche Italiane Società Cooperativa per azioni (di seguito indicata anche come “UBI Banca”, la “Banca” o la “Società”) ha adottato un proprio modello di organizzazione, gestione e controllo conforme ai requisiti previsti dal d.lgs. 231/2001 (di seguito, il “Modello”) e coerente con il contesto normativo e regolamentare di riferimento, con i principi già radicati nella propria cultura di *governance* e con le indicazioni contenute nelle *Linee guida dell’Associazione Bancaria Italiana per l’adozione di modelli organizzativi sulla responsabilità amministrativa delle banche* (di seguito, “Linee guida ABI”).

Il Modello di UBI Banca rappresenta un insieme coerente di principi, procedure e disposizioni che: i) incidono sul funzionamento interno della Banca e sulle modalità con le quali la stessa si rapporta con l’esterno e ii) regolano la diligente gestione di un sistema di controllo delle attività sensibili, finalizzato a prevenire la commissione, o la tentata commissione, dei reati (e degli illeciti amministrativi) rilevanti ai fini della responsabilità amministrativa degli enti.

Il Modello è rappresentato nel “*Documento descrittivo del modello di organizzazione, gestione e controllo di UBI Banca S.C.p.A.*”, approvato dal Consiglio di Gestione e dal Consiglio di Sorveglianza di UBI Banca, il quale è suddiviso in due parti le quali contengono, rispettivamente:

- (i) nella parte generale, una descrizione relativa:
 - al quadro normativo di riferimento;
 - alla realtà aziendale (sistema di *governance* e assetto organizzativo di UBI Banca);
 - alla struttura del Modello e alla metodologia scelta per la definizione e l’aggiornamento dello stesso;
 - alla individuazione e nomina dell’organismo di vigilanza di UBI Banca, con specificazione di poteri, compiti e flussi informativi che lo riguardano;
 - alla funzione del sistema disciplinare e al relativo apparato sanzionatorio;
 - al piano di formazione e comunicazione da adottare al fine di garantire la conoscenza delle misure e delle disposizioni del Modello;
 - ai criteri di aggiornamento del Modello;
- (ii) nella parte speciale, una descrizione relativa:
 - alle fattispecie di reato (e di illecito amministrativo) rilevanti ai fini della responsabilità amministrativa degli enti che la Banca ha stabilito di prendere in considerazione in ragione delle caratteristiche della propria attività;
 - ai processi/attività sensibili e relativi protocolli di controllo.

La documentazione di cui UBI Banca si è dotata per rappresentare il proprio assetto organizzativo e per disciplinare il proprio operato anche in relazione alle attività sensibili ai fini del modello di organizzazione, gestione e controllo *ex d.lgs. 231/2001* include:

- il Codice Etico, che definisce principi etici generali e di condotta nelle relazioni con gli Stakeholder che ispirano lo stile di gestione della banca, approvato dal Consiglio di Gestione e dal Consiglio di Sorveglianza rispettivamente in data 14/12/2010 e 13/12/2010;
- il Regolamento di Gruppo, che definisce i rapporti tra gli Organi collegiali e l’Alta Direzione della Capogruppo con gli Organi collegiali e l’Alta Direzione delle società che fanno parte del Gruppo stesso approvato dal Consiglio di Gestione e dal Consiglio di Sorveglianza rispettivamente in data 27/10/2009 e 4/11/2009;
- il Regolamento Generale Aziendale, che definisce l’interazione degli Organi collegiali con le strutture della Capogruppo approvato dal Consiglio di Gestione e dal Consiglio di Sorveglianza rispettivamente in data 27/10/2009 e 4/11/2009;
- la Normativa interna, che integra le normative vigenti relative agli intermediari bancari e finanziari.

Il Codice Etico, che costituisce parte integrante del Modello, definisce le modalità con cui UBI Banca e le società del Gruppo intendono perseguire la propria missione e rapportarsi con i diversi Stakeholder improntando le attività gestionali ed operative al rispetto delle obbligazioni morali e legali nei confronti della collettività, descrivendo i principi etici generali, i principi di condotta nelle relazioni con gli Stakeholder e le conseguenti modalità di attuazione e controllo.

L’organismo di vigilanza di UBI Banca.

In base alle previsioni del d.lgs. 231/2001, l’ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti qualificati *ex art. 5 del d.lgs. 231/2001*, se l’organo dirigente ha, fra l’altro:

- adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- 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.

L’affidamento dei suddetti compiti ad un organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi rappresentano, quindi, presupposti indispensabili per l’esonero dalla responsabilità dell’ente prevista dal d.lgs. 231/2001.

Il d.lgs. 231/2001 non fornisce indicazioni circa la composizione dell’organismo di vigilanza. In assenza di tali indicazioni, UBI Banca ha optato per una soluzione che, tenuto conto delle finalità perseguite dalla legge e delle indicazioni delle associazioni di categoria maggiormente rappresentative (tra le quali *in primis* l’ABI), è in grado di assicurare, in relazione alle proprie dimensioni e alla propria complessità organizzativa, l’effettività dei controlli cui l’organismo di vigilanza è preposto, identificando il proprio organismo di vigilanza (di seguito, “Organismo di Vigilanza”) in un organismo collegiale composto da:

- due componenti del Consiglio di Gestione, di cui uno munito dei requisiti di indipendenza ai sensi dell’art. 147-quater TUF e l’altro esponente del Consiglio di Gestione non esecutivo ;
- il Responsabile dell’Area Affari Legali e Contenzioso;

- il Responsabile dell'Area *Compliance*;
- un professionista esterno.

Principi generali in tema di istituzione e nomina dell'Organismo di Vigilanza.

L'Organismo di Vigilanza di UBI Banca è istituito con delibera del Consiglio di Gestione, sentito il Consiglio di Sorveglianza; i suoi membri decadono in concomitanza della cessazione del Consiglio di Gestione che li ha nominati e sono rieleggibili.

In caso di decadenza, l'Organismo di Vigilanza continua a svolgere *ad interim* le proprie funzioni fino a nuova nomina dei suoi componenti.

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza di requisiti soggettivi di eleggibilità.

Il componente dell'Organismo di Vigilanza che intenda rinunciare all'incarico deve darne immediatamente notizia agli altri componenti dell'Organismo di Vigilanza.

L'Organismo di Vigilanza a sua volta informa tempestivamente sia il Presidente del Consiglio di Gestione, affinché adotti gli opportuni provvedimenti, sia il Presidente del Consiglio di Sorveglianza.

La rinuncia ha effetto immediato, se rimane in carica la maggioranza dei componenti dell'Organismo di Vigilanza.

In caso di rinuncia del presidente dell'Organismo di Vigilanza, la presidenza è assunta fino alla successiva riunione dell'Organismo medesimo dal componente più anziano.

In caso di cessazione, a qualsiasi titolo, di un componente dell'Organismo di Vigilanza, il nuovo componente, ove nominato, scade insieme a quelli in carica all'atto della sua nomina.

In casi di particolare gravità, il Consiglio di Gestione potrà comunque disporre – informato il Consiglio di Sorveglianza – la sospensione dei poteri dell'Organismo di Vigilanza e la nomina di un Organismo *ad interim*.

Funzioni e poteri dell'Organismo di Vigilanza.

Le regole operative di funzionamento dell'Organismo di Vigilanza sono previste nel Regolamento dello stesso che è parte integrante del Modello.

Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura della Banca, fermo restando però che l'organo dirigente è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo operato, in quanto è all'organo dirigente che risale la responsabilità ultima del funzionamento e dell'efficacia del Modello.

All'Organismo di Vigilanza sono conferiti i seguenti compiti e poteri di iniziativa e controllo necessari per assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello secondo quanto stabilito dall'art. 6 del d.lgs. 231/2001:

- verificare la persistenza nel tempo dei requisiti di efficienza ed efficacia del Modello;
- curare, sviluppare e promuovere il costante aggiornamento del Modello, identificando e segnalando all'organo dirigente l'esigenza di eventuali aggiornamenti da realizzarsi mediante le modifiche e/o le integrazioni che si dovessero rendere necessarie, a titolo esemplificativo, in conseguenza di: i) significative violazioni delle prescrizioni del Modello; ii) significative modificazioni dell'assetto interno della Banca e/o delle modalità di svolgimento delle attività d'impresa; iii) modifiche normative;
- assicurare il periodico aggiornamento del sistema di identificazione, mappatura e classificazione delle attività sensibili;

- mantenere un collegamento costante con la società di revisione, salvaguardandone la necessaria indipendenza, e con gli altri consulenti e collaboratori coinvolti nelle attività di efficace attuazione del Modello;
- rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall’analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni;
- segnalare tempestivamente all’organo dirigente, per gli opportuni provvedimenti, le violazioni accertate del Modello che possano comportare l’insorgere di una responsabilità in capo alla Banca;
- curare i rapporti e assicurare i flussi informativi di competenza verso il Consiglio di Gestione, nonché verso il Consiglio di Sorveglianza;
- promuovere e definire le iniziative per la diffusione della conoscenza e della comprensione del Modello, nonché per la formazione del personale e la sensibilizzazione dello stesso all’osservanza dei contenuti del Modello;
- promuovere ed elaborare interventi di comunicazione e formazione sui contenuti del d.lgs. 231/2001, sugli impatti della normativa sull’attività dell’azienda e sulle norme comportamentali;
- fornire chiarimenti in merito al significato e alla applicazione delle previsioni contenute nel Modello;
- predisporre un efficace sistema di comunicazione interna per consentire la trasmissione di notizie rilevanti ai fini del d.lgs. 231/2001 garantendo la tutela e riservatezza del segnalante;
- formulare e sottoporre all’approvazione dell’organo dirigente la previsione di spesa necessaria al corretto svolgimento dei compiti assegnati. Tale previsione di spesa dovrà essere, in ogni caso, la più ampia al fine di garantire il pieno e corretto svolgimento della propria attività;
- accedere liberamente presso, ovvero convocare, qualsiasi struttura/unità organizzativa, esponente o dipendente della Banca – senza necessità di alcun consenso preventivo – per richiedere e acquisire informazioni, documentazione e dati, ritenuti necessari per lo svolgimento dei compiti previsti dal d.lgs. 231/2001, da tutto il personale dipendente e dirigente;
- richiedere informazioni rilevanti a collaboratori, consulenti, agenti, promotori finanziari e rappresentanti esterni alla Banca;
- promuovere l’attivazione di eventuali procedimenti disciplinari e proporre le eventuali sanzioni;
- verificare e valutare l’idoneità del sistema disciplinare ai sensi e per gli effetti del d.lgs. 231/2001;
- vigilare ai sensi dell’art. 52 del d.lgs. 231/2007 sull’osservanza delle norme contenute nel decreto medesimo, relativo alla prevenzione dell’utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo. In particolare, tale obbligo di vigilanza, in conformità all’interpretazione fornita dalle Linee guida ABI, *“deve essere inteso come vigilanza che ognuno degli organi richiamati dalla norma deve espletare nel proprio ambito di attività, senza necessità di produrre inutili duplicazioni di compiti ed attività”*;
- assolvere agli obblighi di comunicazione previsti dal secondo comma del sopra citato art. 52. A tale specifico fine, i soggetti incaricati di supervisione la corretta applicazione della normativa antiriciclaggio nell’ambito della Banca forniscono con regolarità all’Organismo di Vigilanza relazioni informative periodiche in merito alla propria attività nonché comunicano al medesimo tempestivamente la rilevazione di eventuali infrazioni alla normativa stessa;
- in caso di controlli, indagini, richieste di informazioni da parte di autorità competenti finalizzati a verificare la rispondenza del Modello alle previsioni del d.lgs. 231/2001, curare il rapporto con i soggetti incaricati dell’attività ispettiva, fornendo loro adeguato supporto informativo.

L'Organismo di Vigilanza può giovare – sotto la propria diretta sorveglianza e responsabilità – nello svolgimento dei compiti affidatigli, della collaborazione di tutte le funzioni e strutture della Banca ovvero di consulenti esterni, avvalendosi delle rispettive competenze e professionalità. Tale facoltà consente all'Organismo di Vigilanza di assicurare un elevato livello di professionalità e la necessaria continuità di azione.

Verifiche e controlli sul Modello.

L'Organismo di Vigilanza redige un documento descrittivo delle attività di vigilanza attraverso il quale pianifica le proprie attività prevedendo: un calendario delle attività da svolgere nel corso dell'anno, la determinazione delle scadenze temporali dei controlli, l'individuazione dei criteri e delle procedure di analisi, la possibilità di effettuare verifiche e controlli non programmati.

Nello svolgimento della propria attività, l'Organismo di Vigilanza può avvalersi sia del supporto di funzioni e strutture interne alla Banca con specifiche competenze nei settori aziendali di volta in volta sottoposti a controllo sia, con riferimento all'esecuzione delle operazioni tecniche necessarie per lo svolgimento della funzione di controllo, di consulenti esterni.

All'Organismo di Vigilanza sono riconosciuti, nel corso delle verifiche ed ispezioni, i più ampi poteri al fine di svolgere efficacemente i compiti affidatigli.

Obblighi di informazione nei confronti dell'Organismo di Vigilanza – Flussi informativi.

L'Organismo di Vigilanza deve essere tempestivamente informato, mediante apposito sistema di comunicazione interna, in merito a quegli atti, comportamenti od eventi che possono determinare una violazione del Modello o che, più in generale, sono rilevanti ai fini del d.lgs. 231/2001.

Valgono, in proposito, le seguenti prescrizioni di carattere generale:

- devono essere raccolte eventuali segnalazioni relative: i) alla commissione, o al ragionevole pericolo di commissione, dei reati (e degli illeciti amministrativi) rilevanti ai fini della responsabilità amministrativa degli enti; ii) a “pratiche” non in linea con le norme di comportamento emanate dalla Banca; iii) a comportamenti che, in ogni caso, possono determinare una violazione del Modello;
- ogni Responsabile di Unità Organizzativa, cui è attribuita la responsabilità di coordinamento delle strutture di riferimento, deve segnalare formalmente e tempestivamente all'Organismo di Vigilanza eventuali comportamenti difformi al Modello;
- il dipendente, gli agenti, i *partner* commerciali, i consulenti, i collaboratori, i promotori finanziari, i c.d. parasubordinati, e in generale tutti gli *stakeholder*, per quanto riguarda i rapporti con UBI Banca e l'attività svolta nei confronti di UBI Banca, effettuano la segnalazione di una violazione (o presunta violazione) del Modello all'Organismo di Vigilanza secondo quanto di seguito previsto;
- l'Organismo di Vigilanza valuta discrezionalmente e sotto la sua responsabilità le segnalazioni ricevute e i casi in cui è necessario attivarsi;
- nel caso in cui la segnalazione di eventuali violazioni del Modello sia riferita a componenti del Consiglio di Gestione e/o del Consiglio di Sorveglianza, la stessa verrà trasmessa anche al Presidente del Consiglio di Gestione e al Presidente del Consiglio di Sorveglianza ovvero, se riguardante il Presidente del Consiglio di Sorveglianza, al Presidente del Consiglio di Gestione e, se riguardante il Presidente del Consiglio di Gestione, al Presidente del Consiglio di Sorveglianza.

I segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione ed in ogni caso è assicurata la riservatezza dell'identità del segnalante, fatti salvi gli

obblighi di legge e la tutela dei diritti della Banca o delle persone accusate erroneamente e/o in mala fede.

In aggiunta alle segnalazioni relative a violazioni di carattere generale sopra descritte, devono essere trasmesse all'Organismo di Vigilanza, da parte delle funzioni aziendali che operano nell'ambito di attività sensibili, le informazioni concernenti: i) le risultanze periodiche dell'attività di controllo dalle stesse poste in essere per dare attuazione al Modello (*report* riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.); ii) le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non rilevante se singolarmente considerato, potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento).

Invio delle segnalazioni - Raccolta e conservazione delle informazioni.

Le segnalazioni possono essere inviate, per iscritto e in forma non anonima con le seguenti modalità:

- **e-mail:** Organismo.di.Vigilanza.231@ubibanca.it
- **lettera all'indirizzo:** Unione di Banche Italiane Soc. coop. per azioni
Organismo di Vigilanza 231
Piazza Vittorio Veneto, 8
24122 – Bergamo

Ogni informazione, segnalazione, *report*, relazione prevista nel Modello è conservata dall'Organismo di Vigilanza in un apposito archivio (informatico o cartaceo).

Reporting dell'Organismo di Vigilanza verso gli organi societari.

L'Organismo di Vigilanza riferisce in merito all'attuazione del Modello, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi.

Sono previste due distinte linee di *reporting*:

- la prima, su base continuativa, direttamente verso il Consigliere delegato e il Direttore generale;
- la seconda, su base periodica, nei confronti del Consiglio di Gestione e del Consiglio di Sorveglianza.

Sistema disciplinare.

Funzione del sistema disciplinare.

La definizione di un adeguato sistema disciplinare costituisce un presupposto essenziale della valenza scriminante del modello di organizzazione, gestione e controllo *ex d.lgs. 231/2001* rispetto alla responsabilità amministrativa degli enti.

Misure nei confronti di lavoratori subordinati.

L'osservanza delle disposizioni e delle regole comportamentali previste dal Modello costituisce adempimento da parte dei dipendenti di UBI Banca degli obblighi previsti dall'art. 2104, comma 2, del codice civile; obblighi dei quali il contenuto del medesimo Modello rappresenta parte sostanziale ed integrante.

La violazione delle singole disposizioni e regole comportamentali di cui al Modello da parte dei dipendenti di UBI Banca costituisce sempre illecito disciplinare.

Le misure indicate nel Modello, il cui mancato rispetto si intende sanzionare, sono comunicate mediante circolare interna a tutti i dipendenti, affisse in luogo accessibile a tutti e vincolanti per tutti i dipendenti della Banca.

I provvedimenti disciplinari sono irrogabili nei confronti dei lavoratori dipendenti di UBI Banca, conformemente a quanto previsto dall'art. 7 della legge 20 maggio 1970, n. 300 (c.d. "Statuto dei Lavoratori") ed eventuali normative speciali applicabili.

Per quanto riguarda le sanzioni derivanti dalla violazione delle prescrizioni del Modello, trovano applicazione i principi e le regole generali previste nel Codice Disciplinare già emanato da UBI Banca e diffuso con le medesime forme e modalità sopra descritte.

Per i dipendenti di livello non dirigenziale, tali provvedimenti sono quelli previsti dalle norme disciplinari di cui al Contratto Collettivo Nazionale di Lavoro di riferimento.

Ad ogni notizia di violazione del Modello, verrà promossa un'azione disciplinare finalizzata all'accertamento della violazione stessa. Per quanto concerne l'accertamento delle infrazioni, i procedimenti disciplinari e la comminazione delle sanzioni restano validi i poteri già conferiti, nei limiti delle rispettive deleghe e competenze, al *management* di UBI Banca.

Si precisa comunque che, dovrà essere comunicato ogni atto relativo al procedimento all'Organismo di Vigilanza per la valutazione di competenza.

E' fatta salva la prerogativa di UBI Banca di chiedere il risarcimento dei danni derivanti dalla violazione del Modello da parte di un dipendente.

In caso di violazione delle disposizioni e delle regole comportamentali contenute nel Modello da parte di dirigenti, UBI Banca una volta accertata la responsabilità dell'autore della violazione, adotta la misura ritenuta più idonea. Se la violazione del Modello determina la sopravvenuta carenza del rapporto di fiducia tra la Banca e il dirigente, la sanzione è individuata nel licenziamento per giusta causa.

Misure nei confronti dei componenti del Consiglio di Gestione e del Consiglio di Sorveglianza.

Apposite misure sanzionatorie sono previste in caso di violazioni delle disposizioni e delle regole di comportamento del Modello da parte di componenti del Consiglio di Gestione e del Consiglio di Sorveglianza.

Misure nei confronti di partner commerciali, agenti, promotori finanziari, consulenti, collaboratori.

La violazione da parte di *partner* commerciali, agenti, promotori finanziari, consulenti, collaboratori esterni o altri soggetti aventi rapporti contrattuali con la Banca delle disposizioni e delle regole di comportamento previste dal Modello agli stessi applicabili, o l'eventuale commissione dei reati (e degli illeciti amministrativi) rilevanti ai fini della responsabilità amministrativa degli enti da parte degli stessi, sarà sanzionata secondo quanto previsto nelle specifiche clausole contrattuali che saranno inserite nei relativi contratti.

Resta ovviamente salva la prerogativa di UBI Banca di richiedere il risarcimento dei danni derivanti dalla violazione delle disposizioni e delle regole di comportamento previste dal Modello da parte dei suddetti soggetti terzi.

Formazione e comunicazione.

Premessa.

UBI Banca, al fine di dare efficace attuazione al Modello, intende assicurare una corretta divulgazione dei contenuti dello stesso all'interno e all'esterno della propria organizzazione.

In particolare, obiettivo di UBI Banca è estendere la comunicazione dei contenuti del Modello non solo ai propri dipendenti ma anche ai soggetti che, pur non rivestendo la qualifica formale di dipendente, operano – anche occasionalmente – per il conseguimento degli obiettivi di UBI Banca in forza di rapporti contrattuali.

L'attività di comunicazione e formazione, diversificata a seconda dei destinatari cui essa si rivolge, è, in ogni caso, improntata a principi di completezza, chiarezza, accessibilità e continuità al fine di consentire ai diversi destinatari la piena consapevolezza di quelle disposizioni aziendali che sono tenuti a rispettare e delle norme etiche che devono ispirare i loro comportamenti.

L'attività di comunicazione e formazione è supervisionata ed integrata dall'Organismo di Vigilanza.

Dipendenti e componenti degli organi sociali.

Ogni dipendente è tenuto a: i) acquisire consapevolezza dei contenuti del Modello; ii) conoscere le modalità operative con le quali deve essere realizzata la propria attività; iii) contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del Modello, segnalando eventuali carenze riscontrate nello stesso.

Al fine di garantire un'efficace e razionale attività di comunicazione, UBI Banca promuove e agevola la conoscenza dei contenuti del Modello da parte dei dipendenti, con grado di approfondimento diversificato a seconda del grado di coinvolgimento nelle attività individuate come sensibili ai sensi del d.lgs. 231/2001.

È garantita ai dipendenti la possibilità di accedere e consultare la documentazione costituente il Modello (Documento descrittivo del Modello, Codice Etico, informazioni sulle strutture organizzative della Banca, sulle attività e sulle procedure aziendali) anche direttamente sull'*Intranet* aziendale. Inoltre, al fine di agevolare la comprensione del Modello, i dipendenti, con modalità diversificate secondo il loro grado di coinvolgimento nelle attività individuate come sensibili ai sensi del d.lgs. 231/2001, sono tenuti a partecipare ad una specifica attività formativa.

Ai nuovi dipendenti verrà consegnata, all'atto dell'assunzione, copia del Documento descrittivo del Modello e sarà fatta loro sottoscrivere dichiarazione di osservanza dei contenuti del Modello ivi descritti.

Ai componenti degli organi sociali di UBI Banca saranno applicate le medesime modalità di diffusione del Modello previste per i dipendenti.

Idonei strumenti di comunicazione saranno adottati per aggiornare i dipendenti circa le eventuali modifiche apportate al Modello, nonché ogni rilevante cambiamento procedurale, normativo o organizzativo.

Altri destinatari.

L'attività di comunicazione dei contenuti del Modello è indirizzata anche nei confronti di quei soggetti terzi che intrattengano con UBI Banca rapporti di collaborazione contrattualmente regolati o che rappresentano la Banca senza vincoli di dipendenza (ad esempio: *partner* commerciali, agenti, consulenti, promotori finanziari, distributori, procacciatori d'affari e altri collaboratori autonomi). A tal fine, ai soggetti terzi più significativi UBI Banca fornirà una copia del presente documento e una copia del Codice Etico. Ai terzi cui saranno consegnate le copie dei predetti documenti, verrà fatta sottoscrivere una dichiarazione che attesti il ricevimento delle stesse e l'impegno all'osservanza dei contenuti ivi descritti.

UBI Banca, tenuto conto delle finalità del Modello, valuterà l'opportunità di comunicare i contenuti del Modello stesso a terzi, non riconducibili alle figure sopra indicate a titolo esemplificativo, e più in generale al mercato.

Attività di formazione.

UBI Banca predispose, con il supporto delle funzioni aziendali preposte specifici interventi formativi rivolti a tutti i dipendenti al fine di assicurare una adeguata conoscenza, comprensione e diffusione dei contenuti del Modello e di diffondere, altresì, una cultura aziendale orientata verso il perseguimento di una sempre maggiore trasparenza ed eticità.

L'attività formativa viene erogata attraverso le seguenti modalità:

- sessioni in aula, con incontri dedicati oppure mediante l'introduzione di moduli specifici nell'ambito di altre sessioni formative, a seconda dei contenuti e dei destinatari di queste ultime, con questionari di verifica del grado di apprendimento;
- *e-learning*: attraverso un modulo relativo alla parte generale per tutti i dipendenti, con esercitazioni intermedie e test di verifica di apprendimento.

I contenuti degli interventi formativi vengono costantemente aggiornati in relazione ad eventuali interventi di aggiornamento del Modello.

La partecipazione agli interventi formativi è obbligatoria. L'Organismo di Vigilanza, per il tramite delle preposte strutture aziendali, raccoglie e archivia le evidenze/attestazioni relative all'effettiva partecipazione a detti interventi formativi.

Criteri di aggiornamento del Modello.

Aggiornamento del Modello.

All'Organismo di Vigilanza è affidato il compito di curare l'aggiornamento del Modello.

A tal fine l'Organismo di Vigilanza, anche avvalendosi del supporto delle funzioni aziendali preposte al monitoraggio delle innovazioni normative, delle modifiche organizzative e attinenti alle tipologie di attività svolte dalla Banca – e in particolare dei flussi informativi a tali fini con continuità assicurati in favore dell'Organismo rispettivamente dalle funzioni Area Affari Legali e Contenzioso, Area *Compliance* e Area Organizzazione – identifica e segnala al Consiglio di Gestione l'esigenza di procedere all'aggiornamento del Modello, fornendo altresì indicazioni in merito alle modalità secondo cui procedere alla realizzazione dei relativi interventi.

Il Consiglio di Gestione valuta l'esigenza di aggiornamento del Modello segnalata dall'Organismo di Vigilanza e, sentito il Consiglio di Sorveglianza, delibera in merito all'aggiornamento del Modello in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza di:

- modifiche normative in tema di responsabilità amministrativa degli enti e significative innovazioni nell'interpretazione delle disposizioni in materia;
- identificazione di nuove attività sensibili, o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività d'impresa, modificazioni dell'assetto interno della Banca e/o delle modalità di svolgimento delle attività d'impresa;
- emanazione e modifica di linee guida da parte dell'associazione di categoria di riferimento comunicate al Ministero della Giustizia a norma dell'art. 6 del d.lgs. 231/2001 e degli artt. 5 e ss. del D.M. 26 giugno 2003, n. 201;
- commissione dei reati (e degli illeciti amministrativi) rilevanti ai fini della responsabilità amministrativa degli enti da parte dei destinatari delle previsioni del Modello o, più in generale, di significative violazioni del Modello;
- riscontro di carenze e/o lacune nelle previsioni del Modello a seguito di verifiche sull'efficacia del medesimo.

Elementi di Sintesi del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 di UBI Banca S.C.p.A. approvato dal Consiglio di Gestione e dal Consiglio di Sorveglianza rispettivamente in data 25 gennaio e 25 febbraio 2011

Contestualmente all'assunzione delle proprie delibere attinenti allo svolgimento di attività di aggiornamento del Modello, il Consiglio di Gestione identifica le funzioni aziendali che saranno tenute ad occuparsi della realizzazione e attuazione dei predetti interventi di aggiornamento e le correlate modalità degli stessi, autorizzando l'avvio di un apposito progetto.

Le funzioni incaricate realizzano gli interventi deliberati secondo le istruzioni ricevute e, previa informativa all'Organismo di Vigilanza, sottopongono all'approvazione del Consiglio di Gestione le proposte di aggiornamento del Modello scaturenti dagli esiti del relativo progetto.

Il Consiglio di Gestione, sentito il Consiglio di Sorveglianza, approva gli esiti del progetto, dispone l'aggiornamento del Modello e identifica le funzioni aziendali che saranno tenute ad occuparsi dell'attuazione delle modifiche/integrazioni derivanti dagli esiti del progetto medesimo e della diffusione dei relativi contenuti all'interno e all'esterno della Banca.

L'approvazione dell'aggiornamento del Modello viene immediatamente comunicata all'Organismo di Vigilanza, il quale, a sua volta, vigila sulla corretta attuazione e diffusione degli aggiornamenti operati.

L'Organismo di Vigilanza provvede, altresì, mediante apposita relazione, a informare il Consiglio di Gestione circa l'esito dell'attività di vigilanza intrapresa in ottemperanza alla delibera che dispone l'aggiornamento del Modello.

Il Modello è, in ogni caso, sottoposto a procedimento di revisione periodica con cadenza triennale da disporsi mediante delibera del Consiglio di Gestione.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai reati nei confronti della pubblica amministrazione.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dagli articoli 24 e 25 del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati nei confronti della pubblica amministrazione:

1. negoziazione, stipulazione ed esecuzione di contratti/convenzioni con Soggetti Pubblici mediante procedure negoziate (affidamento diretto o trattativa privata) o ad evidenza pubblica (aperte o ristrette);
2. attività svolte dalla Banca in qualità di incaricato di pubblico servizio (es. gestione del servizio di tesoreria per Enti Pubblici; gestione delle deleghe fiscali; distribuzione di titoli del debito pubblico);
3. gestione dei procedimenti istruttori, delle attività di erogazione e delle connesse formalità amministrative relative alla erogazione di finanziamenti che godono di contributi pubblici;
4. gestione dei rapporti con Soggetti Pubblici relativi a diritti sugli immobili (Conservatoria e Catasto);
5. gestione dei rapporti con Soggetti Pubblici – incluse le Autorità Pubbliche di Vigilanza (es. Banca d'Italia; UIF; Consob; Autorità Garante per la Concorrenza e il Mercato; Autorità per l'Energia Elettrica ed il Gas; Autorità garante per le comunicazioni; Isvap; Covip; Ministeri; Autorità Garante per la protezione dei dati personali) – che operino quali pubbliche autorità con riferimento a determinate aree di competenza. Adempimenti ed ispezioni;
6. gestione dei rapporti con Soggetti Pubblici per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali;

7. assunzione di personale, ivi inclusa l'assunzione di soggetti appartenenti alla categorie protette o la cui assunzione è agevolata. Rapporti con Enti previdenziali e assistenziali;
8. rapporti con autorità inquirenti (Carabinieri, Polizia di Stato, Polizia Municipale, Guardia di Finanza);
9. promozioni commerciali e sponsorizzazioni ad Enti Pubblici;
10. gestione dei rapporti con l'amministrazione finanziaria;
11. acquisizione e/o gestione di contributi/sovvenzioni/finanziamenti concessi da Enti Pubblici a favore della Società;
12. gestione dei contenziosi giudiziali e stragiudiziali (es. civili, tributari, giuslavoristici, amministrativi, penali, ecc.), nomina dei legali e coordinamento delle loro attività;
13. gestione del contenzioso relativo al recupero crediti, nomina dei legali e coordinamento delle loro attività;
14. gestione di *software* di Enti Pubblici o forniti da terzi per conto di Enti Pubblici e collegamenti telematici (in entrata e in uscita) o trasmissione di dati su supporti informatici a Enti Pubblici;
15. rapporti con mandatari, agenti, promotori finanziari e intermediari (selezione, instaurazione e regolamento del rapporto, determinazione del compenso, gestione e scioglimento del rapporto);
16. poteri di firma nell'ambito della gestione delle risorse finanziarie.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare un'attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-bis del d.lgs. 231/2001. Qui di seguito è indicata l'attività identificata come sensibile o a rischio con riferimento ai reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.:

1. ogni possibilità di detenere, maneggiare o utilizzare denaro/valori di bollo. Disponibilità di fondi.
2. ideazione, riproduzione, realizzazione o utilizzo a fini commerciali o industriali di marchi, segni distintivi, brevetti, disegni o modelli industriali;
3. introduzione nel territorio dello Stato, detenzione per la vendita o messa in circolazione sul mercato dei consumatori di opere dell'ingegno o prodotti industriali con marchi o segni distintivi nazionali o esteri.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai reati societari.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-ter del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati societari:

1. redazione del bilancio, delle relazioni e delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico e osservanza degli adempimenti introdotti dalla legge 262/2005 in materia di documenti contabili societari;
2. predisposizione di prospetti richiesti per l'offerta al pubblico di prodotti finanziari, e/o ammissione alla quotazione nei mercati regolamentati o documenti da pubblicare in occasione

delle offerte pubbliche di acquisto, di vendita o di scambio o altri prospetti assimilabili (opa, opv, ops);

3. gestione dei rapporti con Consiglio di Sorveglianza, società di revisione e soci. Redazione, tenuta e conservazione dei documenti su cui gli stessi potrebbero esercitare il controllo;
4. operazioni su azioni e quote proprie, operazioni sul capitale e destinazione degli utili;
5. attività di preparazione delle riunioni assembleari, svolgimento e verbalizzazione delle assemblee;
6. comunicazioni alle Autorità preposte alla vigilanza sul settore bancario e alle altre Autorità di vigilanza e gestione dei rapporti con le stesse;
7. comunicazione del conflitto di interessi ai sensi dell'art. 2391, comma 1, c.c.;
8. liquidazione di società;
9. gestione delle transazioni infragruppo.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai delitti con finalità di terrorismo o di eversione dell'ordine democratico.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-*quater* del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai delitti con finalità di terrorismo o di eversione dell'ordine democratico:

1. autorizzazione ed esecuzione di servizi e attività bancarie, finanziarie e/o di investimento come definite nel D.Lgs. 385/1993 (TUB) e nel D.Lgs. 58/1998 (TUF), e relative norme di attuazione;
2. autorizzazione ed esecuzione dell'attività di intermediazione assicurativa ai sensi del D.Lgs. 109/2005 e dei successivi Regolamenti attuativi emanati dall'ISVAP;
3. gestione di investimenti diversi dai servizi bancari e finanziari (quali ad es. acquisizioni di partecipazioni o aziende, accordi strategici, altre operazioni di finanza straordinaria);
4. negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio;
5. gestione dei procedimenti istruttori, delle attività di erogazione e delle connesse formalità amministrative relative alla concessione di agevolazioni finanziarie;
6. realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà in favore, in particolare, di enti con sede od operanti in Paesi considerati a rischio;
7. gestione del processo di approvvigionamento;
8. operazioni di *back-to-back* e rapporti di corrispondenza con banche estere;
9. selezione dei *partner* commerciali/finanziari e gestione dei relativi rapporti;
10. attività di selezione e formazione al fine della corretta applicazione delle disposizioni del d.lgs. 231/2007;
11. gestione di *server* della Società o di siti *Internet*;
12. assunzione di personale;
13. locazione di immobili.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai reati contro la personalità individuale.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-*quinquies* del d.lgs. 231/2001. Qui di seguito vengono indicate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati contro la personalità individuale:

1. concessione di garanzie e finanziamenti;
2. attività che prevedono il ricorso diretto o indiretto a manodopera (es.: affidamenti di appalti);
3. realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà;
4. gestione di *server* della Società o di siti *Internet*;
5. organizzazione/promozione di viaggi (es.: viaggi premio) per dipendenti o *partner* commerciali (es.: agenti, gestori, ecc.);
6. attività che prevedono il ricorso a prestazioni di servizi forniti da agenzie specializzate o *tour operator*.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento al reato di agiotaggio e ai reati (ed illeciti amministrativi) di abuso di informazioni privilegiate e di manipolazione del mercato.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente essere realizzati il reato di agiotaggio, le fattispecie di reato richiamate dall'articolo 25-*sexies* del d.lgs. 231/2001 e gli illeciti amministrativi richiamati dall'art. 187-*quinquies* del d.lgs. 58/1998. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento al reato di agiotaggio e ai reati (ed illeciti amministrativi) di abuso di informazioni privilegiate e di manipolazione del mercato:

1. emissione di comunicati tramite *media* (ad es.: stampa, sito *internet*, ecc.) informativa al mercato e rapporti con analisti e società di *rating*;
2. operazioni su strumenti finanziari;
3. gestione delle informazioni privilegiate.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai reati transnazionali.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente essere realizzate le fattispecie di reato richiamate dalla legge 146/2006. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati transnazionali:

1. autorizzazione ed esecuzione in riferimento ad attività transnazionali di servizi e attività bancarie, finanziarie e/o di investimento come definite nel D.Lgs. 385/1993 (TUB) e nel D.Lgs. 58/1998 (TUF), e relative norme di attuazione;
2. autorizzazione ed esecuzione in riferimento ad attività transnazionali dell'attività di intermediazione assicurativa ai sensi del D.Lgs. 109/2005 e dei successivi Regolamenti attuativi emanati dall'ISVAP;
3. gestione di investimenti diversi dai servizi bancari e finanziari in relazione ad attività transnazionali (quali ad es. acquisizioni di partecipazioni o aziende, accordi strategici, altre operazioni di finanza straordinaria);
4. negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio in riferimento ad attività transnazionali;
5. gestione dei procedimenti istruttori, delle attività di erogazione e delle connesse formalità amministrative relative alla concessione di agevolazioni finanziarie in relazione ad attività transnazionali;
6. nomina di componenti degli organi sociali di società estere del Gruppo;
7. gestione dei rapporti con componenti di organi sociali, dipendenti o terzi coinvolti in procedimenti giudiziari;

8. gestione di richieste provenienti da autorità inquirenti (Carabinieri, Polizia di Stato, Guardia di Finanza);
9. gestione di attività finalizzate a consentire l'ingresso di una persona nel territorio di uno Stato;
10. locazione di immobili in riferimento ad attività transnazionali;
11. realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà in riferimento ad attività transnazionali;
12. assistenza, consulenza o altra forma di collaborazione nella costituzione, amministrazione e gestione di trust in relazione ad attività transnazionali;
13. gestione del processo di approvvigionamento in riferimento ad attività transnazionali;
14. selezione dei *partner* commerciali/finanziari e gestione dei relativi rapporti in relazione ad attività transnazionali.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai reati in materia di tutela della salute e sicurezza sul lavoro.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-septies del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati in materia di tutela della salute e sicurezza sul lavoro:

1. pianificazione e organizzazione dei ruoli e delle attività connesse alla tutela della salute, sicurezza e igiene sul lavoro;
2. sistema di deleghe di funzione in tema di salute, sicurezza e igiene sul lavoro;
3. individuazione, valutazione e gestione dei rischi in tema di salute, sicurezza e igiene sul lavoro;
4. gestione del rischio rapina;
5. attività di informazione in tema di salute, sicurezza e igiene sul lavoro;
6. attività di formazione in tema di salute, sicurezza e igiene sul lavoro;
7. rapporti con i fornitori con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro;
8. gestione degli *asset* aziendali con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro;
9. controllo e azioni correttive con riferimento alle attività connesse alla salute, sicurezza e igiene sul lavoro.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-octies del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita:

1. autorizzazione ed esecuzione di servizi e attività bancarie, finanziarie e/o di investimento come definite nel D.Lgs. 385/1993 (TUB) e nel D.Lgs. 58/1998 (TUF), e relative norme di attuazione;
2. autorizzazione ed esecuzione dell'attività di intermediazione assicurativa ai sensi del D.Lgs. 109/2005 e dei successivi Regolamenti attuativi emanati dall'ISVAP ;
3. gestione di investimenti diversi dai servizi bancari e finanziari (quali ad es. acquisizioni di partecipazioni o aziende, accordi strategici, altre operazioni di finanza straordinaria);

4. negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio;
5. gestione dei procedimenti istruttori, delle attività di erogazione e delle connesse formalità amministrative relative alla concessione di agevolazioni finanziarie;
6. realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà;
7. gestione del processo di approvvigionamento;
8. operazioni di *back-to-back* e rapporti di corrispondenza con banche estere;
9. assistenza, consulenza o altra forma di collaborazione nella costituzione, amministrazione e gestione di trust;
10. selezione dei *partner* commerciali/finanziari e gestione dei relativi rapporti;
11. attività di selezione e formazione al fine della corretta applicazione delle disposizioni del d.lgs. 231/2007;
12. gestione di *server* della Società o di siti *Internet*.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai delitti informatici e trattamento illecito di dati.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 24-*bis* del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai delitti informatici e trattamento illecito di dati:

1. definizione delle regole da adottare in materia di sicurezza del sistema informatico e telematico;
2. gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione;
3. gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni;
4. gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni, ecc.) e delle attività di inventariazione dei beni;
5. acquisizione e gestione di apparecchiature, di dispositivi (anche di rilevazione) connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione);
6. monitoraggio/verifica periodica del sistema informatico e gestione degli incidenti e dei problemi di sicurezza informatica;
7. gestione degli aspetti infrastrutturali delle transazioni *on-line*.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai delitti di criminalità organizzata.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 24-*ter* del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai delitti di criminalità organizzata:

1. autorizzazione ed esecuzione di servizi e attività bancarie, finanziarie e/o di investimento come definite nel D.Lgs. 385/1993 (TUB) e nel D.Lgs. 58/1998 (TUF), e relative norme di attuazione;
2. autorizzazione ed esecuzione dell'attività di intermediazione assicurativa ai sensi del D.Lgs. 109/2005 e dei successivi Regolamenti attuativi emanati dall'ISVAP;

3. gestione di investimenti diversi dai servizi bancari e finanziari (quali ad es. acquisizioni di partecipazioni o aziende, accordi strategici, altre operazioni di finanza straordinaria);
4. negoziazione, stipula ed esecuzione di contratti di mandato, intermediazione, consulenza, agenzia, promozione finanziaria e brokeraggio;
5. gestione dei procedimenti istruttori, delle attività di erogazione e delle connesse formalità amministrative relative alla concessione di finanziamenti anche agevolati;
6. gestione di attività finalizzate a consentire l'ingresso di una persona nel territorio di uno Stato;
7. locazione di immobili;
8. realizzazione, promozione e gestione di iniziative umanitarie e di solidarietà;
9. gestione del processo di approvvigionamento;
10. selezione dei partner commerciali/finanziari e gestione dei relativi rapporti.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai delitti contro l'industria e il commercio.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-bis.1 del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai delitti contro l'industria e il commercio:

1. partecipazione a gare;
2. organizzazione di gare;
3. gestione dei rapporti con i soggetti incaricati o esercizio diretto delle seguenti attività:
 - a) offerta sul mercato di beni o servizi;
 - b) vendita o messa in commercio di sostanze o prodotti alimentari;
 - c) vendita o messa in circolazione di opere dell'ingegno o prodotti industriali;
 - d) introduzione nel territorio dello Stato o detenzione per la messa in circolazione di oggetti o altri beni.

Le attività individuate come sensibili ai fini del d.lgs. 231/2001 in UBI Banca con riferimento ai delitti in materia di violazione dei diritti d'autore.

L'analisi dei processi aziendali di UBI Banca ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-novies del d.lgs. 231/2001.

Le seguenti attività:

- a) detenzione a qualunque titolo
- b) importazione
- c) diffusione o messa in circolazione sotto qualsiasi forma
- d) riproduzione o duplicazione
- e) utilizzo a qualunque titolo
- f) produzione
- g) modificazione del contenuto

si considerano come sensibili o a rischio con riferimento ai delitti in materia di violazione del diritto d'autore laddove riferite ad alcuno degli oggetti di seguito riportati:

- i) programmi per elaboratori
- ii) mezzi destinati a superare le barriere di protezione dei programmi medesimi
- iii) contenuto di banche dati
- iv) supporti contenenti fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento

- v) opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, anche se inserite in opere collettive o composite o banche dati
- vi) servizi criptati
- vii) dispositivi o elementi di decodificazione speciale o decodificazione di trasmissione audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale
- viii) attrezzature, prodotti o componenti ovvero servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di protezione
- ix) altre opere dell'ingegno o parti di esse o altri materiali protetti ai fini dei diritti d'autore, anche sotto forma di informazioni elettroniche.

Il sistema dei controlli.

I presidi finalizzati alla prevenzione del rischio di commissione dei reati (e degli illeciti amministrativi), rilevanti ai fini della responsabilità amministrativa degli enti, ai quali si affiancano le previsioni del Codice Etico, si articolano su due livelli di controllo:

- **protocolli generali delle attività**, che sono sempre presenti in tutte le attività sensibili prese in considerazione dal Modello;
- **protocolli specifici** che prevedono disposizioni particolari volte a disciplinare gli aspetti peculiari delle attività sensibili.

I protocolli prevedono sia disposizioni immediatamente precettive sia disposizioni che trovano invece attuazione nella normativa aziendale (es. regolamenti aziendali, procedure, circolari, ecc.).

I protocolli generali di controllo delle attività sono:

- a) **Segregazione delle attività**: l'esercizio delle attività sensibili viene realizzato in osservanza del principio di segregazione tra chi esegue, chi controlla e chi autorizza.
- b) **Norme**: la Società adotta e applica disposizioni organizzative idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività sensibile in conformità alle prescrizioni del Modello.
- c) **Poteri di firma e poteri autorizzativi**: l'esercizio di poteri di firma e poteri autorizzativi interni avviene sulla base di regole formalizzate a tal fine introdotte.
- d) **Tracciabilità**: i soggetti, le funzioni interessate e/o i sistemi informativi utilizzati assicurano l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati che supportano la formazione e l'attuazione delle decisioni della Società e le modalità di gestione delle risorse finanziarie.

I protocolli specifici sono analiticamente indicati nei 13 capitoli – ciascuno dedicato ad una categoria di reati (e di illeciti amministrativi), rilevanti ai fini della responsabilità amministrativa degli enti, che la Società ha stabilito di prendere in considerazione in ragione delle caratteristiche della propria attività – che compongono la parte speciale del Documento descrittivo del Modello.

La struttura di ogni capitolo è caratterizzata dall'associazione tra fattispecie di reato (descritte nel paragrafo 1), attività sensibili individuate dalla Società con riferimento alle predette fattispecie di reato (elencate nel paragrafo 2) e protocolli specifici (paragrafo 3).

I protocolli generali e specifici sono stati definiti utilizzando come riferimento le Linee guida ABI, le linee guida di Confindustria e quelle ad oggi pubblicate dalle principali associazioni di categoria e le *best practice* internazionali, e sono stati successivamente adottati dalla Banca con gli opportuni adattamenti operati in ragione del proprio modello di *governance* e assetto organizzativo.

In conformità a quanto specificamente prescritto dalle Linee guida ABI, il rischio di verifica dei reati e l'individuazione dei relativi protocolli volti alla prevenzione degli stessi è stata operata tenendo in considerazione la particolarità della realtà bancaria e muovendo dal conseguente assunto che, in linea generale, per talune fattispecie di illecito il rischio di verifica è, nella banca, uguale a quello di qualunque altro ente (cc.dd. "reati generali"), laddove invece per altre tipologie di fattispecie nella banca sussiste un più elevato rischio di verifica in ragione delle particolari attività svolte dalla banca stessa (cc.dd. "reati peculiari").

Sempre secondo le citate Linee guida, per talune fattispecie di reato (quali quelle relative ai fenomeni di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita), detta bipartizione assumerebbe minor rilievo ritenendosi che, per le ragioni ivi specificamente indicate, con riferimento alle imprese bancarie i reati in esame possano essere considerati sia come reati peculiari che come reati generali.

Con particolare riferimento ai reati generali, nell'accezione precedentemente indicata, si rileva che il sistema di gestione delle risorse finanziarie, oltre a essere espresso dai protocolli che danno attuazione ai principi di "tracciabilità" e "segregazione" (quest'ultimo relativamente alla separazione dei compiti e alla contrapposizione di funzioni), trova manifestazione anche nell'ambito del sistema delle deleghe, istituito dalla Banca in ossequio al protocollo "poteri di firma e poteri autorizzativi", che prevede differenziazione delle soglie di approvazione delle spese in capo a soggetti diversi e modalità di esercizio della firma sociale nell'autorizzazione di operazioni finanziarie.

I protocolli specifici relativi ai reati in materia di tutela della salute e sicurezza sul lavoro sono stati definiti, in conformità a quanto previsto dall'art. 30, comma 5, d.lgs. 81/2008, utilizzando come riferimento le linee guida UNI-INAIL per la realizzazione di un sistema di gestione della salute e sicurezza sul lavoro.

In attesa di una sezione delle Linee guida ABI (o di altre associazioni) espressamente dedicata alla materia, i protocolli specifici relativi ai delitti informatici e trattamento illecito dei dati sono stati elaborati sulla base:

- dello *standard* ISO 27001, che fornisce i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (ISMS) finalizzato ad una corretta gestione dei dati sensibili dell'azienda;
- del *framework* COBIT, che rappresenta il modello di riferimento per la gestione della *Information and Communication Technology* (ICT);
- del SAS 70, *audit standard* riconosciuto a livello internazionale per i controlli di sicurezza rivolti ai fornitori di servizi, che prevedono controlli sulle reti, ambienti informatici e relativi processi.

Detti protocolli specifici, laddove l'attività sensibile ai fini di tali delitti informatici e trattamento illecito dei dati cui sono associati sia svolta in regime di *outsourcing* da altra società del Gruppo o fornitore esterno, potranno essere recepiti nell'ambito dei contratti di servizio relativi allo svolgimento dell'attività.

Si rileva, infine, che nel caso in cui un'attività sensibile individuata dalla Società sia, in tutto o in parte, svolta da soggetti terzi in nome e/o per conto della Società, trovano applicazione – in sostituzione e/o a complemento dei protocolli specifici previsti per le singole attività sensibili – i seguenti protocolli:

- **Contratti:** per ogni attività sensibile affidata, in tutto o in parte, in *outsourcing* viene stipulato uno specifico contratto che disciplina lo svolgimento dell'attività sensibile e definisce i livelli di servizio (SLA) in modo dettagliato e analitico, in modo da delineare chiaramente le attività di competenza della Società e quelle di competenza dell'*outsourcer* e regolare le modalità secondo le quali, in conformità alle prescrizioni del Modello, l'attività sensibile deve essere eseguita da parte dell'*outsourcer*.
- **Referente:** con riferimento ad ogni attività affidata, in tutto o in parte, in *outsourcing* viene individuato, all'interno della Società, un soggetto/funzione responsabile del rispetto delle disposizioni contenute nel *Service Level Agreement* (norme contrattuali, livelli di servizio), a presidio delle responsabilità facenti capo alla Società con riferimento all'attività affidata all'esterno.
- **Clausole *ad hoc*:** nei contratti di servizio stipulati con soggetti terzi sono previsti richiami alla disciplina prevista dal Modello per lo svolgimento dell'attività sensibile e sono inserite clausole risolutive espresse volte a sanzionare comportamenti, da parte dei soggetti terzi, contrari alle previsioni contenute nel Modello.
- **Presidi di controllo:** nei contratti di servizio i soggetti terzi, cui viene affidata da parte della Società – in tutto o in parte – la gestione dell'attività, si impegnano a dotarsi di misure idonee a prevenire il rischio di commissione dei reati e degli illeciti amministrativi rilevanti ai fini della responsabilità amministrativa *ex* d.lgs. 231/2001 che potrebbero essere ascritti alla Società.