

2014



Modello di Organizzazione, Gestione e Controllo

(ai sensi del D.Lgs. 231/2001)



Sommario

| | |
|---|----|
| Parte generale | 8 |
| 1 Introduzione..... | 9 |
| 1.1 Definizioni..... | 9 |
| 1.2 La normativa di riferimento: il D.Lgs. 231/2001 e le fonti internazionali..... | 11 |
| 1.3 I presupposti della responsabilità degli enti, la funzione del MOG e il profilo Sanzionatorio..... | 11 |
| 1.4 Presupposti di esclusione della responsabilità dell'ente..... | 12 |
| 1.5 I riflessi del nuovo profilo di responsabilità penale delle imprese sul mondo assicurativo e bancario | 13 |
| 2 Il Modello di organizzazione e gestione | 14 |
| 2.1 Le aree di operatività del Gruppo | 14 |
| 2.2 Funzione, principi ispiratori e struttura del modello | 14 |
| 2.3 Approccio metodologico..... | 15 |
| 2.3.1 Fase preliminare | 16 |
| 2.3.2 Fase di mappatura rischi e controlli | 16 |
| 2.3.3 Fase di valutazione rischi e controlli | 16 |
| 2.3.4 La procedura di adozione, di modifica ed integrazione del modello..... | 17 |
| 3 Le deleghe e i poteri..... | 17 |
| 4 Principi di comportamento generali per i destinatari | 18 |
| 5 La diffusione del modello organizzativo tra i portatori di interesse | 19 |
| 5.1 Informativa e formazione per dipendenti e dirigenti | 19 |
| 5.2 Informativa e formazione per i collaboratori..... | 20 |
| 6 L'organismo di Vigilanza..... | 20 |
| 6.1 L'Organismo di Vigilanza come previsto dal D.Lgs. 231/01 | 20 |
| 6.2 I requisiti dell'Organismo di Vigilanza..... | 21 |
| 6.3 Le regole di funzionamento dell'Organismo di Vigilanza e le situazioni di Incompatibilità..... | 22 |
| 6.3.1 Rapporti tra l'Organismo di Vigilanza e gli organi sociali..... | 22 |
| 6.3.2 Coordinamento tra gli OdV del Gruppo | 22 |
| 6.3.3 Coordinamento tra gli organismi di vigilanza delle Società del Gruppo Bancario | 23 |
| 6.3.4 Flussi informativi nei confronti dell'Organismo di Vigilanza | 23 |
| 6.3.5 Cause d'incompatibilità | 23 |
| 6.4 Nomina e composizione dell'Organismo di Vigilanza..... | 24 |
| 7 Il sistema disciplinare e sanzionatorio | 25 |

CRED.IT SOCIETÀ FINANZIARIA SPA

| | | |
|--|---|----|
| 7.1 | Funzioni del sistema disciplinare..... | 25 |
| 7.2 | Procedimento e misure disciplinari | 25 |
| 7.2.1 | Dipendenti | 25 |
| 7.2.2 | Membri del Consiglio di Amministrazione e Sindaci..... | 26 |
| 7.2.3 | Collaboratori | 26 |
| 7.3 | Segnalazioni verso l'Organismo di Vigilanza | 26 |
| 8 | I reati ex D. Lgs. 231/2001 in CRED.IT SOCIETÀ FINANZIARIA SPA | 27 |
| Parte speciale 1 Reati societari..... | | 29 |
| 1 | Funzione della Parte Speciale prima..... | 30 |
| 2 | I reati societari..... | 30 |
| 2.1 | Falsità in comunicazioni, prospetti e relazioni | 30 |
| 2.2 | Tutela penale del capitale sociale | 31 |
| 2.3 | Tutela penale del funzionamento della società | 31 |
| 2.4 | Tutela penale delle funzioni di vigilanza | 31 |
| 3 | Attività sensibili nell'ambito dei reati societari | 32 |
| 4 | I presidi e gli strumenti di controllo | 32 |
| 4.1 | Premessa | 32 |
| 4.2 | Principi di comportamento | 33 |
| 4.2.1 | Falsità in comunicazioni, prospetti e relazioni | 33 |
| 4.2.2 | Tutela penale del capitale sociale | 33 |
| 4.2.3 | Tutela penale del funzionamento della società | 34 |
| 4.2.4 | Tutela penale delle funzioni di vigilanza..... | 34 |
| 4.3 | Principi di controllo..... | 34 |
| 4.3.1 | Falsità in comunicazioni, prospetti e relazioni | 34 |
| 4.3.2 | Tutela penale del capitale sociale | 36 |
| 4.3.3 | Tutela penale del funzionamento della società | 36 |
| 4.3.4 | Tutela penale delle funzioni di vigilanza..... | 37 |
| Parte speciale 2: Reati contro la Pubblica Amministrazione | | 38 |
| 1 | Funzione della Parte Speciale seconda..... | 39 |
| 1.1 | Definizione di Pubblica Amministrazione e di soggetti incaricati di Pubblico Servizio | 39 |
| 2 | I reati contro la Pubblica Amministrazione | 40 |
| 2.1 | Malversazione a danno dello Stato | 40 |
| 2.2 | Indebita percezione di erogazioni a danno dello Stato | 40 |
| 2.3 | Corruzione e concussione | 41 |

| | |
|--|----|
| 2.4 Corruzione in atti giudiziari | 42 |
| 2.5 Truffa in danno dello Stato o di altro ente pubblico | 42 |
| 3 Attività sensibili nell'ambito dei reati contro la Pubblica Amministrazione..... | 42 |
| 4 I presidi e gli strumenti di controllo | 43 |
| 4.1 Premessa | 43 |
| 4.2 Principi di comportamento | 43 |
| 4.2.1 Malversazione a danno dello Stato..... | 44 |
| 4.2.2 Indebita percezione di erogazioni a danno dello Stato | 44 |
| 4.2.3 Corruzione e concussione di funzionari pubblici o di persone incaricate di pubblico Servizio..... | 44 |
| 4.2.4 Corruzione in atti giudiziari | 44 |
| 4.2.5 Truffa in danno dello Stato o di altro ente pubblico | 44 |
| 4.3 Principi di controllo..... | 45 |
| 4.3.1 Malversazione a danno dello Stato ed indebita percezione di erogazioni a danno dello Stato..... | 45 |
| 4.3.2 Concussione e corruzione di funzionari pubblici e truffa in danno dello Stato..... | 46 |
| 4.3.3 Corruzione in atti giudiziari | 47 |
| Parte speciale 3: Reati di market Abuse e Aggiotaggio | 49 |
| 1 Funzione della Parte Speciale terza..... | 50 |
| 2 I reati di Market Abuse e di aggioaggio..... | 50 |
| 2.1 Abuso di informazioni privilegiate | 50 |
| 2.2 Manipolazione del mercato ed aggioaggio | 51 |
| 3 Attività sensibili nell'ambito dei reati di market abuse e di aggioaggio | 51 |
| 4 I presidi e gli strumenti di controllo | 51 |
| 4.1 Premessa | 52 |
| 4.2 Principi di comportamento | 52 |
| 4.2.1 Abuso di informazioni privilegiate..... | 52 |
| 4.2.2 Manipolazione del mercato e aggioaggio | 53 |
| 4.3 Principi di controllo..... | 53 |
| 4.3.1 Abuso di informazioni privilegiate..... | 53 |
| 4.3.2 Manipolazione del mercato e aggioaggio | 53 |
| Parte speciale 4: Reati di riciclaggio, ricettazione e impiego di beni-denaro o altra utilità di provenienza illecita e i reati con finalità di terrorismo o di eversione dell'ordine democratico..... | 54 |
| 1 Funzione della Parte Speciale quarta | 55 |
| 2 I reati di riciclaggio, ricettazione e terrorismo..... | 55 |

CRED.IT SOCIETÀ FINANZIARIA SPA

| | |
|--|----|
| 3 Attività sensibili nell'ambito dei reati di riciclaggio, ricettazione e terrorismo | 56 |
| 4 I presidi e gli strumenti di controllo | 56 |
| 4.1 Premessa | 57 |
| 4.2 Principi di comportamento | 57 |
| 4.3 Principi di controllo..... | 58 |
| Parte speciale 5: Reati informatici..... | 59 |
| 1 Funzione della Parte Speciale Quinta..... | 60 |
| 2 I reati informatici | 60 |
| 2.1 Falsità in un documento informatico | 60 |
| 2.2 Accesso abusivo e detenzione abusiva di codici di accesso | 60 |
| 2.3 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche..... | 61 |
| 2.4 Danneggiamento | 61 |
| 3 Attività sensibili nell'ambito dei reati informatici..... | 62 |
| 4 I presidi e gli strumenti di controllo | 62 |
| 4.1 Premessa | 62 |
| 4.2 Principi di comportamento | 63 |
| 4.3 Principi di controllo..... | 63 |
| Parte speciale 6: Le nuove fattispecie di reato in materia di tutela della salute e della sicurezza sul lavoro | 65 |
| 1 Funzione della Parte Speciale Sesta | 66 |
| 3 Attività sensibili nell'ambito dei reati in materia di tutela della salute e..... | 67 |
| della sicurezza sul lavoro | 67 |
| 4 I presidi e gli strumenti di controllo | 67 |
| 4.1 Premessa | 67 |
| 4.2 Principi di comportamento | 67 |
| 4.3 Principi di controllo..... | 68 |
| Allegato 1..... | 70 |
| 1 Elenco reati ex D.Lgs. 231/2001 | 71 |
| 1.1 Reati contro la Pubblica Amministrazione | 71 |
| 1.2 Reati di falsità in monete | 71 |
| 1.3 Reati societari..... | 71 |
| 1.4 Reati aventi finalità di terrorismo o di eversione ordine democratico | 72 |
| 1.5 Reati contro la personalità individuale..... | 72 |
| 1.6 Reati di market abuse | 72 |
| 1.7 Reati transnazionali | 72 |

CRED.IT SOCIETÀ FINANZIARIA SPA

| | | |
|------|--|----|
| 1.8 | Reati di omicidio colposo e lesioni colpose gravi o gravissime | 73 |
| 1.9 | Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza..... | 73 |
| | Illecita..... | 73 |
| 1.9 | Reati informatici..... | 73 |
| 1.10 | Delitti di criminalità organizzata | 73 |
| 1.11 | Delitti contro l'industria e il commercio | 74 |
| 1.12 | Delitti in materia di violazione del diritto d'autore..... | 74 |
| 1.13 | Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci..... | 75 |
| | Allegato 2..... | 76 |
| | 1 Regolamento dell'Organismo di Vigilanza..... | 77 |

Parte generale

PARTE GENERALE

1 Introduzione

1.1 Definizioni

| | |
|-------------------------|--|
| Banca d'Italia | Banca d'Italia Banca centrale italiana, con funzioni di vigilanza sulle banche, sulle società di gestione del risparmio, sulle società di investimento a capitale variabile, sulle società d'intermediazione mobiliare, sugli istituti di moneta elettronica e sugli intermediari finanziari iscritti nell'elenco speciale di cui all'art. 106 e 107 TUB. |
| Collaboratori | Collaboratori Soggetti che intrattengono con l'ente rapporti di collaborazione a vario titolo (consulenti, avvocati esterni, etc.). |
| Consob | Consob Commissione Nazionale per le Società e la Borsa. |
| D. Lgs. 231/2001 | Decreto o D.Lgs. 231/2001 Decreto Legislativo n. 231 dell'8 giugno 2001, "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica". |
| D. Lgs. 231/2007 | Decreto o D.Lgs. 231/07 il Decreto Legislativo 21 novembre 2007, n.231, di attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione. |
| Destinatari | Destinatari Soggetti in posizione apicale e soggetti sottoposti alla loro direzione o vigilanza, ivi compresi collaboratori e società in service. |
| Enti | Enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica. |
| ISVAP | ISVAP Istituto per la Vigilanza sulle Assicurazioni Private e di Interesse Collettivo. |
| Linee Guida ABI | Linee Guida ABI Linee Guida per il settore bancario in materia di responsabilità amministrativa emanate dall'Associazione Bancaria Italiana. |
| Linee Guida ANIA | Linee Guida ANIA Linee guida per il settore assicurativo in materia di responsabilità amministrativa emanate dall'Associazione Nazionale fra le Imprese Assicuratrici. |
| Modello | Modello Il presente modello di organizzazione e gestione, così come previsto dall'art. 6, comma 1, lett. a), del D.Lgs. 231/2001. |

| | |
|----------------------------|---|
| OdV | OdV Organismo di Vigilanza previsto all'art. 6, comma 1, lettera b) del D.Lgs. 231/2001, cui è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello e di curarne l'aggiornamento. |
| Reati | Reati I reati (delitti e contravvenzioni) di cui agli artt. 24 e ss. del D.Lgs. 231/2001. |
| Soggetti Apicali | Soggetti in posizione apicale Persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società 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 della stessa. |
| Soggetti Rilevanti | Soggetti rilevanti I soggetti la cui attività può essere fonte di responsabilità per l'ente, come indicati dall'art. 5, comma 1, lett. a) e b), del D.Lgs. 231/2001. |
| Soggetti Sottoposti | Persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale. |
| T.U.F. | T.U.F D.Lgs. n. 58/1998, "Testo unico delle disposizioni in materia di intermediazione finanziaria". |
| U.I.F | U.I.F. Unità Informazione Finanziaria della Banca d'Italia. |
| Consob | CONSOB Commissione Nazionale per le Società e la Borsa. |

1.2 La normativa di riferimento: il D.Lgs. 231/2001 e le fonti internazionali

Il Decreto Legislativo 231/2001 (di seguito "il Decreto"), entrato in vigore il 4 luglio 2001, individua le disposizioni normative concernenti la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica".

Tale Decreto prevede una presunzione di corresponsabilità delle imprese nella commissione di alcune tipologie di reato da parte di propri amministratori, dirigenti, dipendenti e/o collaboratori, con significative sanzioni amministrative e interdittive, a meno che le stesse imprese non abbiano adottato modelli di organizzazione, gestione e controllo idonei a prevenire la commissione dei reati ivi previsti.

Il D.Lgs. 231/2001 è stato emanato in esecuzione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 e pubblicato nella Gazzetta Ufficiale del 19 giugno 2001 n. 140, al fine di adeguare la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali, cui l'Italia ha già da tempo aderito, quali:

- la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee;
- la Convenzione del 26 maggio 1997, anch'essa firmata a Bruxelles, sulla lotta alla corruzione in cui sono coinvolti funzionari della Comunità Europea e degli Stati Membri;
- la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali, che ha introdotto il principio della responsabilità delle Società per specifiche tipologie di reati commessi da propri amministratori, dipendenti e collaboratori, nell'interesse o a vantaggio delle società stesse.

1.3I presupposti della responsabilità degli enti, la funzione del MOG e il profilo Sanzionatorio

Ai sensi dell'art. 1, c. 2, del Decreto, i soggetti destinatari della normativa sono: enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica; sono invece esclusi lo Stato, gli enti pubblici territoriali, altri enti pubblici non economici e gli enti che svolgono funzioni di rilievo costituzionale. Secondo quanto previsto dall'art. 5 del Decreto, gli enti rispondono in via amministrativa della commissione dei reati, analiticamente indicati dal Legislatore nel D.Lgs. 231/2001 e sue successive integrazioni, qualora sussistano determinati presupposti:

- sia stato commesso uno dei reati previsti dal Decreto;
 - il reato sia stato commesso nell'interesse o a vantaggio dell'ente;
 - il reato sia stato commesso da un soggetto apicale o da persone sottoposte alla sua direzione o vigilanza.
- Infatti, presupposto per la determinazione della responsabilità dell'ente, così come previsto dall'art. 5, c. 1, è la commissione di determinati reati nell'interesse o a vantaggio dell'ente stesso da parte di:
- a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché persone che esercitano, anche di fatto, la gestione e il controllo della stessa (ad esempio, amministratori e direttori generali) cosiddetti "soggetti apicali";
 - b) persone sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati alla precedente lettera a) (ad esempio, dipendenti).

In particolare, relativamente alla definizione di soggetto apicale si riporta quanto previsto dalle Linee Guida di ANIA: "i soggetti in posizione apicale sono coloro che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente e ad essi sono equiparati sia coloro che svolgono le medesime funzioni in una unità organizzativa dotata di autonomia finanziaria e funzionale, sia coloro che esercitano la

gestione e il controllo - anche solo in via di fatto - dell'ente, così realizzando un "dominio penetrante" sullo stesso". Peraltro, l'art. 25 ter limita i soggetti apicali rilevanti per i reati da esso richiamati ai soli "amministratori, direttori generali o liquidatori", da integrare, in via interpretativa, con i "dirigenti preposti alla redazione dei documenti contabili societari" ai sensi del D.Lgs. n. 262/2005.

La distinzione tra le due categorie di soggetti (apicali e sottoposti a direzione e vigilanza) riveste indubbia rilevanza, in quanto ne deriva una diversa graduazione di responsabilità dell'ente coinvolto, nonché una differente previsione dell'onere della prova; infatti, nel caso di reati commessi da soggetti apicali, sussiste in capo all'ente una presunzione di responsabilità determinata dalla circostanza che tali soggetti esprimono e rappresentano la politica aziendale dell'ente stesso e, quindi, la sua volontà e azione esteriore.

Sotto il profilo sanzionatorio, vale precisare che per tutti gli illeciti commessi è sempre prevista a carico della persona giuridica l'applicazione di una sanzione pecuniaria. Per le ipotesi di maggiore gravità è prevista anche l'applicazione di sanzioni interdittive, quali l'interdizione dall'esercizio dell'attività, la sospensione o la revoca di autorizzazioni, licenze o concessioni, il divieto di contrarre con la Pubblica Amministrazione, l'esclusione da finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni e servizi. Sono inoltre previsti la confisca del profitto conseguito e la pubblicazione della sentenza.

Le fattispecie di reato suscettibili di configurare la responsabilità amministrativa degli enti sono soltanto quelle espressamente contemplate dal legislatore, in via originaria e a seguito delle successive modifiche al D.Lgs. 231/2001.

Dette fattispecie di reato sono riconducibili alle seguenti categorie:

- reati commessi nei rapporti con la Pubblica Amministrazione;
- delitti informatici e trattamento illecito dei dati;
- reati contro la fede pubblica;
- reati societari;
- reati con finalità di terrorismo o di eversione dell'ordine democratico (delitti contro la personalità dello Stato);
- pratiche di mutilazione degli organi genitali femminili;
- delitti contro la personalità individuale;
- reati di market abuse;
- omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;
- reati transnazionali;
- ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

1.4 Presupposti di esclusione della responsabilità dell'ente

Il Decreto prevede, agli articoli 6 e 7, nel caso in cui uno dei Reati sia stato commesso dai soggetti di cui all'art. 5, c 1, lettera a), una forma di esonero dalla responsabilità qualora l'ente dimostri:

- di aver adottato ed efficacemente attuato, prima della commissione del fatto, "modelli di organizzazione, gestione e controllo" idonei a prevenire i reati della specie di quello commesso;
- che il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;
- che le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

– che non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui ai punti precedenti. L'ente, in ogni caso, non risponde, se i predetti soggetti hanno agito nell'interesse esclusivo proprio o di terzi (art. 5, comma 2).

Il medesimo articolo prevede al comma 2, alcune specifiche esigenze alle quali un modello di organizzazione, gestione e controllo idoneo deve rispondere:

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

Lo stesso Decreto nonché il relativo Regolamento di attuazione emanato con Decreto Ministeriale del 26 giugno 2003 n. 201, afferma inoltre che i modelli possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento redatti da associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni osservazioni sull'idoneità dei modelli a prevenire i Reati.

In linea con quanto sopra, anche i punti fondamentali che le Linee Guida di categoria (in particolare le linee guida emanate da ABI, ANIA e Confindustria) individuano nella costruzione dei Modelli possono essere così sintetizzati e schematizzati:

- individuazione delle aree di rischio, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei Reati previsti dal Decreto;
- obblighi di informazione dell'Organismo di Vigilanza, volti a soddisfare l'attività di controllo sul funzionamento, l'efficacia e l'osservanza del Modello;
- predisposizione di un sistema di controllo interno ragionevolmente in grado di prevenire o ridurre il rischio di commissione dei Reati attraverso l'adozione di appositi protocolli;
- conformità alle leggi, regolamenti, norme e politiche interne.

In particolare, Confindustria individua i passi operativi che l'ente deve compiere per attivare un sistema di gestione dei rischi coerente con i requisiti imposti dal Decreto e per la costruzione di un modello organizzativo, ovvero:

- Inventariazione degli ambiti aziendali di attività in base alle attività, alle funzioni, ai processi attraverso una revisione periodica esaustiva della realtà aziendale, con l'obiettivo finale di individuare le aree che risultano interessate dalle potenziali casistiche di reato.
- Analisi dei rischi potenziali con riguardo alle possibili modalità attuative dei reati nelle diverse aree aziendali con l'obiettivo finale di mappare le potenziali modalità attuative degli illeciti nelle aree a rischio individuate con il criterio del punto precedente.
- Valutazione/costruzione/adeguamento del sistema di controlli preventivi eventualmente esistente e con il suo adeguamento quando ciò si riveli necessario, o con una sua costruzione quando l'ente ne sia sprovvisto, per renderlo tale da garantire che i rischi di commissione dei reati, secondo le modalità individuate e documentate nella fase precedente, siano ridotti ad un "livello accettabile" e con l'obiettivo finale di descrivere in maniera documentale il sistema dei controlli preventivi attivato, con dettaglio delle singole componenti del sistema, nonché degli adeguamenti eventualmente necessari.

1.5 I riflessi del nuovo profilo di responsabilità penale delle imprese sul mondo

assicurativo e bancario

Per un gruppo assicurativo e bancario, i principi di organizzazione, gestione e controllo richiesti dal Decreto, sono anche espressione di quanto richiesto e raccomandato dalle Autorità di Vigilanza dei citati settori.

Banca d'Italia ha imposto un sistema integrato di controlli che permea l'intera attività aziendale e coinvolge soggetti diversi. Accanto ai Sindaci (orientati sempre più verso un controllo sulla gestione piuttosto che meramente contabile) ed alle Società di Revisione, infatti, specifico rilievo assume la funzione di internal auditing, disegnata seguendo le indicazioni contenute nelle Istruzioni di vigilanza. Il sistema dei controlli interni – ormai da anni attuato e continuamente aggiornato – ha quindi consentito alle banche di dotarsi di standard organizzativi, in linea con il principio di sana gestione il quale costituisce, seppure in un'accezione più ampia, ciò che il D.Lgs. 231/2001 intende affermare nell'ordinamento. Le banche, nel rispetto di quanto previsto da Banca d'Italia, devono:

- assicurare la necessaria separazione tra le funzioni operative e quelle di controllo ed evitare situazioni di conflitto d'interesse nell'assegnazione delle competenze;
- essere in grado di identificare, misurare e monitorare adeguatamente tutti i rischi assunti o assumibili nei diversi segmenti operativi;
- stabilire attività di controllo ad ogni livello operativo; assicurare sistemi informativi affidabili e idonei a riferire tempestivamente anomalie riscontrate nell'attività di controllo;
- consentire la registrazione di ogni fatto di gestione con adeguato grado di dettaglio;
- effettuare un monitoraggio finalizzato alla prevenzione di rischi connessi a frodi e infedeltà dei dipendenti e di quelli derivanti dall'eventuale coinvolgimento della società in operazioni di riciclaggio di denaro proveniente da attività illecite, nonché un monitoraggio sulle attività che possano determinare rischi di perdite risultanti da errori o inadeguatezza dei processi interni, delle risorse umane e dei sistemi oppure derivanti da eventi esterni.

2 Il Modello di organizzazione e gestione

2.1 Le aree di operatività del Gruppo

La Cred.it Società Finanziaria SpA opera nel settore finanziario e in particolare nel campo dei Leasing per le energie rinnovabili e di tutti i prodotti accessori a quest'ultimo. La società svolge anche attività di advisor per le PMI italiane e in via marginale il rilascio di polizze fideiussorie nei confronti dei propri azionisti.

2.2 Funzione, principi ispiratori e struttura del modello

Nell'ambito del processo di riorganizzazione societaria e del più ampio spettro di iniziative volte al rafforzamento degli elementi identitari, valoriali e di corporate governance il Gruppo ha deciso di avviare un progetto finalizzato alla predisposizione di un nuovo Modello secondo le Linee Guida di Gruppo.

L'adozione e l'efficace attuazione del Modello non solo consente alle società del Gruppo di beneficiare dell'esimente prevista dal D.Lgs. 231/2001, ma migliora la sua Corporate Governance, limitando il rischio di commissione dei Reati.

Scopo del Modello è pertanto la predisposizione di un sistema strutturato ed organico di prevenzione, dissuasione e controllo, finalizzato a sviluppare nei soggetti che direttamente o indirettamente operano nell'ambito delle attività sensibili, la consapevolezza nel potenziale autore del Reato di commettere un reato e, grazie ad un monitoraggio costante dell'attività, a consentire di prevenire o di reagire tempestivamente per impedire la commissione del Reato stesso.

Nella predisposizione del presente Modello che, fermo restando la funzione peculiare descritta nei precedenti paragrafi, si inserisce nel più ampio sistema di controllo costituito principalmente dalle regole di

CRED.IT SOCIETÀ FINANZIARIA SPA

Corporate Governance, si è tenuto conto delle procedure e dei sistemi di controllo esistenti e già ampiamente operanti in azienda in quanto idonei a valere anche come misure di prevenzione dei Reati e di controllo sui processi coinvolti nelle attività sensibili.

Le regole, procedure e principi emersi ed esaminati durante le fasi progettuali di definizione del Modello, pur non riportati dettagliatamente nel presente Modello, fanno parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare.

Al fine dell'individuazione dei principi a cui ispirarsi per la redazione del Modello, sono stati analizzati e considerati:

- i principi di Corporate Governance contenuti nel *Codice di Corporate Governance* di Cred.it Società Finanziaria SpA adottato il **09 Novembre 2012**, strumento con il quale CRED.IT SOCIETÀ FINANZIARIA SPA ha inteso definire chiaramente ruoli e responsabilità di esecuzione delle strategie e delle attività d'impresa, nonché la composizione e le funzioni degli organi sociali responsabili del governo della Capogruppo e delle società operative del Gruppo, dando in particolare puntuale descrizione della composizione, del ruolo e delle regole di funzionamento per gli organi collegiali, mentre per gli organi individuali vengono descritte le regole di nomina e il ruolo;
- le norme di comportamento, i valori ed i principi enunciati nel *Codice Etico* e nella *carta dei valori*;
- le Direttive in materia di Sistema dei Controlli Interni del Gruppo CRED.IT SOCIETÀ FINANZIARIA SPA adottate in data **09 Novembre 2012**, nonché le procedure aziendali di Gruppo che disciplinano compiti e responsabilità nell'ambito del sistema di controllo interno;
- la documentazione e gli ordini di servizio inerenti la struttura gerarchico funzionale aziendale e organizzativa della Società e del Gruppo;
- le comunicazioni e circolari aziendali al personale;
- il sistema di deleghe e poteri in essere;
- le norme per la gestione e la comunicazione delle informazioni privilegiate ai sensi della normativa sugli "Abusi di mercato".

Inoltre, per la redazione del Modello ci si è ispirati alle disposizioni contenute nelle Linee Guida di ABI, ANIA e Confindustria, ai requisiti indicati dal Decreto ed ai principi generali previsti per un adeguato sistema di controllo interno, quali:

- definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- rispetto del principio della separazione delle funzioni;
- svolgimento di specifiche attività di controllo;
- tracciabilità del processo sia a livello di sistema informativo sia in termini documentali;
- comunicazione all'OdV delle informazioni rilevanti.

Il presente Modello è strutturato in una "Parte Generale" e singole "Parti speciali" predisposte per le diverse categorie di reato contemplate nel Decreto.

La Parte Generale contiene un'introduzione dedicata alla struttura del Decreto e all'applicabilità dello stesso ai settori assicurativo e bancario e le regole ed i principi generali del Modello.

Le Parti speciali trattano l'esegesi delle norme rilevanti relative alle varie categorie di Reati, l'esemplificazione delle condotte rilevanti, le attività sensibili all'interno della realtà della Società e i presidi e gli strumenti di controllo esistenti adottati dalla stessa.

2.3 Approccio metodologico

In ottemperanza a quanto richiesto dall'art. 6, comma 2, lettera a) del Decreto, nonché dalle indicazioni fornite dalle linee guida in precedenza citate, l'approccio adottato dal Gruppo per la conduzione della fase istruttoria propedeutica alla redazione del MOG ha previsto le seguenti fasi.

2.3.1 Fase preliminare

In tale fase, finalizzata alla predisposizione della documentazione di supporto ed alla pianificazione delle attività di rilevazione, sono state condotte analisi puntuali sulla documentazione oggi esistente (organigrammi, rilevazioni di processo, rilevazioni e valutazione dei rischi e controlli) e confronti con le funzioni aziendali interessate, allo scopo di identificare i soggetti apicali e sottoposti da coinvolgere nella successiva fase di valutazione dei rischi e del sistema dei controlli.

Inoltre, sono state individuate le aree di attività (ambiti societari, ambiti organizzativi, processi e sottoprocessi operativi) nelle quali esiste il rischio di commissione dei reati previsti dal Decreto (matrice processi/reati) e, allo scopo di facilitare la successiva fase di valutazione dei rischi, sono state identificate le possibili modalità di conduzione della condotta illecita.

2.3.2 Fase di mappatura rischi e controlli

In tale fase, tenuto conto di quanto suggerito dalle Linee Guida, è stata effettuata un'approfondita indagine della complessiva organizzazione dell'ente, ovvero una ricognizione delle aree, dei settori e degli uffici, delle relative funzioni e procedure e delle entità esterne in vario modo correlate con l'ente stesso.

Per ciascuna di tali aree sono state condotte puntuali analisi documentali e interviste alle figure apicali e sottoposte coinvolte nelle attività esaminate, per identificare i reati effettivamente commissibili, le concrete modalità di commissione, la natura dei controlli esistenti (ad es. quelli di tipo organizzativo connessi alla chiara individuazione e segregazione di responsabilità e funzioni; quelli di tipo procedurale, connessi alla formalizzazione delle attività in regole interne; quelli derivanti dalle soluzioni ICT attraverso la previsione di passaggi formali obbligatori, etc.) e la loro efficacia. Nel dettaglio si è proceduto a:

- identificare la “macro-operatività” adottata dalla Società in merito ai cosiddetti processi “sensibili”;
- descrivere, nell’ambito organizzativo analizzato, le posizioni e i soggetti coinvolti, le loro responsabilità ed i loro poteri, distinguendo fra figure “apicali” o “sottoposte”, così come indicato nel Decreto;
- identificare e descrivere i reati commissibili e le conseguenze che essi potrebbero avere;
- individuare e descrivere la possibile condotta illecita propria dell’attività in esame e le modalità pratiche attraverso cui i reati potrebbero essere commessi;
- stimare la frequenza con la quale, nella normale operatività aziendale, si svolgono le attività in esame e dunque con quale frequenza si presentino occasioni di commissione dei reati individuati;
- individuare in maniera puntuale i controlli esistenti (preventivi e successivi) e valutare l’allineamento della struttura di controllo ai dettami del Decreto in termini di esistenza, efficacia ed efficienza dei controlli, esistenza di procedure formalizzate, adeguatezza del sistema delle deleghe e procure, esistenza e adeguatezza del sistema disciplinare.

In particolare per i processi sensibili ai nuovi reati di natura informatica si è proceduto, attraverso la redazione del DPS, alla valutazione delle misure di sicurezza ossia dell’insieme di regole, politiche, procedure e controlli atte a garantire l’integrità, la disponibilità e la riservatezza delle informazioni da crimini informatici.

La fase di rilevazione dei rischi e dei controlli ha consentito di pervenire alla ricostruzione di dettaglio delle aree aziendali “sensibili”, con identificazione delle funzioni e dei soggetti coinvolti e della loro responsabilità nonché dei sistemi di controllo adottati per la mitigazione dei rischi.

2.3.3 Fase di valutazione rischi e controlli

In tale fase si è provveduto, per ciascuno dei processi sensibili, alla valutazione del grado di rischiosità con il metodo del "Control and Risk Assessment" (Valutazione di Controlli e Rischi Guidata):

- al responsabile di ciascun sottoprocesso è stato richiesto di valutare la probabilità, e l'eventuale impatto economico, del rischio che vengano commessi illeciti amministrativi dipendenti da reato, tenuto conto del grado di efficacia e di efficienza delle procedure e dei sistemi di controllo esistenti all'interno del sottoprocesso, in quanto idonei a valere anche come misure di prevenzione dei reati;
- sulla base di dette valutazioni e delle metriche di valutazione definite è stato determinato il livello di criticità, sotto il profilo del rischio ai sensi del Decreto, nell'ambito di ciascun sottoprocesso identificato;
- in relazione alle aree di rischio identificate sono state individuate le opportune azioni correttive per migliorare il sistema dei controlli e ridurre il livello di criticità.

Affinché tale momento potesse rappresentare una reale occasione di sensibilizzazione e coinvolgimento, l'intero processo valutativo e le relative evidenze emerse sono state condivise con il top management.

Il processo di valutazione da parte dei responsabili è stato coordinato e supportato dal team di consulenti che hanno fornito apposita documentazione ed il supporto metodologico per la sua compilazione.

Al termine dell'analisi sono state evidenziate le macro-criticità del modello organizzativo e di controllo esistente, rispetto a quanto richiesto dal Decreto in termini di adeguatezza degli standard etici, presidio delle attività sensibili, efficacia della struttura di delega, efficacia del disegno del sistema normativo interno e dei compiti e funzionamento degli organismi di controllo.

Al fine di fornire una adeguata formalizzazione alle rilevazioni condotte, è stato utilizzato un apposito database sviluppato per l'occasione che coerentemente ai modelli di rilevazione dei processi aziendali e di generale valutazione dei rischi operativi consente di:

- disporre di un'unica base dati per l'archiviazione di tutte le informazioni raccolte;
- valutare sulla base di metriche concordate con il Gruppo il livello di rischio teorico ed effettivo sulle singole aree oggetto di rischi 231;
- fornire una valutazione complessiva del livello di esposizione del Gruppo ai rischi 231;
- identificare e gestire il piano di interventi di miglioramento scaturiti dall'analisi condotta.

2.3.4 La procedura di adozione, di modifica ed integrazione del modello

Sebbene l'adozione del Modello sia prevista dal Decreto come facoltativa e non obbligatoria, il Gruppo, in conformità alle sue politiche aziendali, ha ritenuto necessario procedere all'adozione del Modello. La CRED.IT SOCIETÀ FINANZIARIA SPA ha adottato il Modello con la delibera del **09 Novembre 2012**.

Nella riunione consiliare del 09 Novembre 2012, ciascun membro del Consiglio di Amministrazione ha espressamente dichiarato di impegnarsi al rispetto del presente Modello, come risulta dal verbale della delibera.

Il Collegio Sindacale ha preso atto del presente Modello nella riunione del 09 Novembre 2012 e nel corso della stessa si è impegnato formalmente al rispetto del Modello medesimo.

Essendo il Modello un "atto di emanazione dell'organo dirigente", in conformità alle prescrizioni dell'art. 6, comma I, lettera a) del Decreto, le successive modifiche e integrazioni sono rimesse alla competenza del Consiglio di Amministrazione.

3 Le deleghe e i poteri

In linea generale il sistema di controllo del Gruppo si basa su un sistema di deleghe di funzioni e di procure formalizzato ed adeguatamente comunicato.

La **procura** è l'atto con il quale una persona (fisica o giuridica) conferisce ad un'altra il potere di rappresentarla, così come espressamente previsto dal Codice Civile in materia di rappresentanza e normalmente viene autenticata da un notaio, che verifica firma e poteri di chi la sottoscrive.

CRED.IT SOCIETÀ FINANZIARIA SPA

La procura si sostanzia nel potere del delegato a rappresentare la società in merito alla svolgimento di alcune attività; può essere generale (l'oggetto è il compimento di uno o più atti giuridici e si estende a tutti gli affari del rappresentato o ad una categoria di affari) o speciale (conferita ad hoc per atti specificati) ed ha una valenza verso l'esterno della società.

La **delega di funzioni** è la formalizzazione (di regola in forma non notarile) dell'incarico di svolgere una attività all'interno dell'organizzazione della società delegante.

I requisiti essenziali del sistema di procure e di deleghe di funzioni, ai fini di un'efficace prevenzione dei reati sono i seguenti:

- tutti coloro che intrattengono rapporti con la Pubblica Amministrazione per conto del Gruppo devono essere dotati di delega di funzioni in tal senso;
- le deleghe devono essere coerenti con la posizione ricoperta dal delegato nell'organigramma e con le responsabilità a lui attribuite e devono essere costantemente aggiornate per adeguarle ai mutamenti organizzativi;
- ciascuna delega definisce in modo specifico:
 - o i poteri del delegato;
 - o il soggetto a cui il delegato riporta gerarchicamente;
 - o i poteri gestionali assegnati, coerenti con gli obiettivi aziendali;
 - o i poteri di spesa, coerenti con le funzioni conferite.

I requisiti essenziali del sistema di procure, ai fini di un'efficace prevenzione dei reati sono:

- le procure generali sono conferite esclusivamente a soggetti dotati di delega e devono essere coerenti con le funzioni delegate;
- le procure generali descrivono i poteri conferiti e sono accompagnate da apposita comunicazione aziendale che fissa l'estensione dei poteri di rappresentanza e i limiti numerici;
- le modalità di aggiornamento delle procure sono descritte in apposita procedura.

Le autonomie deliberative in materia creditizia definiscono i limiti di erogazione del credito per ciascun organo deliberativo individuato. Tali limiti, su proposta della Direzione Crediti, sono approvati dal Consiglio di Amministrazione della Società, e formalizzati in apposito documento scritto. La documentazione relativa è disponibile presso la Direzione Crediti.

La delibera quadro per le attività di intermediazione mobiliare definisce i poteri e i limiti autorizzativi di effettuazione di operazioni su strumenti finanziari per la proprietà della Società e/o di negoziazione con la clientela.

Le subdeleghe e i limiti operativi relativi all'attività caratteristica della Società sono contenuti in Manuali e documenti presenti presso l'Ufficio Affari Generali o le singole funzioni interessate.

L'ODV effettua verifiche circa la coerenza delle deleghe e delle procure vigenti con la struttura organizzativa di Cred.it Società Finanziaria SpA.

4 Principi di comportamento generali per i destinatari

Tutti i Destinatari del Modello si astengono dal porre in essere comportamenti che possano integrare una fattispecie di reato prevista dal D.Lgs. 231/2001 e, nello svolgimento delle proprie attività lavorative, rispettano:

- il Codice Etico;
- le disposizioni del Modello, in particolare le presenti disposizioni generali e le disposizioni particolari contenute nelle parti speciali;
- le procedure e i protocolli aziendali.

I soggetti in posizione apicale adempiono alle rispettive funzioni nel rispetto delle deleghe e dei poteri conferiti e si attengono altresì:

- alle previsioni dello Statuto Sociale;

– alle delibere del Consiglio di Amministrazione.

I soggetti in posizione apicale e quanti ricoprono posizioni di responsabilità devono altresì ottemperare costantemente e scrupolosamente agli obblighi di direzione e vigilanza loro spettanti in ragione della posizione ricoperta.

I soggetti sottoposti all'altrui direzione o vigilanza eseguono le direttive e le disposizioni operative interne e di Gruppo, purché conformi alle leggi vigenti e non in contrasto con i contenuti del Modello.

5 La diffusione del modello organizzativo tra i portatori di interesse

Ai fini dell'efficacia del presente Modello, risulta necessario garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute sia nei confronti dei dipendenti. Tale obiettivo riguarda tutte le risorse aziendali sia si tratti di risorse già presenti in azienda sia che si tratti di quelle da inserire. Il livello di formazione ed informazione è attuato con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle attività sensibili.

L'Organismo di Vigilanza supervisiona ed integra il sistema di informazione e formazione in collaborazione con la Direzione Risorse Umane e Organizzazione della Capogruppo e con il Responsabile Risorse Umane della Società per i dipendenti ed i dirigenti.

5.1 Informativa e formazione per dipendenti e dirigenti

La diffusione del Modello è effettuata mediante il sito intranet aziendale con la creazione di specifiche pagine web, costantemente aggiornate, i cui contenuti riguardino essenzialmente:

- un'informativa di carattere generale relativa al Decreto, corredata dagli articoli di giornale più significativi e dalle risposte alle domande più frequenti (FAQ) in relazione alla normativa in oggetto;
- struttura e principali disposizioni operative del Modello adottato;
- procedura di segnalazione all'OdV per la comunicazione da parte del dipendente di eventuali comportamenti, di altri dipendenti o di terzi, ritenuti potenzialmente in contrasto con i contenuti del Modello, mediante l'apertura di un'apposita casella di posta elettronica.

L'adozione del presente Modello è comunicata ai dipendenti al momento dell'adozione stessa tramite e-mail (o mezzo telematico equivalente) inviata a tutti i dipendenti in organico da parte della struttura competente. La e-mail è corredata da una dichiarazione di ricevuta e accettazione da parte dei dipendenti, da trasmettere all'OdV.

Ai nuovi assunti viene consegnato un set informativo, con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza. Tale set informativo contiene, oltre ai documenti di regola consegnati al neo-assunto, il Codice Etico, il Modello e il Decreto. Il set informativo è corredata da una dichiarazione di ricevuta e accettazione da parte del dipendente, da trasmettere all'OdV.

Oltre agli interventi di sensibilizzazione già condotti dal Gruppo su tutta la popolazione (progetto Unisono ed interventi e-learning già condotti) e agli interventi specifici già effettuati dalla Società, verrà svolta un'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al Decreto aggiornata rispetto ai nuovi reati introdotti, 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 (per dipendenti che rivestono la qualifica di dirigenti, per dipendenti che non rivestono la qualifica di dirigenti):

- Formazione in aula alle linee ed ai responsabili operativi: presentazione a beneficio delle prime linee e dei responsabili operativi della Società nel corso della quale:
 - o si informa in merito alle disposizioni del Decreto;
 - o si sensibilizzano i presenti sull'importanza attribuita dalla Società all'adozione di un sistema di governo e di controllo dei rischi;

- si descrivono la struttura e i contenuti principali del Modello adottato, nonché l'approccio metodologico seguito per la sua realizzazione e il suo aggiornamento;
 - si descrivono i comportamenti da tenere in materia di comunicazione e formazione dei propri dipendenti gerarchici, in particolare del personale operante nelle aree aziendali ritenute sensibili;
 - si illustrano i comportamenti da tenere nei confronti dell'OdV, in materia di comunicazioni, segnalazioni e collaborazione alle attività di vigilanza e aggiornamento del Modello.
- Formazione ai dipendenti operanti nell'ambito di procedure sensibili ai reati contemplati dal Decreto: sensibilizzazione da parte dei responsabili delle funzioni aziendali potenzialmente a rischio di reato dei propri dipendenti gerarchici, in relazione al comportamento da osservare, alle conseguenze derivanti da un mancato rispetto delle stesse e, in generale, del Modello adottato dalla Società.
 - Formazione on-line: predisposizione di un corso di formazione computer based, disponibile a tutti dipendenti sul sito intranet aziendale, con la finalità di diffondere la conoscenza del Decreto e del Modello. La partecipazione ai programmi di formazione sopra descritti è obbligatoria e la verifica circa l'effettiva effettuazione è demandata al Personale, che ne relaziona all'OdV.

5.2 Informativa e formazione per i collaboratori

Anche per i collaboratori è prevista una specifica attività di diffusione e formazione relativa al Modello. I suddetti soggetti devono essere informati del contenuto del Modello e dell'esigenza del Gruppo che il loro comportamento sia conforme a quanto disposto nel Decreto. I collaboratori esterni saranno tenuti a rilasciare al Gruppo una dichiarazione ove si attesti la integrale conoscenza dei contenuti e prescrizioni contenute nel Decreto e l'impegno al rispetto dello stesso, prevedendo specifica informativa nell'ambito del contratto.

Nei confronti dei citati soggetti, inoltre, è stato predisposto un piano di formazione e comunicazione, che prevede:

- la pubblicazione del Modello sul sito internet aziendale con creazione di specifiche pagine web, costantemente aggiornate, ai fini della diffusione al pubblico dello stesso, contenenti in particolare un'informativa di carattere generale relativa al Decreto e all'importanza attribuita all'adozione di un sistema di governo e di controllo dei rischi e la struttura e le principali disposizioni operative del Modello;
- inserimento di una dichiarazione, in qualunque contratto di fornitura, servizio e consulenza (nel corpo del proprio testo o in allegato) di conoscenza delle disposizioni del Decreto e di impegno al rispetto dello stesso.

6 L'organismo di Vigilanza

6.1 L'Organismo di Vigilanza come previsto dal D.Lgs. 231/01

[\(L'Organismo di Vigilanza come previsto dal D.Lgs. 231/01: ruolo, compiti e funzioni – i nuovi doveri di controllo ex art. 231/07\)](#)

Come anticipato, l'art. 6 del Decreto prevede una forma di esonero dalla responsabilità per l'ente che provi, tra l'altro, che "il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo".

L'Organismo di Vigilanza (OdV) ha, quindi, autonomi poteri di iniziativa e controllo al fine di vigilare sul funzionamento e l'osservanza del Modello, ma non ha poteri coercitivi o di intervento modificativi della struttura aziendale o sanzionatori nei confronti di dipendenti, collaboratori o organi sociali, che invece sono demandati agli organi societari (Amministratore Delegato, CdA, Collegio Sindacale e Assemblea) o funzioni aziendali competenti.

CRED.IT SOCIETÀ FINANZIARIA SPA

Compito dell'OdV è in generale quello di vigilare:

- sull'osservanza del Modello da parte di tutti i soggetti interessati (dipendenti, collaboratori o organi sociali);
- sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;
- sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative, sollecitando a tal fine gli organi competenti.

Nello specifico, spetta all'OdV il compito di svolgere attività di verifica e controllo, ovvero:

- verificare l'efficacia e l'attuazione delle procedure di controllo previste dal Modello;
- condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura delle attività sensibili;
- raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere a lui trasmesse o tenute a sua disposizione;
- effettuare periodicamente verifiche mirate su determinate operazioni o specifici atti posti in essere dalla Società, soprattutto nell'ambito delle attività sensibili, i cui risultati devono essere riassunti in un apposito rapporto da esporsi agli organi societari deputati;
- coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività in relazione alle procedure stabilite nel Modello;
- attivare e svolgere le indagini interne, raccordandosi di volta in volta con le funzioni aziendali interessate per acquisire ulteriori elementi di indagine.

Spettano, infine all'OdV:

- il compito di coordinarsi con il Direttore Risorse Umane e Organizzazione della Capogruppo per:
 - o la verifica dei programmi di formazione per il personale;
 - o la verifica del contenuto delle comunicazioni periodiche da inviare ai dipendenti e collaboratori, finalizzate a fornire agli stessi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al Decreto;
 - o il monitoraggio delle iniziative per la diffusione della conoscenza e della comprensione del Modello;
 - o la verifica della documentazione interna necessaria al fine della sua efficace attuazione, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso;
- il compito di valutare le esigenze di aggiornamento del Modello e in relazione a ciò l'adeguamento dell'organigramma, anche attraverso apposite riunioni con le varie funzioni aziendali interessate.

Vale precisare che, il D.Lgs. 231/2007, recante attuazione della c.d. Terza Direttiva Antiriciclaggio concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, prevede, al Titolo IV – Vigilanza e controlli, art. 52 "Organi di controllo", l'obbligo di vigilare sull'osservanza delle disposizioni ivi contenute in capo al collegio sindacale, al consiglio di sorveglianza, al comitato di controllo di gestione e anche "all'Organismo di Vigilanza di cui all'art. 6, comma 1, lettera b) del D.Lgs. 231/2001" ..

6.21 requisiti dell'Organismo di Vigilanza

Per conformarsi al dettato normativo e poter svolgere al meglio i propri compiti, l'OdV deve rispondere a determinate caratteristiche, ovvero:

- *indipendenza e autonomia dai vertici dell'ente*: al fine di garantire l'imparzialità e la possibilità di operare, anche quando esso sia chiamato a vigilare sull'applicazione delle prescrizioni del modello al vertice medesimo.
- *professionalità*: occorre garantire la concreta possibilità di azione all'OdV in un contesto che richiede sia capacità di valutazione e gestione dei rischi, sia competenze e conoscenze in materia di analisi delle procedure, di organizzazione e controllo aziendale e di pratica professionale;

– *continuità d'azione, stabilità e continuità*: al fine di garantire la costante attività di monitoraggio e di aggiornamento del modello e la sua variazione al mutare delle condizioni aziendali di riferimento;

– *onorabilità*: i membri dell'OdV devono possedere requisiti di autorevolezza morale ed onorabilità.

Tali caratteristiche presuppongono che l'OdV sia collocato, all'interno dell'organigramma aziendale, in una posizione gerarchicamente elevata, e che riferisca unicamente ai massimi vertici aziendali (Presidente, Vice Presidente, Consiglio di Amministrazione) e che i membri dell'OdV siano estranei alla gestione operativa dell'ente.

6.3 Le regole di funzionamento dell'Organismo di Vigilanza e le situazioni di

Incompatibilità

6.3.1 Rapporti tra l'Organismo di Vigilanza e gli organi sociali

Pur nel rispetto dei principi di autonomia e indipendenza, al fine di consentire che l'OdV espliciti la massima efficacia operativa, è necessaria l'istituzione di specifici canali di comunicazione e adeguati meccanismi di collaborazione tra l'OdV e gli altri organi sociali della Società.

A tal fine l'OdV relaziona il Consiglio di Amministrazione e il Collegio Sindacale:

– a seguito di una seduta di particolare importanza, su proposta del Presidente, circa l'attività svolta;

– annualmente, sullo stato di attuazione del Modello, evidenziando le attività di verifica e di controllo compiute, l'esito di dette attività, le eventuali lacune del Modello emerse, i suggerimenti per le eventuali azioni da intraprendere. In tale occasione presenterà altresì il piano annuale delle verifiche predisposto per l'anno successivo.

L'OdV potrà chiedere di essere sentito dal Consiglio di Amministrazione ogni qualvolta ritenga opportuno un esame o un intervento di siffatto organo in materie inerenti il funzionamento e l'efficace attuazione del Modello.

L'OdV potrà, a sua volta, essere convocato in ogni momento dal Consiglio di Amministrazione e dagli altri organi sociali per riferire su particolari eventi o situazioni relative al funzionamento e al rispetto del Modello.

A garanzia di un corretto ed efficace flusso informativo, l'OdV ha inoltre la possibilità, al fine di un pieno e corretto esercizio dei suoi poteri, di chiedere chiarimenti o informazioni direttamente al Direttore Generale.

6.3.2 Coordinamento tra gli OdV del Gruppo

Al fine di armonizzare e garantire l'efficacia e la coerenza delle attività di controllo e verifica svolte all'interno del Gruppo e, soprattutto, per assicurare una maggiore tutela dal rischio di commissione del reato, si è ritenuto che ogni singolo OdV istituito in ciascuna società del Gruppo operi coordinandosi e mantenendo contatti periodici con l'OdV della Capogruppo.

E' pertanto assegnato all'OdV della Capogruppo il compito di coordinare le attività degli OdV delle società controllate istituendo appositi flussi e canali informativi, al fine di realizzare un coerente sistema di vigilanza e controllo a livello di Gruppo.

In tal senso, è data facoltà all'OdV della Capogruppo di acquisire documentazione e informazioni e di effettuare controlli periodici e verifiche mirate sulle attività a rischio delle società del Gruppo, attraverso richieste ai rispettivi OdV.

L'OdV della Società riferisce su base periodica all'OdV della Capogruppo in merito all'attuazione del proprio modello di organizzazione, gestione e controllo.

6.3.3 Coordinamento tra gli organismi di vigilanza delle Società del Gruppo Bancario

Al fine di armonizzare e garantire l'efficacia e la coerenza delle attività di controllo e verifica svolte all'interno del Gruppo e, soprattutto, per assicurare una maggiore tutela dal rischio di commissione dei reati, si è ritenuto che ogni singolo OdV istituito in ciascuna società del Gruppo dovrà operare coordinandosi e mantenendo contatti periodici con quello della Capogruppo.

Inoltre è data facoltà all'OdV di Cred.it Società Finanziaria SpA di acquisire documentazione e informazioni e di effettuare controlli periodici e verifiche mirate sulle attività a rischio delle società controllate, attraverso richieste dirette all'OdV di quest'ultime.

6.3.4 Flussi informativi nei confronti dell'Organismo di Vigilanza

Tra le esigenze che il Modello deve soddisfare, il D.Lgs. 231/2001 enuncia anche l'istituzione di obblighi informativi nei confronti dell'OdV.

I flussi informativi hanno ad oggetto tutte le informazioni e tutti i documenti che devono essere portati a conoscenza dell'OdV a carico dei Destinatari del Modello e/o delle Funzioni interessate.

In particolare, devono senza indugio essere trasmesse all'OdV le informazioni concernenti:

- il sistema delle deleghe e l'organigramma tempo per tempo vigenti;
- i provvedimenti e/o le notizie provenienti da organi di Polizia Giudiziaria, o da qualsiasi altra Autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D.Lgs. 231/2001 commessi nell'interesse o a vantaggio di Cred.it Società Finanziaria SpA;
- l'avvio di un procedimento giudiziario per i reati previsti dal D.Lgs. 231/2001;
- ogni atto/documento relativo a finanziamenti pubblici ricevuti dalla Società e/o erogati alla clientela;
- i prospetti riepilogativi redatti a seguito di gare pubbliche ovvero di trattative private con enti pubblici;
- gli eventuali rapporti preparati dai responsabili delle funzioni aziendali nell'ambito della propria attività, dai quali si evincano fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza del D.Lgs. 231/2001;
- gli interventi organizzativi e normativi diretti all'effettiva attuazione, a tutti i livelli aziendali, del Modello;
- le notizie in merito ai procedimenti disciplinari avviati, alle eventuali sanzioni applicate ovvero all'archiviazione di tali procedimenti, con le relative motivazioni.

6.3.5 Cause d'incompatibilità

Sono cause d'incompatibilità per la nomina a membro dell'OdV:

- trovarsi nelle condizioni previste dall'art. 2382 c.c., ovvero interdizione, inabilitazione, fallimento o condanna ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi;
- l'essere membri esecutivi del Consiglio di Amministrazione di società del gruppo bancario o direttori generali della società o della Società di Revisione cui è stato conferito l'incarico di revisione contabile, ai sensi della vigente normativa, o revisori da questa incaricati;
- l'aver relazioni di coniugio, parentela o affinità fino al quarto grado con i componenti del Consiglio di Amministrazione, con i direttori generali della società o della Società di Revisione o con i revisori incaricati dalla Società di Revisione;
- l'aver intrattenuto rapporti di lavoro autonomo o subordinato, nell'ultimo biennio, con entità con le quali, o nei confronti delle quali, possono essere compiuti i reati e gli illeciti di cui al Decreto;
- intrattenere, direttamente o indirettamente, relazioni economiche con la CRED.IT SOCIETÀ FINANZIARIA SPA, con le sue controllate o con la controllante, con gli amministratori esecutivi, con l'azionista o gruppo di

azionisti che esercitano il controllo sulla Società, di rilevanza tale da condizionare l'autonomia di giudizio e compromettere l'indipendenza.

Ulteriore causa di cessazione dall'incarico di componente dell'OdV è rappresentata dalla decadenza dalla funzione o carica (es. Consigliere di Amministrazione) ricoperta al momento della nomina e in virtù della quale l'incarico è stato attribuito.

I membri dell'OdV devono essere in possesso dei requisiti di onorabilità previsti dalla vigente normativa per gli amministratori di imprese di assicurazione e non avere riportato condanne, anche non definitive, per uno dei reati previsti dal D.Lgs. 231/2001.

Il Consiglio di Amministrazione valuta, preventivamente all'insediamento dell'interessato nella posizione societaria e/o aziendale da cui deriva il ruolo di membro dell'OdV e successivamente, con adeguata periodicità, la sussistenza dei suddetti requisiti soggettivi dei membri dell'OdV.

Il venir meno dei predetti requisiti, ovvero l'insorgenza di cause di incompatibilità, in costanza del mandato, determina la decadenza dall'incarico e in tal caso il Consiglio di Amministrazione provvede tempestivamente alla nomina del membro mancante, nel rispetto dei principi indicati.

L'OdV resta in carica due anni, è rieleggibile ed i suoi membri possono essere revocati dal Consiglio di Amministrazione in qualsiasi momento per giusta causa e/o giustificato motivo. In tal caso, il Consiglio di Amministrazione provvede tempestivamente alla sostituzione del membro revocato. L'OdV decade per la revoca di tutti i suoi membri. In tal caso il Consiglio di Amministrazione provvede tempestivamente alla sua ricostituzione.

Tenuto conto delle responsabilità attribuite e dei contenuti professionali specifici richiesti, l'OdV è coadiuvato, nello svolgimento dei propri compiti, dalla struttura di Internal Auditing di Gruppo e può avvalersi del supporto di altre funzioni interne, nonché di consulenti esterni.

Il compenso dei membri dell'OdV è determinato dal Consiglio di Amministrazione al momento della nomina e rimane invariato per l'intero periodo di durata dell'incarico.

Il Consiglio di Amministrazione approva, annualmente e su proposta dell'OdV, la previsione delle spese, anche di carattere straordinario, necessarie allo svolgimento delle attività di vigilanza e controllo previste dal Modello, nonché il consuntivo delle spese dell'anno precedente.

6.4 Nomina e composizione dell'Organismo di Vigilanza

In considerazione di quanto esposto e della realtà del Gruppo, il relativo incarico è stato affidato con apposita delibera, ad un organismo costituito in forma collegiale.

L'OdV è, quindi, composto da almeno tre membri:

- da un amministratore non esecutivo in quanto dotato della visibilità e del potere di farsi diretto portavoce anche in occasione delle sedute del Consiglio di Amministrazione degli orientamenti e delle decisioni assunte dall'OdV per assicurare una concreta ed efficace implementazione del Modello ovvero da un terzo esterno alla Società;
- da un esponente della Direzione Legale, Societario e Compliance della Capogruppo in quanto dotato di specifiche professionalità, di conoscenza delle strutture societarie e dell'organizzazione ovvero di un terzo esterno alla Società;
- dal Responsabile (o da un esponente del) Internal Auditing della Capogruppo in quanto dotato di una strutturale indipendenza ed autonomia dalle aree operative della società oltre che del potere/dovere di svolgere una costante attività di verifica sul corretto funzionamento dei sistemi dei controlli della società ovvero da un terzo esterno alla Società.

La scelta di tale composizione è stata determinata dal fatto che le suddette figure sono state riconosciute come le più adeguate ad assumere il ruolo dell'OdV in quanto, oltre ai requisiti di autonomia, indipendenza, professionalità e continuità d'azione che si richiedono per tale funzione, e alle capacità specifiche in tema di attività ispettive e consulenziali, possiedono altresì quei requisiti soggettivi formali che garantiscano ulteriormente l'autonomia e l'indipendenza richiesta dal compito affidato, quali onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice.

L'OdV così costituito provvederà a darsi le proprie regole di funzionamento attraverso un specifico regolamento (Cfr. in allegato Bozza Regolamento OdV), in linea con i principi considerati per la redazione del Modello e per lo svolgimento dell'attività della Società.

In ogni caso, il conferimento dell'incarico all'OdV e la revoca del medesimo sono funzioni riservate alla competenza del Consiglio di Amministrazione della Società.

7 Il sistema disciplinare e sanzionatorio

7.1 Funzioni del sistema disciplinare

Un efficiente sistema disciplinare rappresenta un sistema idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello così come previsto dall'art. 6, par. 2, comma e) del Decreto.

In particolare, tale sistema definisce le sanzioni e le modalità applicative da intraprendere nei confronti dei soggetti (dipendenti o terze parti) responsabili di comportamenti illeciti o di violazione delle norme contenute nei documenti di cui si compone il Modello.

Il Sistema disciplinare, individuate le possibili infrazioni, descrive le tipologie di sanzioni applicabili, differenziate in base alla categoria di appartenenza del soggetto responsabile dell'illecito, tenuto conto delle leggi vigenti che regolano i rapporti di lavoro. In particolare:

- Contratto Collettivo Nazionale di Lavoro per i quadri direttivi e per il personale delle aree professionali dipendenti dalle imprese creditizie, finanziarie e strumentali;
- Contratto Collettivo Nazionale per i dirigenti bancari;
- Legge 300 del 20 maggio 1970 (Statuto dei Lavoratori), art. 7 Sanzioni disciplinari;
- Legge 604 del 15 luglio 1966 (Norme sui licenziamenti individuali);
- Libro V Codice Civile, art. 2104 Diligenza del Prestatore di lavoro, art. 2105 Obbligo di fedeltà, art. 2106 Sanzioni disciplinari, art. 2118-2119 Licenziamento con e senza preavviso, art. 2392 Responsabilità (degli Amministratori) verso la società, art. 2407 Responsabilità (dei Sindaci), art.2409 Denuncia al tribunale, art. 2409 sexies Responsabilità (dei controllori e delle Società di Revisione).

La definizione, attraverso un sistema disciplinare, di un sistema di sanzioni (commisurate alla violazione e dotate di deterrenza) applicabili in caso di violazione delle regole di cui al presente Modello, rende efficiente l'azione di vigilanza dell'Organismo di Vigilanza ed ha lo scopo di garantire l'effettività del Modello stesso.

Come anticipato, infatti, la definizione di tale sistema sanzionatorio costituisce, ai sensi dell'art. 6 primo comma lettera e) del Decreto, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità dell'ente.

L'applicazione del sistema sanzionatorio presuppone la semplice violazione delle disposizioni del Modello; pertanto essa verrà attivata indipendentemente dallo svolgimento e dall'esito del procedimento penale, eventualmente avviato dall'autorità giudiziaria nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del Decreto.

7.2 Procedimento e misure disciplinari

7.2.1 Dipendenti

CRED.IT SOCIETÀ FINANZIARIA SPA

La violazione delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare. A tali comportamenti si applicano pertanto le disposizioni in materia di sanzioni disciplinari previste dal CCNL e dal Regolamento aziendale di disciplina.

In particolare, per i dipendenti, nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e delle eventuali normative speciali applicabili, il Regolamento aziendale di disciplina prevede i seguenti provvedimenti:

- rimprovero verbale;
- biasimo inflitto per iscritto;
- sospensione dal servizio e dal trattamento economico, nei limiti stabiliti all'art. 25 CCNL;
- licenziamento (nei casi previsti dalla legge).

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, agli organi societari e funzioni aziendali competenti.

I comportamenti sanzionabili che costituiscono violazione del presente del Modello sono la violazione di procedure interne previste dal Modello o l'adozione di comportamenti non conformi alle prescrizioni del Modello (indipendentemente dal fatto che esponano o meno la Società ad una situazione oggettiva di rischio imminente di commissione di un Reato).

Le sanzioni e l'eventuale richiesta di risarcimento dei danni verranno commisurate al livello di responsabilità ed autonomia del dipendente, all'eventuale esistenza di precedenti disciplinari a carico del dipendente, all'intenzionalità del comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Società può ragionevolmente ritenersi esposta - ai sensi e per gli effetti del D.Lgs. 231/2001 - a seguito della condotta censurata.

Il sistema sanzionatorio è soggetto a costante verifica e valutazione da parte dell'OdV e, per i dipendenti, del Direttore Risorse Umane e Organizzazione della Capogruppo, rimanendo quest'ultimo responsabile della concreta applicazione delle misure disciplinari qui delineate, su eventuale segnalazione dell'OdV. Per le situazioni che coinvolgono Dirigenti del Gruppo, il Direttore Risorse Umane e Organizzazione della Capogruppo agisce sulla base delle indicazioni del Comitato per la valutazione delle situazioni irregolari.

7.2.2 Membri del Consiglio di Amministrazione e Sindaci

Ancora, in caso di violazione del Modello da parte di uno o più membri del CdA o da parte di uno o più Sindaci, l'OdV informa il Collegio Sindacale e l'intero CdA i quali prendono gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee previste dalla legge e/o la revoca di deleghe eventualmente conferite all'Amministratore/Sindaco ovvero la comunicazione alla Consob da parte dei Sindaci delle irregolarità verificatesi.

7.2.3 Collaboratori

Ogni violazione delle regole di cui al presente Modello applicabili ai collaboratori o ogni commissione dei Reati previsti dal Modello è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti, nonché ai sensi delle norme di legge tempo per tempo vigenti.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla società, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal Decreto.

7.3 Segnalazioni verso l'Organismo di Vigilanza

CRED.IT SOCIETÀ FINANZIARIA SPA

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni, da parte dei dipendenti, degli organi sociali e dei collaboratori in merito ad eventi che potrebbero ingenerare responsabilità della Società ai sensi del Decreto.

In particolare, i Destinatari hanno l'obbligo di trasmettere all'OdV eventuali segnalazioni relative alla commissione, o alla ragionevole convinzione di commissione, dei Reati poste in essere da dipendenti e collaboratori, di cui essi siano venuti a conoscenza.

Le segnalazioni devono pervenire all'OdV in forma non anonima, indirizzandole alla casella e-mail appositamente predisposta (odv@creditspa.it). I segnalanti in buona fede devono essere garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Se un dipendente desidera segnalare una violazione (o presunta violazione) del Modello, deve riferire al suo diretto superiore. Qualora la segnalazione non dia esito, o il dipendente si senta a disagio nel rivolgersi al suo diretto superiore per la presentazione della segnalazione, può riferire direttamente all'OdV. I collaboratori, per quanto riguarda la loro attività svolta nei confronti o per conto della Società, devono effettuare la segnalazione direttamente all'OdV.

L'OdV valuta le segnalazioni ricevute e gli eventuali provvedimenti conseguenti applicabili in conformità a quanto previsto dal sistema sanzionatorio.

Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte, i dipendenti devono obbligatoriamente ed immediatamente trasmettere all'OdV le informazioni concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità Giudiziaria o di Controllo, dai quali si evinca lo svolgimento o l'avvio di indagini per i Reati, anche nei confronti di ignoti qualora tali indagini coinvolgano la Società o suoi dipendenti e collaboratori;
- le richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario per i Reati;
- i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- le notizie relative ai procedimenti sanzionatori svolti e alle eventuali misure irrogate (come i provvedimenti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di Reati o violazione delle regole di comportamento o procedurali del Modello.

Relativamente agli obblighi di segnalazione dei collaboratori, si rimanda a quanto specificato in apposite clausole inserite nei contratti che legano tali soggetti alla Società.

8 I reati ex D. Lgs. 231/2001 in CRED.IT SOCIETÀ FINANZIARIA SPA

La tabella di seguito riportata mostra le aree di attività sensibili in relazione alle tipologie di reati rilevanti per Cred.it Società Finanziaria SpA, secondo le modalità di classificazione adottate internamente.

CRED.IT SOCIETÀ FINANZIARIA SPA

| Macro processi | Processi | Reati | | | | | | |
|----------------|-----------------------------|-----------|--------------|----------------------|---------------------------------------|-------------------|-------------|----------------------|
| | | Societari | Contro la PA | Market abuse e aggio | Riciclaggio ricettazione e terrorismo | Falsità in monete | Informativi | Sicurezza sul lavoro |
| Business | Conces. del credito | | ✓ | | | | | |
| | Gest. commerciale | | ✓ | | ✓ | | | |
| | Gest. mandati reti | | ✓ | | | | | |
| | Gest. contratti | | ✓ | | ✓ | | | |
| Supporto | G. amministrativo contabile | ✓ | ✓ | | | | | |
| | Risorse umane (*) | ✓ | ✓ | | | | | ✓ |
| | Legale e recupero | ✓ | ✓ | | | | | |
| | Segnalazioni vigilanza | ✓ | | | | | | |
| | Servizi informatici(*) | | | | | | ✓ | |
| | Immobiliare (*) | | | ✓ | | | | |
| Governance | Affari Generali (*) | ✓ | ✓ | | | | | |
| | Gest. Controllo (*) | ✓ | ✓ | | | | | |

Parte speciale 1 Reati societari

PARTE SPECIALE 1

1 Funzione della Parte Speciale prima

La Parte Speciale prima si riferisce ai comportamenti posti in essere dai Destinatari del Modello, ed in particolare dai soggetti coinvolti nelle attività sensibili rispetto ai reati societari.

Obiettivo della presente Parte Speciale è che i suddetti soggetti adottino le presenti regole di condotta al fine di prevenire la commissione di tali reati.

In particolare, la presente Parte Speciale ha lo scopo di:

- indicare le procedure che i Destinatari del Modello sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

2 I reati societari

(I reati societari: esegesi delle norme rilevanti ed esemplificazioni di condotte illecite)

Il presente paragrafo si riferisce ai reati societari, secondo le fattispecie contemplate dall'art. 25 ter del D.Lgs. 231/2001, limitatamente ai casi che potrebbero configurarsi in capo alla Società.

2.1 Falsità in comunicazioni, prospetti e relazioni

I reati in oggetto sono previsti da:

- Art. 2621 del Codice Civile - False comunicazioni sociali
- Art. 2622 del Codice Civile - False comunicazioni sociali in danno della società, dei soci o dei creditori
- Art. 2623 e 173 bis del D.Lgs. 58/1998 - Falso in prospetto

Fattispecie

- Esposizioni non veritiere in bilanci, relazioni, comunicazioni sociali od omissioni di informazioni obbligatorie relativamente alla situazione economica, patrimoniale e finanziaria della società o del Gruppo al quale essa appartiene, per ingannare i soci o il pubblico.
- Prospettazioni false o comunque ingannevoli in relazione alla società nel caso di sollecitazioni all'investimento, di ammissione alla quotazione nei mercati regolamentati, di offerte pubbliche di acquisto o di scambio.

Esemplificazioni di condotte illecite

- Predisposizione impropria di dati contabili con l'intento di fornire alla struttura competente per la redazione del bilancio una situazione economica e patrimoniale non veritiera tale da alterare il bilancio, attraverso, ad esempio l'alterazione della valutazione dei crediti.

2.2 Tutela penale del capitale sociale

I reati in oggetto sono previsti da:

- Art. 2626 del Codice Civile - Indebita restituzione dei conferimenti
- Art. 2627 del Codice Civile - Illegale ripartizione degli utili e delle riserve
- Art. 2628 del Codice Civile - Illecite operazioni sulle azioni o quote sociali o della società controllante
- Art. 2629 del Codice Civile - Operazioni in pregiudizio dei creditori
- Art. 2632 del Codice Civile - Formazione fittizia del capitale

Fattispecie

– Le fattispecie di reato si realizzano nel caso di restituzione anche simulata di conferimenti ai soci ovvero liberazione dei soci dall'obbligo di eseguire i conferimenti, fuori dai casi di legittima riduzione del capitale sociale o nell'ipotesi di ripartizione di utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserve.

Esemplificazioni di condotte illecite

- Stipula di contratti fittizi con un socio/amministratore allo scopo di distribuire gli utili.
- Acquisto o sottoscrizione di azioni della Società o della sua controllante al di fuori dei casi contemplati dagli articoli 2357 e 2359 bis del Codice Civile, causando una lesione all'integrità del patrimonio sociale.

2.3 Tutela penale del funzionamento della società

I reati in oggetto sono previsti da:

- Art. 2636 del Codice Civile – Illecita influenza sull'assemblea
- Art. 2629 bis del Codice Civile – Omessa comunicazione del conflitto d'interessi
- Art. 2625 del Codice Civile – Impedito controllo

Fattispecie

- La condotta illecita si manifesta nel caso di determinazione di maggioranze in assemblea mediante il compimento di atti simulati o fraudolenti;
- La condotta illecita si manifesta quando l'amministratore o il componente del Consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione Europea, diffusi tra il pubblico in misura rilevante ovvero un soggetto sottoposto a vigilanza ai sensi del Testo Unico Bancario (n.385 del 1° settembre 1993) e del T.U.F. non dà notizia degli interessi di cui è portatore, per conto proprio o di terzi, nell'ambito di una determinata operazione societaria;
- Impedimento mediante azioni od omissioni, dello svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alla Società di Revisione.

Esemplificazioni di condotte illecite

- Omissioni o falsità nella consegna di documentazione relativa a procure o ad atti societari.
- Comunicazioni non veritiere o incomplete a fronte di richieste di informazioni da parte della Società di Revisione.

2.4 Tutela penale delle funzioni di vigilanza

CRED.IT SOCIETÀ FINANZIARIA SPA

I reati in oggetto sono previsti da:

- Art. 2638 del Codice Civile – Ostacolo all’esercizio delle funzioni delle autorità pubbliche di vigilanza

Fattispecie

- Esposizione nelle comunicazioni di fatti non rispondenti al vero sulla situazione economica, patrimoniale e finanziaria della Società ovvero occultamento di fatti sulla suddetta situazione che si sarebbero dovuti comunicare.
- Omissione di comunicazioni obbligatorie.

Esemplificazioni di condotte illecite

- Produzione e comunicazione di segnalazioni non veritiere alle autorità di vigilanza quali Banca d’Italia, Consob e Antitrust e a altre Autorità di vigilanza.

3 Attività sensibili nell’ambito dei reati societari

Le aree di attività della Società più specificatamente a rischio riguardo le fattispecie dei reati societari di cui trattasi sono le seguenti:

| Area | Macroprocessi | Reati societari | | | |
|------------|--------------------------------------|---|------------------------------------|---|---|
| | | Falsità in comunicazioni, prospetti e relazioni | Tutela penale del capitale sociale | Tutela penale del funzionamento della società | Tutela penale delle funzioni di Vigilanza |
| Governance | Affari generali (*) | | ✓ | ✓ | ✓ |
| | Controllo di gestione(*) | ✓ | | ✓ | ✓ |
| Supporto | Gestione amministrativo contabile(*) | ✓ | | | |
| | Risorse umane(*) | ✓ | | ✓ | ✓ |
| | Legale e recupero | ✓ | | | |
| | Segnalazioni di vigilanza | | | | ✓ |

4 I presidi e gli strumenti di controllo

4.1 Premessa

Nell’espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, gli organi sociali, i dipendenti e i collaboratori di Cred.it Società Finanziaria SpA devono conoscere e rispettare:

CRED.IT SOCIETÀ FINANZIARIA SPA

- i principi di Corporate Governance a cui il Gruppo si ispira, contenuti nel “Codice di Corporate Governance del Gruppo CRED.IT SOCIETÀ FINANZIARIA SPA” approvato dal Consiglio di Amministrazione della Capogruppo del 09 Novembre 2012;
- le norme di comportamento, i valori ed i principi etici enunciati nel Codice Etico;
- le procedure aziendali e di Gruppo, la documentazione e gli ordini di servizio inerenti la struttura gerarchico-funzionale aziendale ed organizzativa del Gruppo e il sistema di controllo della gestione;
- in generale, la normativa italiana e straniera applicabile.

4.2 Principi di comportamento

La presente Parte Speciale prevede l'espresso obbligo a carico dei Destinatari di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure aziendali interne, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative agli strumenti finanziari emessi dalla Società, necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della Società, sull'evoluzione della sua attività, nonché sui suoi strumenti finanziari e relativi diritti;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge;
- evitare situazioni caratterizzate da un conflitto tra il loro interesse e l'interesse di Cred.it Società Finanziaria SpA, essendo comunque tenuti a dare notizia, nelle forme di legge, di ogni interesse in conflitto che, per conto proprio o di terzi, abbiano in determinate operazioni della società;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non interponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

4.2.1 Falsità in comunicazioni, prospetti e relazioni

In particolare, a titolo meramente esemplificativo e non esaustivo, è fatto divieto di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà sulla situazione economica, patrimoniale e finanziaria della Società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- alterare i dati e le informazioni destinati alla predisposizione dei prospetti informativi;
- illustrare i dati e le informazioni utilizzate in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della Società e sull'evoluzione della sua attività, nonché sugli strumenti finanziari e relativi diritti.

4.2.2 Tutela penale del capitale sociale

In particolare, a titolo meramente esemplificativo e non esaustivo, è fatto divieto di:

- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- acquistare o sottoscrivere azioni della Società o di società controllate fuori dei casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- procedere a formazione e/o aumenti fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale.

4.2.3 Tutela penale del funzionamento della società

In particolare, a titolo meramente esemplificativo e non esaustivo è fatto divieto di porre in essere comportamenti che impediscano materialmente mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione del Collegio Sindacale o della Società di Revisione.

4.2.4 Tutela penale delle funzioni di vigilanza

In particolare, a titolo meramente esemplificativo e non esaustivo, è fatto divieto di:

- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di Vigilanza cui è soggetta l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificatamente richiesti dalle predette autorità;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità pubbliche di Vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

4.3 Principi di controllo

4.3.1 Falsità in comunicazioni, prospetti e relazioni

I documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Società e i Prospetti Informativi devono essere redatti in base alle specifiche procedure, prassi e logiche aziendali che:

- identificano con chiarezza e completezza le funzioni interessate nonché i dati e le notizie che le stesse devono fornire;
- identificano i criteri per le rilevazioni contabili dei fatti aziendali e per la valutazione delle singole poste;
- determinano le scadenze, gli argomenti oggetto di comunicazione e informativa, l'organizzazione dei relativi flussi e l'eventuale richiesta di rilascio di apposite attestazioni;

CRED.IT SOCIETÀ FINANZIARIA SPA

- prevedono la trasmissione dei dati ed informazioni alla struttura responsabile della raccolta attraverso un sistema che consente la tracciabilità delle singole operazioni e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- prevedono criteri e modalità per l'elaborazione dei dati di bilancio consolidato da parte della Capogruppo e la trasmissione degli stessi da parte delle società rientranti nel perimetro di consolidamento.

Il processo di predisposizione dei documenti contenenti Comunicazioni sociali, Prospetti Informativi e Relazioni è governato secondo linee guida declinate da un'apposita Disposizione Interna di Gruppo in risposta alle sollecitazioni provenienti dalla Legge 262/2005 ed in particolare dall'art. 154 bis del T.U.F, che ha qualificato normativamente la figura del "Dirigente Preposto alla redazione dei documenti contabili societari" a cui è affidata la responsabilità di attestare la corrispondenza delle risultanze documentali, ai libri e alle scritture contabili degli atti delle comunicazioni diffuse dalla società al mercato e relativi all'informativa contabile anche infrannuale.

In particolare, al Dirigente Preposto:

- sono conferiti gli adeguati poteri e mezzi per l'esercizio dei compiti attribuiti dalla normativa;
- è affidata la gestione dei rischi di non conformità ai postulati di bilancio nell'ambito delle procedure amministrativo-contabili e dei relativi controlli-chiave.

In tal senso, all'interno della Capogruppo è stata costituita un'apposita funzione denominata "Adempimenti di Vigilanza e Controlli Legge 262" a cui è assegnato il compito di supportare il Dirigente Preposto nell'espletamento dei propri compiti, nonché di coordinarsi con le altre funzioni del Gruppo al fine di ottemperare alle disposizioni normative.

Il sistema di controllo posto in essere da Cred.it Società Finanziaria SpA si basa sui seguenti fattori:

- Ruoli e responsabilità definiti:
 - o ogni singola struttura è responsabile dei processi che contribuiscono alla produzione delle voci contabili e/o delle attività valutative ad essa demandate e degli eventuali commenti in bilancio di propria competenza;
 - o sono definiti diversi profili di utenza per l'accesso alle procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione alle funzioni attribuite;
 - o come anticipato è istituita una specifica struttura in staff al Dirigente Preposto, nominato secondo quanto disposto dalla alla Legge 262/2005 ed in particolare dall'art 154 bis del T.U.F alla redazione dei documenti contabili e societari. In particolare la funzione Adempimenti di Vigilanza e Controlli Legge 262:
 - definisce i controlli-chiave per ciascun processo sensibile;
 - verifica sistematicamente l'adeguatezza dei controlli predisposti;
 - effettua test periodici di verifica sulla corretta esecuzione di tali controlli;
 - identifica le criticità e i relativi piani di azione correttivi;
 - o effettua il monitoraggio sull'avanzamento e sull'efficacia delle azioni correttive intraprese.
- Segregazione delle funzioni:
 - o il processo di predisposizione dei documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Società e dei Prospetti Informativi prevede il coinvolgimento di diverse strutture della Società, responsabili, relativamente alle specifiche competenze, delle diverse fasi del processo amministrativo-contabile e di redazione dei Prospetti Informativi.
- Attività di controllo:
 - o le attività di predisposizione dei documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Società e dei Prospetti Informativi, sono soggette a puntuali controlli di completezza e veridicità sia di sistema sia manuali, sia da parte delle strutture interne sia da parte delle strutture esterne incaricate (Sindaci e Revisori).
 - o Si riportano di seguito i principali controlli svolti dalle singole strutture:
 - ☉ verifiche con cadenza periodica, dei saldi dei conti di contabilità generale, al fine di garantirne la quadratura con i rispettivi partitari;

- verifica, con periodicità prestabilita, di tutti i saldi dei conti lavorazione, transitori e similari, per assicurare che le strutture interessate che hanno alimentato la contabilità eseguano le necessarie scritture nei conti appropriati;
 - produzione, per le operazioni registrate in contabilità, di prima nota contabile, debitamente validata, e della relativa documentazione giustificativa;
 - controllo di merito in sede di accensione di nuovi conti ed aggiornamento del piano dei conti;
 - quadratura della versione definitiva del bilancio con i dati contabili.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
- il processo decisionale, con riferimento all'attività di predisposizione dei documenti che contengono comunicazioni ai soci e/o al mercato, relative alla situazione economica, patrimoniale e finanziaria della Società è garantito dalla completa tracciabilità di ogni operazione contabile sia tramite sistema informatico sia tramite supporto cartaceo;
 - tutte le scritture di rettifica effettuate dalle singole strutture responsabili dei conti di propria competenza o dall'ufficio deputato alla gestione del Bilancio, sono supportate da adeguata documentazione dalla quale sia possibile desumere i criteri adottati e, analiticamente, lo sviluppo dei relativi calcoli;
 - tutta la documentazione relativa ai controlli periodici effettuati viene archiviata presso ciascun ufficio coinvolto per le voci di bilancio di propria competenza.

4.3.2 Tutela penale del capitale sociale

Tutte le operazioni sul capitale sociale di Cred.it Società Finanziaria SpA e delle società controllate, nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto del "Codice di Corporate Governance del Gruppo CRED.IT SOCIETÀ FINANZIARIA SPA" e delle procedure aziendali e di Gruppo predisposte.

4.3.3 Tutela penale del funzionamento della società

Le Strutture della Società, a qualsiasi titolo coinvolte nella gestione dei rapporti con i Comitati e la Società di Revisione, sono tenute alla massima diligenza, professionalità, trasparenza, collaborazione, disponibilità e al pieno rispetto del ruolo istituzionale degli stessi. In particolare il sistema di controllo a presidio si basa sui seguenti fattori:

- Ruoli e responsabilità definiti:
 - i rapporti con i Comitati e la Società di Revisione, sono intrattenuti dal Responsabile della struttura di riferimento o dai soggetti dal medesimo appositamente incaricati.
- Attività di controllo:
 - ciascuna struttura competente è tenuta ad evadere tempestivamente le richieste di documentazione specifica avanzate dalla Società di Revisione nell'espletamento delle proprie attività di verifica e controllo e valutazione dei processi amministrativo-contabili;
 - ciascuna struttura ha la responsabilità di raccogliere e predisporre le informazioni richieste e provvedere alla consegna delle stesse, sulla base degli obblighi contrattuali presenti nel contratto di incarico di revisione, mantenendo chiara evidenza della documentazione consegnata a risposta di specifiche richieste informative formalmente avanzate dai revisori.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - le attività di verifica e controllo dei Comitati sono sistematicamente verbalizzate;
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica.

4.3.4 Tutela penale delle funzioni di vigilanza

Il sistema di controllo a presidio si basa sui seguenti fattori:

– Ruoli e responsabilità definiti:

○ ad eccezione delle visite ispettive i rapporti con le Autorità di Vigilanza sono intrattenuti dal Responsabile della struttura di riferimento o da soggetti dallo stesso incaricati tramite delega interna, da conservare a cura della struttura medesima.

– Segregazione delle funzioni:

○ ciascuna struttura operativa competente, al ricevimento di una comunicazione/riciesta proveniente dalle Autorità di Vigilanza, ne invia una copia alla funzione Adempimenti Normativi e Compliance. La funzione Adempimenti Normativi e Compliance potrà richiedere copia di quanto predisposto dalle strutture operative prima dell'inoltro all'Autorità.

○ la Direzione accoglie le visite ispettive da parte delle Autorità di Vigilanza e, dopo aver accertato l'oggetto dell'ispezione; provvede a coinvolgere i Responsabili delle strutture interessate e ad individuare le risorse deputate a gestire i rapporti con i Funzionari pubblici durante la loro permanenza presso la Società.

– Attività di controllo:

○ la struttura responsabile della trasmissione delle informazioni alle Autorità di Vigilanza, effettua controlli di completezza ed accuratezza sul contenuto delle informazioni da inviare;

○ le segnalazioni periodiche alle Autorità di Vigilanza sono soggette a controlli automatici per verificare la corretta trasmissione delle informazioni.

– Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

○ dopo l'inoltro all'Autorità, copia di ogni lettera/nota di accompagnamento (indipendentemente dalla modalità di trasmissione utilizzata) munita della firma dell'organo competente, copia della documentazione comprovante l'avvenuta spedizione, nonché copia degli allegati dovranno essere inviate alla funzione Adempimenti Normativi e Compliance;

○ ogni comunicazione nei confronti delle Autorità avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della Società è documentata ed archiviata presso la struttura di competenza o fatte salve le situazioni in cui non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, il personale della struttura interessata che ha presenziato alla visita ispettiva assiste il Funzionario pubblico nella stesura del verbale di accertamento ed eventuale prescrizione, riservandosi le eventuali controdeduzioni, firmando, per presa visione il verbale, comprensivo degli allegati, prodotto dal Funzionario stesso;

○ ad ogni visita ispettiva da parte di Funzionari rappresentanti delle Autorità di Vigilanza il Responsabile della struttura interessata provvede a trasmettere alle Direzioni/Servizi/Uffici aziendali competenti copia del verbale rilasciato dal Funzionario pubblico e degli annessi allegati. Qualora non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, il Responsabile della struttura interessata dall'ispezione od un suo delegato provvede alla redazione di una nota di sintesi dell'accertamento effettuato e alla trasmissione della stessa alle Direzioni/Servizi/Uffici aziendali competenti. La suddetta documentazione è archiviata dal Responsabile della struttura interessata dall'ispezione.

Parte speciale 2: Reati contro la Pubblica Amministrazione

PARTE SPECIALE 2

1 Funzione della Parte Speciale seconda

La Parte Speciale seconda si riferisce ai comportamenti posti in essere dai Destinatari del Modello, ed in particolare dai soggetti coinvolti nelle attività sensibili rispetto ai reati contro la Pubblica Amministrazione. Obiettivo della presente Parte Speciale è che i suddetti soggetti adottino le presenti regole di condotta al fine di prevenire la commissione di tali reati.

In particolare, la presente Parte Speciale ha lo scopo di:

- indicare le procedure che i Destinatari del Modello sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

1.1 Definizione di Pubblica Amministrazione e di soggetti incaricati di Pubblico

Servizio

Obiettivo del presente paragrafo è indicare criteri generali ed un elenco esemplificativo dei soggetti nei cui confronti sono ipotizzabili i reati contro la Pubblica Amministrazione previsti dagli articoli 24 e 25 del D.Lgs. 231/2001.

Per quanto riguarda i reati di malversazione, indebita percezione di erogazioni e truffa in danno dello Stato o di un ente pubblico (ex. art.24), ai fini del D.Lgs. 231/2001 e del Modello, la Società, in via prudenziale, ha deciso di adottare una interpretazione ampia del concetto di Pubblica Amministrazione.

Di seguito si fornisce un'elencazione volutamente ampia, ma non esaustiva, degli enti pubblici:

- Camera dei Deputati, Senato della Repubblica, Amministrazioni dello Stato, Regioni, enti territoriali e locali, altri enti pubblici non economici, organismi di diritto pubblico comunque denominati e loro associazioni, quali:
 - Magistratura, Forze Armate e di Polizia (Guardia di Finanza, Arma dei Carabinieri, Polizia di Stato, Polizia Municipale, etc.);
 - ISVAP, Banca d'Italia, U.I.F., CONSOB, Autorità Garante della Concorrenza e del Mercato, Autorità Garante per la protezione dei dati personali, Autorità per le Garanzie nelle Comunicazioni, Autorità per l'Energia Elettrica ed il Gas;
 - Agenzia delle Entrate, Agenzia delle Dogane e del Territorio, Amministrazioni, aziende e enti del Servizio Sanitario Nazionale, Camere di commercio, industria, artigianato e agricoltura e loro associazioni, Istituti e Scuole di ogni ordine e grado e le istituzioni educative, Istituzioni universitarie;
 - ACI - Automobile Club d'Italia, ASI - Agenzia Spaziale italiana, CNEL – Consiglio Nazionale dell'Economia e del Lavoro, CNR - Consiglio Nazionale delle Ricerche, CONI – Comitato Olimpico Nazionale, CRI - Croce Rossa italiana, ENEA - Ente per le nuove tecnologie, l'energia e l'ambiente, ENPALS - Ente nazionale di previdenza e di assistenza per i lavoratori dello spettacolo, ICE – Istituto nazionale per il commercio estero, INAIL - Istituto nazionale assicurazioni infortuni sul lavoro, INPDAP - Istituto nazionale di previdenza per i dipendenti dell'amministrazione pubblica, INPS - Istituto nazionale della previdenza sociale, ISS - Istituto superiore di sanità, ISAE - Istituto di Studi e Analisi Economica, ISTAT – Istituto nazionale di statistica, IPZS - Istituto poligrafico e zecca dello Stato, Amministrazione dei Monopoli di Stato, ENASARCO - Ente Nazionale di Assistenza per gli Agenti e i Rappresentanti di Commercio, ASL - Azienda sanitaria locale.
- Organi della Commissione Europea e della Pubblica Amministrazione di Stati esteri.
- Imprese pubbliche e soggetti privati che adempiono una funzione pubblicistica, quali:
 - Poste Italiane S.p.A., RAI - Radiotelevisione Italiana, Ferrovie dello Stato;

o Enel S.p.A., Eni S.p.A., Telecom Italia S.p.A., Hera S.p.A., etc.

Per quanto riguarda i reati di concussione e corruzione (ex. art.25), le figure che assumono rilevanza a tal fine sono pubblici ufficiali e incaricati di pubblico servizio:

– ai sensi dell’art. 357, comma 1 del Codice Penale, è considerato pubblico ufficiale colui il quale esercita una pubblica funzione legislativa, giudiziaria o amministrativa;

– ai sensi dell’art. 358 del Codice Penale, “sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un’attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale”¹.

L’elemento discriminante per individuare se un soggetto rivesta o meno la qualità di incaricato di un pubblico servizio è rappresentato non dalla natura giuridica dell’ente, ma dalle funzioni affidate al soggetto, le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

I Destinatari del Modello devono prestare la massima attenzione nei rapporti, di qualsiasi tipo ed a qualsiasi livello, con i soggetti sopra elencati ed i loro dirigenti, dipendenti e collaboratori.

2 I reati contro la Pubblica Amministrazione

(I reati contro la Pubblica Amministrazione: esegesi delle norme rilevanti ed esemplificazioni di condotte illecite)

Il presente paragrafo si riferisce ai reati nei confronti della Pubblica Amministrazione secondo le fattispecie contemplate dagli artt. 24 e 25 del D.Lgs. 231/2001, limitatamente ai casi che potrebbero configurarsi in capo alla Società.

2.1 Malversazione a danno dello Stato

I reati in oggetto sono previsti da:

– Art. 316 bis del Codice Penale – Malversazione ai danni dello Stato o dell’Unione Europea

Fattispecie

– La fattispecie di reato si configura nel caso in cui, dopo aver ottenuto contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non si proceda all’utilizzo delle somme ottenute per gli scopi a cui erano destinate.

¹ Il servizio, affinché possa definirsi pubblico, deve essere disciplinato – così come la pubblica funzione - da norme di diritto pubblico, ma senza i poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

Esemplificazioni di condotte illecite

– Concorso nel reato di malversazione a danno dello Stato o dell’Unione Europea commesso da propri clienti, mediante consapevole rilascio di lettere di referenze o garanzie fideiussorie a garanzia di contributi a fondo perduto o agevolazioni da parte dello Stato o dell’Unione Europea, nella consapevolezza che tali erogazioni verranno distratte dal loro fine.

2.2 Indebita percezione di erogazioni a danno dello Stato

I reati in oggetto sono previsti da:

- Art. 316 ter del Codice Penale – Indebita percezione di erogazioni a danno dello Stato

Fattispecie

– La fattispecie di reato si realizza nel caso in cui, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dalla comunità Europea.

Esemplificazioni di condotte illecite

– Falsificazione di questionari finalizzati ad ottenere finanziamenti pubblici per la formazione del personale dipendente.

2.3 Corruzione e concussione

I reati in oggetto sono previsti da:

- Art. 317 del Codice Penale – Concussione
- Art. 318 del Codice Penale – Corruzione per un atto d'ufficio
- Art. 319 del Codice Penale – Corruzione per un atto contrario ai doveri d'ufficio
- Art. 319 bis del Codice Penale - Circostanze aggravanti
- Art. 320 del Codice Penale - Corruzione di persona incaricata di un pubblico servizio
- Art. 321 del Codice Penale – Pene per il corruttore
- Art. 322 del Codice Penale - Istigazione alla corruzione
- Art. 322 bis del Codice Penale – Peculato, concussione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri.

Fattispecie

– La fattispecie di reato di corruzione si realizza quando un pubblico ufficiale o un incaricato di pubblico servizio, riceva per sé o un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta, o ne accetti la promessa.

– La fattispecie di reato di concussione si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli.

Esemplificazioni di condotte illecite

- Liquidazione di provvigioni "gonfiate" alla Rete Commerciale che potrebbero essere utilizzate per la corruzione di funzionari pubblici.
- Concessione di credito alla clientela pur in presenza di requisiti economici/di rischio inadeguati ad ottenere l'erogazione del credito a scopo corruttivo.
- Offerta di denaro ad un funzionario pubblico per ottenere l'assegnazione di una gara d'appalto indetta dall'ente.
- Creazione di fondi neri da utilizzare a scopo corruttivo mediante il pagamento di fatture fittizie.

2.4 Corruzione in atti giudiziari

I reati in oggetto sono previsti da:

- Art. 319 ter del Codice Penale - Corruzione in atti giudiziari

Fattispecie

- Tale ipotesi di reato si configura nel caso in cui la Società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (un magistrato, un cancelliere o altro funzionario).

Esemplificazioni di condotte illecite

- Versamento di denaro ad un cancelliere del Tribunale affinché accetti delle memorie o delle produzioni documentali fuori termine, consentendo quindi di superare i limiti temporali previsti dai codici di procedura.
- Pagamento di una parcella maggiorata o alterazione dell'incarico dei legali in contatto con Organi giudiziari affinché condizionino favorevolmente l'esito di un processo a carico della Società.

2.5 Truffa in danno dello Stato o di altro ente pubblico

I reati in oggetto sono previsti da:

- Art. 640 comma 2, n.1 del Codice Penale – Truffa in danno dello Stato o di altro ente pubblico
- Art. 640 bis del Codice Penale – Truffa aggravata per il conseguimento di erogazioni pubbliche
- Art. 640 ter del Codice Penale. – Frode informatica, rilevante ai fini del D.Lgs. 231/2001 solo se commesso in danno dello Stato o di altro ente pubblico

Fattispecie

- Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto per la Società, siano posti in essere artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro ente pubblico o all'Unione Europea).

Esemplificazioni di condotte illecite

- Predisposizione di documenti falsi per la partecipazione a procedure di gara al fine di ottenere l'aggiudicazione della gara stessa.

3 Attività sensibili nell'ambito dei reati contro la Pubblica Amministrazione

Le aree di attività della Società più specificatamente a rischio riguardano le fattispecie di reati contro la Pubblica Amministrazione di cui trattasi sono le seguenti:

| Reati contro la Pubblica Amministrazione | | | | | | |
|--|--------------------------|-------------------------------------|---|---|-------------------------------|-----------------------------|
| Area | Macro Processo | Malversazioni e a danno dello Stato | Indebita percezione di erogazioni a danno dello Stato | Corruzione e concussione di funzionari pubblici | Corruzione in atti giudiziari | Truffa in danno dello Stato |
| Governance | Servizi societari(*) | | | ✓ | | |
| | Controllo di gestione(*) | | | ✓ | | |
| Business | Conc. del credito | | | ✓ | | ✓ |
| | G. commerciale | | | | | ✓ |
| | G. mandati rete | | | ✓ | | |
| | G. contratti | | | | | ✓ |
| Supporto | G. amm. Contab. | | | ✓ | | ✓ |
| | Ris. Umane(*) | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Legale e recupero | | | ✓ | | |
| | Immobiliare(*) | | | ✓ | | |

4 I presidi e gli strumenti di controllo

4.1 Premessa

Nell'espletamento di tutte le operazioni che comportano rapporti con la Pubblica Amministrazione, come definito precedentemente, oltre alle regole di cui al presente Modello, gli organi sociali, i dipendenti e i collaboratori di Cred.it Società Finanziaria SpA devono conoscere e rispettare:

- le norme di comportamento, i valori ed i principi etici enunciati nel Codice Etico;
- le procedure aziendali e di Gruppo, la documentazione e gli ordini di servizio inerenti la struttura gerarchico - funzionale aziendale ed organizzativa del Gruppo;
- in generale, la normativa italiana e straniera applicabile.

4.2 Principi di comportamento

I seguenti principi di carattere generale si applicano agli organi sociali e ai dipendenti in via diretta ed ai collaboratori in forza di apposite clausole contrattuali.

I Responsabili delle funzioni in contatto con la Pubblica Amministrazione devono:

- provvedere almeno annualmente a formare i propri collaboratori, fornendo direttive sulle modalità di condotta operativa da adottare nei contatti formali ed informali intrattenuti con i diversi soggetti pubblici, trasferendo conoscenza della normativa e consapevolezza delle situazioni a rischio di reato;
- prevedere adeguati meccanismi di tracciabilità dei flussi informativi verso la Pubblica Amministrazione.

Gli incarichi, conferiti a soggetti esterni, di rappresentare Cred.it Società Finanziaria SpA nei confronti della Pubblica Amministrazione devono essere assegnati in modo formale.

Nei contratti con i collaboratori è contenuta apposita dichiarazione dei medesimi con cui si afferma:

- di essere a conoscenza della normativa di cui al D.Lgs. 231/2001 e delle sue implicazioni per la Società;
- di non essere mai stati implicati in procedimenti giudiziari relativi ai reati nello stesso contemplati (o, se lo sono stati, devono dichiararlo ai fini di una maggiore attenzione da parte della Società in caso si addivenga all'instaurazione del rapporto);
- di impegnarsi al rispetto dei principi del Decreto.

I Destinatari che siano membri di organi elettivi di Pubbliche Amministrazioni ovvero che collaborino, anche in veste di dipendenti, con le Pubbliche Amministrazioni, si astengono dal compiere atti nei quali essi siano portatori di interessi in potenziale conflitto con quelli della Società.

Di seguito sono dettagliati i principi di comportamento specifici per prevenire il compimento di ciascuna tipologia di reato.

4.2.1 Malversazione a danno dello Stato

In particolare a titolo meramente esemplificativo e non esaustivo è fatto divieto ai Destinatari di destinare contributi/sovvenzioni/finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti.

4.2.2 Indebita percezione di erogazioni a danno dello Stato

In particolare a titolo meramente esemplificativo e non esaustivo è fatto divieto ai Destinatari di:

- esibire alla Pubblica Amministrazione documenti/dati falsi o alterati;
- omettere informazioni dovute al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione.

4.2.3 Corruzione e concussione di funzionari pubblici o di persone incaricate di pubblico

Servizio

In particolare a titolo meramente esemplificativo e non esaustivo è fatto divieto ai Destinatari di:

- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore;
- promettere o effettuare erogazioni in denaro per finalità diverse da quelle istituzionali e di servizio;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;
- promettere o concedere omaggi/regalie non di modico valore;
- riconoscere compensi in favore dei collaboratori esterni, ivi compresi i legali, che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti;
- promettere o accordare somme di denaro, doni, prestazioni gratuite o vantaggi di qualsiasi natura a pubblici ufficiali o persone incaricate di pubblico servizio al fine di favorire interessi della Società.

4.2.4 Corruzione in atti giudiziari

In particolare a titolo meramente esemplificativo e non esaustivo è fatto divieto ai Destinatari di:

- effettuare pagamenti di parcelle maggiorate ai legali o di altri soggetti coinvolti in processi di rappresentanza legale della Società al fine di costituire fondi per comportamenti corruttivi;
- adottare comportamenti contrari alle leggi e al Codice Etico, in tutte le fasi del procedimento anche a mezzo di professionisti esterni e soggetti terzi per favorire indebitamente gli interessi della Società.

4.2.5 Truffa in danno dello Stato o di altro ente pubblico

In particolare a titolo meramente esemplificativo e non esaustivo è fatto divieto ai Destinatari di tenere condotte ingannevoli che possano indurre la Pubblica Amministrazione in errore nella valutazione tecnicoeconomica dei prodotti e servizi offerti/forniti.

4.3 Principi di controllo

4.3.1 Malversazione a danno dello Stato ed indebita percezione di erogazioni a danno dello

Stato

Le Strutture della Società, a qualsiasi titolo coinvolte nelle attività di richiesta e gestione di contributi, sovvenzioni e finanziamenti pubblici sono tenute ad osservare le modalità esposte nel presente Modello, le procedure aziendali e di Gruppo predisposte.

In particolare la richiesta di contributi/sovvenzioni/finanziamenti pubblici deve avvenire in conformità ad apposite procedure formalizzate ed appositi controlli.

Il sistema di controllo a presidio si basa sui seguenti fattori:

– Ruoli e responsabilità definiti:

- tutti i soggetti che intervengono a qualsiasi titolo nella gestione delle richieste di concessione di contributi, sovvenzioni e finanziamenti che abbiano carattere pubblico devono essere individuati ed autorizzati dal Responsabile della struttura di riferimento tramite delega interna, da conservare a cura della struttura medesima;

- le richieste di contributi/sovvenzioni/finanziamenti pubblici sono sottoscritte dal Responsabile della struttura competente specificamente e formalmente facoltizzato in virtù del vigente sistema dei poteri e delle deleghe;

- in caso di ricorso a consulenti esterni, il processo di attribuzione dell'incarico avviene secondo le modalità previste dalle procedure aziendali, in ogni caso prevedendo l'acquisizione di una pluralità di offerte e la scelta mediante criteri oggettivi e codificati.

– Segregazione delle funzioni:

- la struttura competente attribuisce a ciascun ufficio le attività operative e di controllo, al fine di garantire la contrapposizione dei ruoli tra i soggetti che gestiscono le fasi istruttorie e realizzative e i soggetti deputati alle attività di verifica.

– Attività di controllo:

- la struttura competente è responsabile della verifica della coerenza dei contenuti del progetto rispetto a quanto disposto dalle direttive del bando di finanziamento;

- la struttura competente è altresì responsabile dei controlli sulla regolarità formale e sostanziale della documentazione da consegnare per l'accesso al bando di finanziamento;

- sono inoltre predisposti a cura della struttura competente, accertamenti periodici derivanti da specifici obblighi di controllo e monitoraggio previsti dal bando. In particolare, per quanto riguarda la formazione finanziata:

- tenuta del registro delle presenze durante l'erogazione dei progetti formativi;
- raccolta e verifica della documentazione degli oneri aziendali dei dipendenti;
- raccolta a verifica delle parcelle/ fatture relative ai costi sostenuti per l'iniziativa;
- verifica sulla puntuale e corretta contabilizzazione degli introiti.

– Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta, ivi inclusa quella trasmessa all'ente finanziatore, anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività di richiesta di contributi/sovvenzioni/finanziamenti pubblici.

4.3.2 Concussione e corruzione di funzionari pubblici e truffa in danno dello Stato

Le Strutture della Società e i collaboratori, a qualsiasi titolo coinvolte in attività che comportano rapporti con la Pubblica Amministrazione sono tenuti ad osservare le modalità esposte nel presente Modello nonché le procedure aziendali e di Gruppo predisposte.

Il sistema di controllo atto a prevenire i reati di concussione e corruzione e truffa in danno dello Stato o di altro ente pubblico, si basa sui seguenti fattori:

– Ruoli e responsabilità definiti:

- gli atti che impegnano contrattualmente la Società nei confronti della Pubblica Amministrazione devono essere sottoscritti soltanto dai soggetti appositamente incaricati;
- la gestione dei rapporti con i funzionari pubblici in caso di accertamenti/sopralluoghi è attribuita al Responsabile della struttura competente e/o ai soggetti da quest'ultimo appositamente individuati;
- al fine di evitare la generazione di fondi da utilizzare per azioni corruttive, il processo degli acquisti avviene secondo apposita procedura aziendale formalizzata che prevede che l'approvazione della richiesta di acquisto, la scelta dei fornitori, il perfezionamento del contratto, l'emissione dell'ordine e l'autorizzazione al pagamento spettino esclusivamente ai soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere;
- la scelta dei fornitori di beni e servizi e dei professionisti avviene tra i nominativi selezionati in base a criteri individuati nell'ambito della normativa interna, fatte salve esigenze/forniture occasionali che devono essere adeguatamente motivate;
- il pagamento delle fatture è effettuato da una specifica struttura aziendale dedicata;
- il processo di selezione e assunzione del personale è accentrato in capo alla struttura competente della Capogruppo che riceve le richieste formali di nuovo personale da parte delle strutture interessate e le valuta in coerenza con il budget ed i piani interni di sviluppo;
- il processo di selezione dei fiduciari (ad esempio legali) è accentrato in capo alle strutture competenti che provvedono alla gestione di appositi albi;
- tutte le deliberazioni relative alle compravendite ed alle locazioni immobiliari spettano esclusivamente a soggetti muniti di idonei poteri in base al vigente sistema dei poteri e delle deleghe che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno;
- sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite.

– Segregazione dei compiti:

- le Strutture incaricate della gestione operativa dei prodotti/servizi contrattualizzati, sono diverse da quelle incaricate dello sviluppo commerciale;
- tutta la corrispondenza inerente a rilievi o eccezioni relative alla sfera dell'operatività aziendale indirizzata alle Autorità di Vigilanza è preventivamente condivisa con la funzione Legale;
- è compito del Responsabile della struttura interessata dalla visita ispettiva, dopo aver accertato l'oggetto dell'ispezione, individuare le risorse deputate a gestire i rapporti con i funzionari pubblici durante la loro permanenza presso la Società. Le funzioni Legale, Internal Audit, Compliance e nei casi particolarmente rilevanti l'Organismo di Vigilanza devono essere tempestivamente informate della visita ispettiva in atto e di eventuali prescrizioni o eccezioni rilevate dall'Autorità. – Attività di controllo:
 - la stipula di contratti da parte della Società con soggetti pubblici attraverso la partecipazione a procedure ad evidenza pubblica (appalto-concorso, asta pubblica, licitazione privata e trattativa privata), deve avvenire in conformità ad apposite procedure diramate dalle Direzioni competenti, che prevedono il monitoraggio dei limiti assuntivi, specifici controlli ed anche appositi blocchi automatici sul sistema informativo;
 - il rilascio di garanzie fidejussorie necessarie per ottenere erogazioni pubbliche da parte di propri garantiti deve rispettare le apposite procedure, che prevedono il monitoraggio dei limiti assuntivi, specifici controlli e appositi blocchi automatici sul sistema informativo;
 - la normativa interna di riferimento identifica i controlli che devono essere svolti dalle strutture competenti in merito a:

- verifica dei limiti di spesa e di pertinenza della stessa;
- monitoraggio degli incarichi affidati a professionisti/consulenti e del relativo corrispettivo;
- in fase di selezione del personale, i candidati compilano un'apposita modulistica per garantire la raccolta omogenea delle informazioni. Tale modulistica prevede in particolare l'autocertificazione del possesso dei requisiti di legge per l'assunzione e la dichiarazione di eventuali legami con esponenti della Pubblica Amministrazione;
- la normativa interna identifica i controlli che devono essere svolti dalle strutture competenti in merito alla gestione immobiliare, con particolare riguardo a:
 - verifica della congruità del canone di locazione passiva e attiva per tutte le nuove locazioni e le rinegoziazioni;
 - effettuazione delle attività di due diligence sulla controparte;
 - verifica della congruità del prezzo di compravendita dell'immobile rispetto al valore di mercato, anche attraverso l'acquisizione di perizie redatte da esperti indipendenti ogni qualvolta la controparte sia una Pubblica Amministrazione o un esponente della medesima;
- per ciascuna struttura interessata allo svolgimento delle attività di natura contabile/amministrativa sono definiti specifici controlli di linea in riferimento ad apposite procedure interne. I controlli sono volti ad assicurare la verifica della regolarità delle operazioni nonché della completezza, della correttezza e tempestività delle scritture contabili.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
 - per ciascuna fase rilevante degli accordi con la Pubblica Amministrazione le procedure di Cred.it Società Finanziaria SpA prevedono che la documentazione prodotta venga, archiviata dalla struttura competente in apposito fascicolo da tenere aggiornato, con modalità formalizzata, nel corso dello svolgimento dell'attività;
 - ogni accordo/convenzione/contratto con la Pubblica Amministrazione è formalizzato in un documento debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
 - la realizzazione delle operazioni nella esecuzione degli adempimenti contrattuali verso la Pubblica Amministrazione prevede l'utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle informazioni elaborate. Le strutture provvedono alla archiviazione della documentazione cartacea inerente all'esecuzione degli adempimenti svolti;
 - la struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione del processo di acquisto di beni e servizi, con particolare riferimento alla fase di individuazione del fornitore/professionista in termini di motivazione della scelta e pertinenza/congruità della spesa;
 - la struttura di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente al processo di selezione e assunzione del personale e di selezione dei fiduciari;
 - ogni atto dispositivo relativo alla gestione immobiliare è formalizzato in apposito documento, debitamente firmato da soggetti muniti di idonei poteri, ed archiviato a cura della struttura competente.
- Sistemi premianti o di incentivazione:
 - i sistemi premianti e di incentivazione della Società sono concepiti per assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente Modello, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

4.3.3 Corruzione in atti giudiziari

Il sistema di controllo atto a prevenire il reato di corruzione in atti giudiziari si basa sui seguenti fattori:

– Ruoli e responsabilità definiti:

- la gestione dei contenziosi e degli accordi transattivi prevede l'accentramento delle responsabilità di indirizzo e/o gestione e monitoraggio in capo a diverse strutture della Società, a seconda che si tratti di

profili giuridici di natura amministrativa, civile, penale, fiscale, giuslavoristica e previdenziale. Nell'ambito di ciascuna fase del processo:

- il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla definizione delle transazioni, nonché le facoltà di autonomia per la gestione del contenzioso;
- il conferimento degli incarichi a legali esterni avviene nell'ambito dell'albo predisposto. Eventuali incarichi a legali esterni diversi da quelli individuati nell'albo devono essere adeguatamente motivati e autorizzati dal Responsabile della struttura competente;
- la struttura competente effettua un costante monitoraggio degli sviluppi processuali per poter prontamente valutare opportunità transattive che dovessero profilarsi all'esito dell'attività istruttoria o in corso di causa.

– Attività di controllo:

o le strutture competenti provvedono periodicamente alla rilevazione e monitoraggio delle vertenze pendenti e alla verifica della regolarità, completezza e correttezza di tutti gli adempimenti connessi a vertenze e transazioni.

– Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

- o ciascuna fase rilevante del contenzioso deve risultare da apposita documentazione scritta;
- o al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la struttura competente è responsabile dell'archiviazione e della conservazione della documentazione di competenza, anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività di gestione dei contenziosi e degli accordi transattivi.

Parte speciale 3: Reati di market Abuse e Aggiotaggio

PARTE SPECIALE 3

1 Funzione della Parte Speciale terza

La Parte Speciale terza si riferisce ai comportamenti posti in essere dai Destinatari del Modello, ed in particolare dai soggetti coinvolti nelle attività sensibili ai reati di Market Abuse e Aggiotaggio.

Lo scopo preventivo è di particolare importanza dal momento che obiettivo primario della norma penale è la tutela del mercato e del risparmio.

Obiettivo della presente Parte Speciale è che i suddetti soggetti adottino le presenti regole di condotta al fine di prevenire la commissione di tali reati.

In particolare, la presente Parte Speciale ha lo scopo di:

- indicare le procedure che i Destinatari del Modello sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

2 I reati di Market Abuse e di aggioaggio

(I reati di Market Abuse e di aggioaggio: esegesi delle norme rilevanti ed esemplificazioni di condotte illecite)

Il presente paragrafo si riferisce sia alle fattispecie di reato introdotte con L. 62/05, e previste agli articoli 184 e 185 del T.U.F., sia alla fattispecie di aggioaggio, prevista dall'art. 2637 c.c., come modificato dalla suddetta normativa, limitatamente ai casi che potrebbero verificarsi in relazione all'operatività della Società. Si riferisce inoltre alle fattispecie di illeciti amministrativi previste agli articoli 187 bis e 187 ter del T.U.F. per i quali è previsto, all'art. 187 quinquies del T.U.F. un regime di responsabilità dell'ente.

2.1 Abuso di informazioni privilegiate

Le fattispecie in oggetto sono previste da:

- Art. 184 del T.U.F. - Abuso di informazioni privilegiate
- Art. 187 bis del T.U.F. - Abuso di informazioni privilegiate

Fattispecie

– Partendo dal possesso di informazioni privilegiate, è punito il soggetto che, proprio approfittando delle suddette informazioni, compie operazioni di acquisto/vendita di strumenti finanziari al fine di trarne profitto, oppure divulga illecitamente (in quanto al di fuori del normale esercizio delle proprie mansioni) le suddette informazioni, oppure, ancora, induce soggetti terzi a compiere operazioni su strumenti finanziari, facendo leva sulle summenzionate informazioni.

Esemplificazioni di condotte illecite

– Utilizzo o divulgazione a vantaggio della Società di informazioni privilegiate, riguardanti società quotate clienti, in merito alle loro posizioni creditizie/debitorie.

2.2 Manipolazione del mercato ed aggio

Le fattispecie in oggetto sono previste da:

- Art. 185 del T.U.F. - Manipolazione del mercato
- Art. 187 ter del T.U.F. - Manipolazione del mercato
- Art. 2637 del Codice Civile - Aggio

Fattispecie

- Art. 185 T.U.F. - E' punito chiunque diffonde notizie false o pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.
- Art. 187 ter T.U.F. - Salve le sanzioni penali quando il fatto costituisce reato, è punito chiunque, tramite mezzi di informazione, compreso internet o ogni altro mezzo, diffonde informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti in merito agli strumenti finanziari. E' inoltre punito chiunque pone in essere:
 - o operazioni od ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
 - o operazioni od ordini di compravendita che consentono, tramite l'azione di una o di più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più strumenti finanziari ad un livello anomalo o artificiale;
 - o operazioni od ordini di compravendita che utilizzano artifici od ogni altro tipo di inganno o di espediente;
 - o altri artifici idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.
- Art. 2637 del Codice Civile - Il reato si configura con la diffusione di notizie false, la messa in essere di operazioni simulate od ogni altro artificio, purché idonei a provocare una sensibile alterazione dei prezzi degli strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, o ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

Esemplificazioni di condotte illecite

- Diffusione sul mercato, anche attraverso internet, di notizie non veritiere, ma dotate di particolare credibilità, in ordine ad importanti operazioni economiche effettuate da CRED.IT SOCIETÀ FINANZIARIA SPA, in modo da condizionare il prezzo dello strumento finanziario .
Un'interessante casistica di manipolazioni di mercato è contenuta nella comunicazione Consob n. DME/5078692 del 29.11.2005 che può essere utilmente consultata.

3 Attività sensibili nell'ambito dei reati di market abuse e di aggio

Le aree di attività di Cred.it Società Finanziaria SpA più specificatamente a rischio riguardo le fattispecie dei reati di market abuse e di aggio di cui trattasi sono le seguenti:

- concessione del credito
- gestione commerciale
- segnalazione di vigilanza

4 I presidi e gli strumenti di controllo

4.1 Premessa

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, oltre alle regole di cui al presente Modello, gli organi sociali, i dipendenti e i collaboratori della Società devono conoscere e rispettare:

- i principi di Corporate Governance a cui il Gruppo si ispira, contenuti nel “Codice di Corporate Governance del Gruppo CRED.IT SOCIETÀ FINANZIARIA SPA” approvato dal Consiglio di Amministrazione della Capogruppo del 10 maggio 2007;
- le norme di comportamento, i valori ed i principi etici enunciati nel Codice Etico;
- le regole di internal dealing contenute nella “Procedura per la comunicazione delle operazioni aventi ad oggetto azioni emesse da Cred.it Società Finanziaria SpA S.p.A. o altri strumenti finanziari ad esse collegati” istituita a norma degli Artt. 114, comma settimo del D.Lgs. 58/1998 e 152 sexies e ss. del Regolamento adottato da Consob con Delibera n. 11971 del 14 maggio 1999 e successive modificazioni, approvata dal Consiglio di Amministrazione della Capogruppo del 13 settembre 2007;
- le norme per la gestione e la comunicazione delle informazioni privilegiate ai sensi della normativa sugli “Abusi di Mercato” contenute nella Disposizione Interna di Gruppo emanata in data 11 febbraio 2008 e gli allegati “Procedura per la gestione e la comunicazione delle Informazioni Privilegiate” e “Linee Guida”;
- le procedure aziendali e di Gruppo, la documentazione e gli ordini di servizio inerenti la struttura gerarchico-funzionale aziendale ed organizzativa del Gruppo;
- in generale, la normativa italiana e straniera applicabile.

4.2 Principi di comportamento

La presente Parte Speciale prevede l'espresso obbligo a carico dei Destinatari di tenere comportamenti in linea con i principi di correttezza ed onestà, oltre che rispettosi dei doveri di riservatezza inerenti alla gestione delle informazioni in proprio possesso.

In tal senso, chiunque venga a conoscenza, in modo regolare o occasionale, anche in ragione delle sue funzioni, di informazioni privilegiate aventi ad oggetto le Società del Gruppo e/o Società terze è tenuto a:

- mantenerle strettamente riservate e non diffonderle al di fuori del normale esercizio del lavoro;
- astenersi dall'effettuare, raccomandare o indurre altri ad effettuare operazioni sulla base delle stesse, che abbiano l'effetto di procurare a sé e al Gruppo un profitto.

4.2.1 Abuso di informazioni privilegiate

In relazione a tali possibili condotte illecite è fatto obbligo:

- di mantenere riservate tutte le informazioni e i documenti acquisiti nello svolgimento delle proprie funzioni, sia aventi ad oggetto la Società o la Capogruppo, sia riguardanti società terze in rapporto d'affari con la Società nonché di utilizzare le informazioni o i documenti stessi esclusivamente per l'espletamento dei propri compiti lavorativi;
- secondo quanto stabilito dalle “Linee Guida” per la gestione delle informazioni privilegiate, di custodire accuratamente documenti contenenti informazioni confidenziali e riservate provvedendo a:
 - assicurare la tracciabilità della gestione delle informazioni privilegiate, a partire dal momento in cui ne siano entrati in possesso, attraverso la compilazione di apposite liste di distribuzione;
 - accertare che, qualora le informazioni privilegiate debbano essere comunicate a terzi per ragioni d'ufficio, costoro siano soggetti ad un obbligo di riservatezza legale, regolamentare o statutario ed eventualmente formalizzare un apposito accordo contenente vincoli di confidenzialità;
 - identificare i documenti contenenti informazioni privilegiate attraverso la dicitura “Riservato – Price Sensitive” e provvedere a proteggerli tramite password se trasmessi/archiviati in modo elettronico ovvero

ad archivarli in appositi locali ad accesso fisico controllato ovvero in archivi protetti da adeguati sistemi di sicurezza se cartacei.

E' fatto espresso divieto di:

- comunicare le informazioni privilegiate a terzi per ragioni diverse da quelle di ufficio ovvero raccomandare o indurre terzi a compiere operazioni connesse alle informazioni privilegiate;
- discutere informazioni privilegiate in luoghi pubblici o in locali in cui siano presenti estranei o comunque soggetti che non hanno necessità di conoscere tali informazioni.

4.2.2 Manipolazione del mercato e agiotaggio

In relazione a tali possibili condotte illecite è fatto esplicito divieto di:

- diffondere attraverso qualsiasi canale informativo informazioni, voci o notizie non corrispondenti alla realtà, ovvero informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti in relazione alla Società o al Gruppo nonché in relazione a società terze in rapporto d'affari con la Società o il Gruppo;

4.3 Principi di controllo

4.3.1 Abuso di informazioni privilegiate

Il sistema di controllo a presidio della corretta gestione delle informazioni privilegiate si basa sui seguenti fattori:

– Ruoli e responsabilità definiti:

- la trasmissione a terzi delle informazioni privilegiate è riservata all'Alta Direzione e ai Responsabili di Direzione, che la effettuano secondo un criterio di opportunità e funzionalità, avvertendo i destinatari della rilevanza delle informazioni trasmesse, e segnalando tempestivamente i nominativi dei destinatari per l'iscrizione nel Registro istituito ai sensi dell'art. 115 bis del T.U.F.;
- la comunicazione delle informazioni privilegiate è riservata alle strutture identificate dalla "Procedura per la gestione e la comunicazione delle Informazioni Privilegiate" secondo le modalità e le responsabilità definite.

– Tracciabilità del processo:

- istituzione del Registro delle persone aventi accesso ad informazioni privilegiate ai sensi dell'art. 115 bis del T.U.F. La normativa interna definisce il processo per l'alimentazione e la gestione del Registro, nonché le funzioni aziendali responsabili della gestione. I Destinatari in possesso di informazioni privilegiate sono iscritti nel Registro e informati di tale iscrizione e degli obblighi e delle sanzioni che derivano loro.

4.3.2 Manipolazione del mercato e agiotaggio

Il sistema di controllo a presidio si basa sui seguenti fattori:

– Ruoli e responsabilità definiti:

- sono definiti limiti operativi e procedure autorizzative in funzione del ruolo e dell'esperienza del personale interessato.

– Segregazione delle funzioni:

- separatezza organizzativa tra le strutture che hanno a disposizione informazioni privilegiate (con particolare riferimento alle strutture che gestiscono la relazione commerciale con la clientela, che svolgono attività assuntive e liquidative nell'ambito delle quali possono entrare in possesso di informazioni privilegiate) e le strutture che hanno rapporti diretti con il mercato.

Parte speciale 4: Reati di riciclaggio, ricettazione e impiego di beni-denaro o altra utilità di provenienza illecita e i reati con finalità di terrorismo o di eversione dell'ordine democratico

PARTE SPECIALE 4

1 Funzione della Parte Speciale quarta

La Parte Speciale quarta si riferisce ai comportamenti posti in essere dai Destinatari del Modello, ed in particolare dai soggetti coinvolti nelle attività sensibili riconducibili rispetto ai reati introdotti con il D.Lgs. 231/07 e che ha recepito la “Terza Direttiva in materia Antiriciclaggio”.

L’implementazione nel Modello della presente fattispecie di reato è di fondamentale importanza, in considerazione dello scopo del Decreto 231/07 (prevenire i fenomeni di riciclaggio di denaro e di finanziamento del terrorismo) e in considerazione del fatto che sia le Compagini bancarie sia le Compagini Assicurative sono state tra i primi soggetti individuati dal legislatore come destinatari della normativa in materia di antiriciclaggio.

Obiettivo della presente Parte Speciale è che i suddetti soggetti adottino le presenti regole di condotta al fine di prevenire la commissione di tali reati.

In particolare, la presente Parte Speciale ha lo scopo di:

- indicare le procedure che i Destinatari del Modello sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all’OdV, e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

2 I reati di riciclaggio, ricettazione e terrorismo

(I reati di riciclaggio, ricettazione e impiego di beni – denaro o altra utilità – di provenienza illecita e i reati con finalità di terrorismo o di eversione dell’ordine democratico: esegesi delle norme rilevanti ed esemplificazioni di condotte illecite)

Il presente paragrafo si riferisce alle fattispecie di reato di ricettazione, riciclaggio e impiego di denaro, beni e utilità di provenienza illecita introdotti recentemente all’art 25 octies del D.Lgs. 231/2001 e ai reati con finalità di terrorismo e di eversione dell’ordine democratico previsti dall’art. 25 quater del D.Lgs. 231/2001, limitatamente ai casi che potrebbero configurarsi in capo alla Società.

I reati in oggetto sono previsti da:

- Art. 648 del Codice Penale – Ricettazione
- Art. 648 bis del Codice Penale – Riciclaggio
- Art. 648 ter del Codice Penale – Impiego di denaro, beni o utilità di provenienza illecita
- Codice Penale e Leggi Speciali per i delitti aventi finalità di terrorismo o di eversione dell’ordine democratico
- Art. 2 della Convenzione Internazionale per la repressione del finanziamento al terrorismo, New York, 9 dicembre 1999
- Art. 600 del Codice Penale – Riduzione o mantenimento in schiavitù o in servitù
- Art. 601 del Codice Penale – Tratta di persone
- Art. 602 del Codice Penale – Acquisto e alienazione di schiavi
- Art. 600 bis del Codice Penale – Prostituzione minorile
- Art. 600 ter del Codice Penale – Pornografia minorile
- Art. 600 quater del Codice Penale – Detenzione di materiale pornografico
- Art. 600 quinquies del Codice Penale – Iniziative turistiche volte allo sfruttamento della prostituzione minorile
- Art. 600 quater 1 del Codice Penale – Pornografia virtuale

CRED.IT SOCIETÀ FINANZIARIA SPA

- Art. 416 del Codice Penale – Associazione per delinquere
- Art. 416 bis del Codice Penale – Associazione di tipo mafioso
- Art. 291 quater T.U. 23 gennaio 1973, n. 43 – Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri
- Art. 74 T.U. 9 ottobre 1990, n. 309 – Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope
- Art. 12 T.U. 25 luglio 1998, n. 286 – Disposizioni contro le immigrazioni clandestine
- Art. 377 bis del Codice Penale – Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- Art. 378 del Codice Penale – Favoreggiamento personale

Fattispecie

La fattispecie di reato di ricettazione si realizza mediante acquisto, ricezione o occultamento di denaro o cose provenienti da un qualsiasi delitto oppure, in alternativa, con l'intromissione di un soggetto nel far sì che i beni rinvenuti da reato vengano da altri acquistati, ricevuti od occultati.

La fattispecie di reato di riciclaggio si realizza mediante la sostituzione o il trasferimento di beni, denaro o altre utilità rinvenuti da delitto non colposo, ovvero il compimento di operazioni, in relazione ai beni, al denaro, alle altre utilità, tali da ostacolare l'identificazione della loro provenienza delittuosa.

La fattispecie di reato relativa all'impiego di denaro, beni o utilità di provenienza illecita si differenzia dal reato di riciclaggio poiché, mentre quest'ultimo reato prevede la sostituzione, il trasferimento o le operazioni di ostacolo all'identificazione della provenienza illecita, la figura in esame punisce l'impiego in attività economiche o finanziarie delle stesse.

Le fattispecie di reato con finalità di terrorismo e/o di eversione dell'ordine democratico si realizzano nel concorso nei suddetti reati commessi da propri clienti, fornitori o garantiti.

Esemplificazioni di condotte illecite

- Collocamento di titoli ad un investitore per il quale la registrazione dei dati di identificazione ai fini della normativa antiriciclaggio risulta mancante o incompleta.
- Investimenti in titoli appartenenti a società legate ad associazioni terroristiche, al fine di garantire un flusso di denaro come fonte di finanziamento.

3 Attività sensibili nell'ambito dei reati di riciclaggio, ricettazione e terrorismo

(Attività sensibili nell'ambito dei reati di riciclaggio, ricettazione e impiego di beni-denaro o altra utilità di provenienza illecita e dei reati con finalità di terrorismo o di eversione dell'ordine democratico)

Le aree di attività della Società più specificatamente a rischio riguardo le fattispecie di reato di riciclaggio, ricettazione e impiego di beni-denaro o altra utilità di provenienza illecita e di reati con finalità di terrorismo o di eversione dell'ordine democratico di cui trattasi sono le seguenti:

- Gestione contratti;
- Gestione commerciale;

4 I presidi e gli strumenti di controllo

4.1 Premessa

Nell'espletamento di tutte le attività attinenti l'identificazione e la conoscenza della clientela e/o dei soggetti per conto dei quali i clienti operano, oltre alle regole di cui al presente Modello, i dipendenti e i collaboratori di Cred.it Società Finanziaria SpA devono conoscere e rispettare:

- le norme di comportamento, i valori ed i principi etici enunciati nel Codice Etico;
- le procedure aziendali e di Gruppo, la documentazione e gli ordini di servizio inerenti la struttura gerarchico - funzionale aziendale ed organizzativa del Gruppo e il sistema di controllo della gestione;
- le circolari e le istruzioni operative emanate dalla funzione Antiriciclaggio di Gruppo;
- in generale, la normativa italiana e straniera applicabile.

4.2 Principi di comportamento

Come previsto dal Codice Etico, la Società profonde il massimo sforzo per il rafforzamento della cultura della legalità e, in particolare per la lotta al riciclaggio e al terrorismo, collaborando fattivamente con le Autorità preposte.

La presente Parte Speciale prevede l'espresso obbligo a carico dei Destinatari di:

- provvedere ad acquisire adeguata conoscenza della clientela, nella consapevolezza che la conoscenza della clientela è condizione essenziale per prevenire l'utilizzo del sistema finanziario a scopo di riciclaggio e l'instaurazione di rapporti con soggetti legati ad organizzazioni dedite ad attività terroristiche/eversive, nonché al fine di valutare e segnalare le operazioni sospette;
- garantire il rispetto delle leggi e delle regolamentazioni vigenti in ogni contesto geografico ed ambito operativo. In particolare per quanto attiene ai provvedimenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio, e le indicazioni operative per la segnalazione delle operazioni sospette.

In generale è fatto divieto di porre in essere qualsiasi attività tendente al riciclaggio, ricettazione ed impiego di denaro, beni o utilità di provenienza illecita o comunque tendente al finanziamento del terrorismo ed in particolare è fatto divieto di:

- acquistare ricevere od occultare denaro o cose provenienti da qualsiasi delitto al fine di procurare a se o ad altri un profitto, o comunque intromettersi nel farle, acquistare, ricevere od occultare;
- sostituire o trasferire denaro beni o altre utilità provenienti da delitto non colposo oppure compiere in relazione ad essi altre operazioni in modo da ostacolare l'identificazione della provenienza delittuosa;
- impiegare in attività economiche e finanziarie denaro beni o altre utilità provenienti da delitto.

In particolare i Destinatari devono provvedere a:

- evidenziare ed immediatamente segnalare le operazioni poste in essere da un soggetto in nome o a favore di terzi in assenza di legami familiari o relazioni commerciali idonee a giustificarle ovvero anche le operazioni poste in essere da soggetti terzi in favore di clienti in assenza di valide ragioni giustificatrici;
- astenersi dal compiere le operazioni individuate come sospette, tranne che l'astensione non sia possibile tenuto conto della normale operatività o possa ostacolare le indagini;
- bloccare o, comunque, non dare esecuzione ad operazioni che vedano coinvolti soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi);
- partecipare fattivamente al processo di analisi della clientela e della relativa attività per l'individuazione e la segnalazione di operazioni sospette, comunicando per iscritto ogni operazione, comportamento, anomalia, per qualsivoglia circostanza conosciuta a ragione delle funzioni esercitate, reputata suscettibile di valutazione ai fini di un eventuale avvio dell'iter di segnalazione come operazione sospetta.

4.3 Principi di controllo

Il sistema di controllo atto a prevenire i reati di riciclaggio, ricettazione e impiego di beni- denaro o altra utilità di provenienza illecita e reati con finalità di terrorismo o di eversione dell'ordine democratico si basa sui seguenti fattori:

– Ruoli e responsabilità definiti:

- o la procedura interna individua i soggetti e le Strutture responsabili dell'attivazione/gestione dell'iter di segnalazione delle operazioni sospette con riferimento alle istruzioni operative "Identificazione della Clientela, Registrazione e Segnalazione delle operazioni sospette" in ottemperanza al D.Lgs. 231/2007 (DIR 2005/60/CE).

– Segregazione dei compiti:

- o i soggetti in posizione apicale e quanti svolgono la propria attività nelle aree a rischio, monitorano le operazioni relative alla loro area di competenza, segnalando i movimenti sospetti al Responsabile Aziendale Antiriciclaggio;

- o il Responsabile Aziendale Antiriciclaggio svolge autonomamente le necessarie indagini sull'operazione sospetta, disponendo l'inoltro o meno delle segnalazioni alla competente Autorità in base alla materia oggetto di indagine.

– Attività di controllo:

- o ogni nuovo cliente è identificato sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente. Inoltre sono raccolte informazioni, mediante la compilazione di apposito questionario di adeguata verifica del cliente per la profilazione del rischio;

- o sono implementati controlli automatici di sistema sulla presenza di tutta la documentazione e le informazioni necessarie all'apertura di un nuovo rapporto;

- o sono effettuate verifiche sia manuali sia automatiche di sistema, sulla correttezza e completezza dei dati censiti in anagrafe che alimentano l'Archivio Unico Informatico, e sulla corretta acquisizione delle informazioni sull'attività economica svolta. Tali informazioni devono essere aggiornate, di volta in volta, in relazione alle motivazioni economiche sottostanti alle operazioni richieste o eseguite;

- o tutte le operazioni sono processate con modalità che consentano la registrazione procedurale nell'Archivio Unico Informatico con dati corretti e completi, anche avvalendosi di controlli automatici sulla qualità dei dati;

- o in occasione dell'identificazione del cliente e nel continuo, è verificata l'eventuale presenza del nominativo nelle versioni aggiornate delle liste antiterrorismo;

- o è istituita una apposita funzione aziendale a presidio della corretta esecuzione degli adempimenti di cui alle disposizioni di legge e di vigilanza in materia di contrasto finanziario al terrorismo.

– Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

- o tutta la documentazione relativa all'operatività e ai controlli periodici effettuati sulle posizioni relative ai clienti è sistematicamente archiviata presso le strutture operative di competenza.

Parte speciale 5: Reati informatici

PARTE SPECIALE 5

1 Funzione della Parte Speciale Quinta

La Parte Speciale sesta si riferisce ai comportamenti posti in essere dai Destinatari del Modello, ed in particolare dai soggetti coinvolti nelle attività sensibili riconducibili ai reati informatici, introdotti nel marzo 2008, a seguito di ratifica, da parte del Parlamento italiano, della “Convenzione del Consiglio d’Europa sulla criminalità informatica”.

Lo scopo preventivo è di particolare importanza dal momento che obiettivo primario della norma penale è, in questo caso, il potenziamento degli strumenti di tutela della sicurezza e della riservatezza dei dati e l’eventuale trattamento illecito degli stessi.

Obiettivo della presente Parte Speciale è che i suddetti soggetti adottino le presenti regole di condotta al fine di prevenire la commissione di tali reati.

In particolare, la presente Parte Speciale ha lo scopo di:

- indicare le procedure che i Destinatari del Modello sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all’OdV, e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

2 I reati informatici

(I reati informatici: esegesi delle norme rilevanti ed esemplificazioni di condotte illecite)

Il presente paragrafo si riferisce ai reati informatici, secondo le fattispecie contemplate dall’art. 24 bis del D.Lgs. 231/2001, limitatamente ai casi che potrebbero configurarsi in capo alla Società.

2.1 Falsità in un documento informatico

I reati in oggetto sono previsti da:

- Art. 491 bis del Codice Penale – Falsità in un documento informatico pubblico o privato

Fattispecie

- La fattispecie di reato si realizza se le falsità previste dagli articoli da 476 a 493 bis del Codice Penale (falsità in atti) riguardano un documento informatico pubblico o privato avente efficacia probatoria.

Esemplificazione di condotte illecite

- Utilizzo di firme digitali della società in modo abusivo o utilizzo di false firme.

2.2 Accesso abusivo e detenzione abusiva di codici di accesso

I reati in oggetto sono previsti da:

- Art. 615 ter del Codice Penale – Accesso abusivo ad un sistema informatico o telematico
- Art. 615 quater del Codice Penale – Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Fattispecie

- La fattispecie di reato si realizza nel caso di accesso abusivo ad un sistema informatico o telematico protetto da misure di sicurezza, o di permanenza contro la volontà espressa o tacita di chi ha il diritto di proibire l'accesso.
- La fattispecie di reato si realizza nel caso in cui, per procurare a sé o ad altri un profitto o di arrecare ad altri un danno si procurano, si riproducono, si diffondono, si comunicano o si consegnano codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque si forniscono indicazioni o istruzioni idonee a tale scopo.

Esemplificazioni di condotte illecite

- Un nuovo dipendente utilizza le password di accesso al sistema della società presso cui lavorava precedentemente per carpire informazioni utili alla Società.

2.3 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

I reati in oggetto sono previsti da:

- Art. 617 quater del Codice Penale - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Art. 617 quinquies del Codice Penale - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Fattispecie

- La fattispecie di reato si realizza nel caso di intercettazione, impedimento o interruzione fraudolenta di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi; il reato è procedibile a querela di parte, fatti salvi i casi in cui:
 - il reato sia commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
 - il reato sia commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso di poteri o con violazione di doveri inerenti alla sua funzione o il suo servizio.
- La fattispecie di reato si realizza nel caso d'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Esemplificazioni di condotte illecite

- Installazione di applicativi software all'interno dei personal computer aziendali o collegamento di dispositivi hardware alla rete aziendale per intercettare/impedire comunicazioni informatiche.

2.4 Danneggiamento

CRED.IT SOCIETÀ FINANZIARIA SPA

I reati in oggetto sono previsti da:

- Art. 635 bis del Codice Penale - Danneggiamento di informazioni, dati e programmi informatici
- Art. 635 ter del Codice Penale - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- Art. 635 quater del Codice Penale - Danneggiamento di sistemi informatici o telematici
- Art. 635 quinquies del Codice Penale - Danneggiamento di sistemi informatici o telematici di pubblica utilità

Fattispecie

- La fattispecie di reato si realizza nel caso in cui si distruggano, deteriorino o rendano, in tutto o in parte, inservibili sistemi informatici altrui, ovvero programmi, informazioni o dati altrui.
- La fattispecie di reato si realizza nel caso in cui si commetta un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere sistemi informatici o telematici, informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. E' prevista un'aggravante se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione dei sistemi informatici o telematici, delle informazioni, dei dati o dei programmi informatici.

Esemplificazioni di condotte illecite

- Alterazione del funzionamento di un sistema informatico o telematico dello Stato o di altro ente pubblico o dei dati in esso contenuti al fine di ottenere un vantaggio per la Società.

3 Attività sensibili nell'ambito dei reati informatici

I reati informatici possono potenzialmente essere commessi in ogni attività aziendale pertanto i principi di comportamento espressi nella presente Parte Speciale devono essere conosciuti e rispettati da tutti i dipendenti e i collaboratori della Società.

Le aree di attività sensibili della Società più specificatamente a rischio riguardo la fattispecie dei reati informatici di cui trattasi sono le seguenti:

- Gestione sistemi informativi.

La gestione dei sistemi informativi di Cred.it Società Finanziaria SpA è gestito in proprio attraverso sistema SIL AS 400 con licenza d'uso e contratto di manutenzione software con il fornitore TREBI s.r.l. installato su macchina di proprietà IBM AS400. Pacchetto di programmi per segnalazione ODV, Banca d'Italia e corrispondenza Centrale Rischi con licenze d'uso e contratto di manutenzione software con Nuova Trend s.r.l. L'infrastruttura di rete e servizi collegati vengono erogati dalla Capogruppo CRED.IT SOCIETÀ FINANZIARIA SPA Banca.

4 I presidi e gli strumenti di controllo

4.1 Premessa

Nell'espletamento di tutte le attività operative attinenti la gestione informatica della rete aziendale oltre alle regole di cui al presente Modello, i dipendenti e i collaboratori di Cred.it Società Finanziaria SpA devono

conoscere e rispettare:

- le norme di comportamento, i valori ed i principi etici enunciati nel Codice Etico;
- le procedure aziendali e di Gruppo, la documentazione e gli ordini di servizio inerenti la struttura gerarchico - funzionale aziendale ed organizzativa del Gruppo;
- in generale, la normativa italiana e straniera applicabile.

4.2 Principi di comportamento

I seguenti principi di carattere generale si applicano ai dipendenti in via diretta ed ai collaboratori in forza di apposite clausole contrattuali.

La presente Parte Speciale prevede l'esplicito obbligo a carico dei Destinatari di:

- utilizzare i personal computer per i soli ambiti inerenti all'attività lavorativa;
- utilizzare le unità di rete come aree di condivisione strettamente professionale;
- non usare né installare programmi distribuiti da chi non ne è ufficialmente preposto, né mezzi di comunicazione propri, salvo esplicita autorizzazione della Direzione Servizi Informatici;
- non modificare le configurazioni impostate sul proprio personal computer;
- non utilizzare software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non accedere in maniera non autorizzata ai sistemi informativi della Pubblica Amministrazione o di terzi per ottenere e/o modificare informazioni a vantaggio della Società.

4.3 Principi di controllo

Il sistema di controllo a presidio dei reati informatici si basa sui seguenti fattori:

- Ruoli e responsabilità definiti:
 - la gestione delle abilitazioni avviene tramite la definizione di "profili abilitativi", ai quali corrispondono le necessarie abilitazioni in ragione delle funzioni svolte all'interno di Cred.it Società Finanziaria SpA;
 - le variazioni al contenuto dei profili sono eseguite dalla Direzione Servizi Informatici, su richiesta delle Strutture interessate, che devono garantire la corrispondenza tra le abilitazioni informatiche richieste e le mansioni lavorative coperte;
 - ogni utente ha associato un solo profilo abilitativo in relazione al proprio ruolo aziendale; in caso di trasferimento o di modifica dell'attività dell'utente, viene attribuito il profilo abilitativo corrispondente al nuovo ruolo assegnato.
- Segregazione dei compiti:
 - le attività di implementazione e modifica dei software, gestione delle procedure informatiche, controllo degli accessi fisici, logici e della sicurezza del software sono demandate alla Direzione Servizi Informatici, a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informativi da parte degli utenti.
- Attività di controllo:
 - le attività di gestione ed utilizzo di sistemi informativi di Cred.it Società Finanziaria SpA sono soggette ad attività di controllo a garanzia della tracciabilità delle modifiche apportate alle procedure informatiche, della rilevazione degli utenti che hanno effettuato tali modifiche e di coloro che hanno effettuato i controlli sulle modifiche apportate. Le principali attività di controllo previste dalle policy interne in materia di sicurezza informatica sono le seguenti:
 - utilizzo di password al fine di limitare gli accessi al sistema e di controllare gli accessi alle applicazioni;
 - sistematico monitoraggio degli accessi e dell'utilizzo delle risorse da parte degli utenti dei sistemi informatici;

CRED.IT SOCIETÀ FINANZIARIA SPA

- protezione dei server e delle postazioni di lavoro della Società attraverso l'utilizzo di sistemi anti-intrusione e di software antivirus costantemente aggiornati;
 - esecuzione di operazioni di backup periodico dei dati;
 - predisposizione di specifici ambienti informatici per lo sviluppo ed il test del software distinti dall'ambiente di produzione utilizzato dagli utenti;
 - installazione del software nelle postazioni di lavoro e nei server solo a cura di soggetti dotati di specifiche abilitazioni.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
- il processo decisionale, con riferimento all'attività di gestione e utilizzo di sistemi informatici, è garantito dalla completa tracciabilità a sistema;
 - tutte le operazioni correttive effettuate tramite sistema (ad esempio rettifiche contabili, variazioni dei profili utente, etc.) sono tracciabili attraverso sistematica registrazione degli eventi (sistema di log files);
 - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna Funzione è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta, anche in via telematica o elettronica.

Parte speciale 6: Le nuove fattispecie di reato in materia di tutela della salute e della sicurezza sul lavoro

PARTE SPECIALE 6

1 Funzione della Parte Speciale Sesta

La Parte Speciale settima si riferisce ai comportamenti posti in essere dai Destinatari del Modello, ed in particolare dai soggetti coinvolti nelle attività sensibili rispetto ai reati introdotti dapprima con Legge 123/07 e poi risistemati e riorganizzati dal T.U. 81/08.

Lo scopo preventivo è di particolare importanza dal momento che obiettivo primario della norma penale è, in questo grado, il potenziamento degli strumenti di tutela della salute e della sicurezza dei lavoratori.

Obiettivo della presente Parte Speciale è che i suddetti soggetti, anche se in questo caso particolare il riferimento è più circoscritto ai soggetti in posizione apicale e a pochi sottoposti ben individuati (vedasi ad esempio il responsabile del Servizio di Prevenzione e Protezione) adottino le presenti regole di condotta al fine di prevenire la commissione di tali reati.

In particolare, la presente Parte Speciale ha lo scopo di:

- indicare le procedure che i Destinatari del Modello sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'OdV, e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

2 Le nuove fattispecie in materia di tutela della salute e della sicurezza sul lavoro

[\(Le nuove fattispecie in materia di tutela della salute e della sicurezza sul lavoro \(D.Lgs. 81/2001\): esegesi delle norme rilevanti ed esemplificazioni di condotte illecite\)](#)

Il presente paragrafo si riferisce ad esempi di reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 septies del D.Lgs. 231/2001), limitatamente ai casi che potrebbero configurarsi in capo ad Cred.it Società Finanziaria SpA.

I reati in oggetto sono previsti da:

- Art. 589 Codice Penale – Omicidio colposo
- Art. 590 Codice Penale – Lesioni personali colpose

Fattispecie

– La fattispecie di reato di omicidio colposo si ipotizza nel caso si cagioni per colpa la morte di una persona; è prevista un'aggravante se l'evento è provocato con violazione delle norme per la prevenzione degli infortuni sul lavoro.

– La fattispecie di reato di lesioni personali colpose si realizza nel caso in cui si cagioni ad altri, per colpa, una lesione personale; se la lesione è grave o gravissima e l'evento è cagionato con violazione delle norme per la prevenzione degli infortuni sul lavoro le pene previste sono ulteriormente aggravate.

Di fatto sono state inserite nel D.Lgs. 231/01 due fattispecie delittuose a natura colposa che, però, assumono particolare rilievo per la natura del bene giuridico tutelato, cioè la salute e l'integrità fisica del lavoratore.

A tutela del suddetto bene giuridico l'ordinamento, oltre alla normativa dettata in materia antinfortunistica, appronta anche ulteriori presidi, identificati nell'articolo 2087 del Codice Civile, il quale

prevede che l'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.

E' necessario precisare che, affinché si parli di responsabilità dell'ente, il reato deve essere commesso nell'interesse o a vantaggio dell'ente stesso.

Esemplificazioni di condotte illecite

- Malattia professionale (ad esempio diminuzione della capacità visiva) dovuta all'ambiente di lavoro non ergonomico che non rispetta i requisiti di legge.
- Incidenti sui cantieri di manutenzione ordinaria e straordinaria causati dal mancato controllo di regolarità sui dipendenti delle imprese appaltatrici, in materia di tutela della salute e della sicurezza sul lavoro.

3 Attività sensibili nell'ambito dei reati in materia di tutela della salute e della sicurezza sul lavoro

La tutela della salute e sicurezza sul lavoro coinvolge tutte le attività aziendali, ne consegue che tutti i dipendenti e i collaboratori della Società sono tenuti ad osservare i principi di comportamento sotto enunciati, per quanto di loro competenza. In particolare, l'area di attività sensibili di Cred.it Società Finanziaria SpA più specificatamente a rischio riguardo le fattispecie di reato di omicidio colposo e di lesioni personali colpose di cui trattasi è la Gestione salute e sicurezza sul lavoro.

Le attività di gestione della salute e della sicurezza sul lavoro sono affidate in outsourcing a CRED.IT SOCIETÀ FINANZIARIA SPA; pertanto i principi di comportamento e controllo derivano dal Modello di CRED.IT SOCIETÀ FINANZIARIA SPA, fermo restando il dovere di Cred.it Società Finanziaria SpA di monitorare costantemente il rispetto, da parte dell'outsourcer, delle condizioni contrattuali prestabilite e rilevare periodicamente il livello di servizio offerto.

4 I presidi e gli strumenti di controllo

4.1 Premessa

Nell'espletamento delle proprie attività lavorative, i Destinatari del Modello devono conoscere e rispettare:

- le disposizioni di legge in materia di salute e sicurezza dei lavoratori sui luoghi di lavoro disciplinate dal Testo Unico sicurezza sul lavoro (D.Lgs. 81/2008);
- la normativa in materia di salute e sicurezza nei cantieri temporanei o mobili contenuta nel D.Lgs. 494/1996;
- le procedure aziendali e di Gruppo, la documentazione e gli ordini di servizio inerenti la struttura gerarchico - funzionale aziendale ed organizzativa del Gruppo;
- in generale, la normativa italiana e straniera applicabili.

4.2 Principi di comportamento

La presente Parte Speciale prevede l'obbligo a carico dei Destinatari del Modello di:

- osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dalle strutture aziendali e dalle Autorità competenti;
- utilizzare correttamente le attrezzature di lavoro e i dispositivi di sicurezza;
- prendere visione del materiale informativo messo a disposizione dalla Società e partecipare attivamente alle attività formative in materia di sicurezza sul lavoro;
- sottoporsi alle visite mediche periodiche;
- segnalare immediatamente al Responsabile e/o agli addetti alla gestione delle emergenze, ogni situazione di pericolo potenziale o reale, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre tale situazione di pericolo.

La presente Parte Speciale prevede inoltre l'obbligo a carico delle Strutture responsabili per la Sicurezza dei Lavoratori di:

- assicurare, per quanto di competenza, gli adempimenti in materia di sicurezza e salute dei lavoratori sul luogo di lavoro osservando le misure generali di tutela e valutando la scelta delle attrezzature di lavoro nonché la sistemazione dei luoghi di lavoro;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia di salute e sicurezza sul lavoro, prevedere che i contratti con tali soggetti contengano apposita dichiarazione di conoscenza della normativa di cui al D.Lgs. 231/2001 e di impegno al suo rispetto;
- astenersi dall'affidare incarichi a eventuali consulenti esterni eludendo criteri documentabili ed obiettivi incentrati su professionalità qualificata, competitività, utilità, prezzo, integrità, solidità e capacità di garantire un'efficace assistenza continuativa. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza;
- adottare una condotta trasparente e collaborativa nei confronti degli enti preposti al controllo (es. Ispettorato del Lavoro, A.S.L., Vigili del Fuoco, etc.) in occasione di accertamenti/procedimenti ispettivi;
- provvedere, nell'ambito dei contratti di somministrazione, appalto e fornitura, a elaborare ed applicare le misure atte a governare in sicurezza le eventuali interferenze fra le imprese compresi gli eventuali lavoratori autonomi;
- favorire e promuovere l'informazione e formazione interna in tema di rischi connessi allo svolgimento delle attività, misure ed attività di prevenzione e protezione adottate, procedure di pronto soccorso, lotta antincendio ed evacuazione dei lavoratori;
- curare il rispetto delle normative in tema di salute e sicurezza nell'ambito dei contratti di appalti di forniture, di servizi o d'opere nonché di quelli regolati dal D.Lgs. 276/2003, e successive modifiche ed integrazioni (legge Biagi).

4.3 Principi di controllo

Il sistema di controllo a presidio dei reati in materia di tutela della salute e della sicurezza sul lavoro si basa sui seguenti fattori:

- Ruoli e responsabilità definiti:
 - il sistema di gestione aziendale prevede la definizione di specifiche responsabilità e procedure al fine di consentire la piena attuazione della politica di salute e sicurezza sul lavoro con un approccio sistematico e pianificato.
- Segregazione dei compiti:
 - le strutture operative che hanno il compito di realizzare e di gestire gli interventi (di natura immobiliare, informatica, di sicurezza fisica, ovvero attinenti ai processi di lavoro e alla gestione del personale), sono distinte e separate dalla struttura alla quale sono attribuiti compiti di consulenza in tema di valutazione dei rischi e di controllo sulle misure atte a prevenirli e a ridurli;
 - le strutture competenti designano i soggetti ai quali sono attribuite specifiche mansioni per la gestione/prevenzione dei rischi per la sicurezza e la salute sul lavoro;
 - i Rappresentanti dei Lavoratori per la Sicurezza collaborano attivamente col Datore di Lavoro al fine di segnalare criticità ed individuare le conseguenti soluzioni.

CRED.IT SOCIETÀ FINANZIARIA SPA

– Attività di controllo:

- la struttura competente per la gestione della sicurezza sul lavoro provvede ad attivare un piano aziendale di controllo sistematico al fine di verificare la corretta gestione delle procedure e delle misure messe in atto per valutare, in ottemperanza alle prescrizioni di legge, i luoghi di lavoro. Il piano, in particolare, definisce le aree e le attività aziendali da verificare, le modalità di esecuzione delle verifiche, le modalità di rendicontazione;
 - la struttura competente per la gestione della sicurezza sul lavoro controlla che tutte le misure di prevenzione e protezione programmate siano attuate, assicurando un costante monitoraggio delle situazioni di rischio e dell'avanzamento dei programmi di intervento previsti dagli specifici documenti di valutazione dei rischi. Tale struttura si avvale, laddove occorra, della collaborazione della struttura deputata alla gestione delle risorse umane, nonché delle strutture di gestione e realizzazione di interventi immobiliari, di progettazione e gestione dei processi lavorativi, della sicurezza fisica e dei sistemi informativi;
 - i Rappresentanti dei Lavoratori per la Sicurezza, nel rispetto delle norme di legge in materia, possono accedere alla documentazione aziendale inerente la valutazione dei rischi e le misure di prevenzione relative e chiedere informazioni al riguardo. I medesimi Rappresentanti possono accedere ai luoghi di lavoro e formulare osservazioni in occasione di visite e verifiche da parte delle Autorità competenti;
 - tutti gli ambienti di lavoro sono visitati e valutati da soggetti in possesso dei requisiti di legge e di adeguata formazione tecnica. Il Medico Competente visita i luoghi di lavoro ove sono presenti lavoratori esposti a rischi specifici ed effettua a campione sopralluoghi negli altri ambienti;
 - figure specialistiche di alta professionalità e con i titoli ed i requisiti previsti dalle norme specifiche, contribuiscono alla valutazione ed alla elaborazione di misure di tutela nei cantieri temporanei e mobili (Responsabili dei lavori, Coordinatori per la Sicurezza, Direttori dei lavori etc.);
 - le competenti strutture individuate dal Datore di Lavoro/Committente provvedono alla verifica dell'idoneità tecnico-professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
- la struttura competente per la gestione della sicurezza sul lavoro è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo della gestione dei rischi in materia di sicurezza e salute dei lavoratori nonché della relativa attività di controllo;
 - la documentazione sanitaria (con il rispetto dei requisiti di riservatezza previsti dalla normativa) e le attività di formazione ed informazione sono tracciate mediante l'utilizzo di appositi sistemi informativi.

Allegato 1

ALLEGATO 1

1 Elenco reati ex D.Lgs. 231/2001

1.1 Reati contro la Pubblica Amministrazione

- Malversazione a danno dello Stato – art. 316 bis c.p.
- Indebita percezione di erogazioni a danno dello Stato – art. 316 ter c.p.
- Truffa – art. 640 c.p., comma 2, n. 1 – rilevante ai fini del D.Lgs. 231/2001 solo se commesso in danno dello Stato o di altro ente pubblico e limitatamente al comma 2, n. 1.
- Truffa aggravata per il conseguimento di erogazioni pubbliche – art. 640 bis c.p.
- Frode informativa – art. 640 ter c.p. – rilevante ai fini del D.Lgs. 231/2001 solo se commesso in danno dello Stato o di altro ente pubblico.
- Concussione – art. 317 c.p.
- Corruzione per atto d'ufficio – art. 318 c.p.
- Corruzione per un atto contrario ai doveri d'ufficio – art. 319 c.p.
- Circostanze aggravanti – art. 319 bis c.p.
- Corruzione in atti giudiziari – art. 319 ter c.p.
- Corruzione di persona incaricata di un pubblico servizio – art. 320 c.p.
- Pene per il corruttore – art. 321 c.p.
- Istigazione alla corruzione – art. 322 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.

1.2 Reati di falsità in monete

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate – 453 c.p.
- Alterazione di monete – 454 c.p.
- Spendita o introduzione nello Stato, senza concerto, di monete falsificate – 455 c.p.
- Spendita di monete falsificate ricevute in buona fede – 457 c.p.
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati – 459 c.p.
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo – 460 c.p.
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata – 461 c.p.
- Uso di valori di bollo contraffatti o alterati – 464 c.p.

1.3 Reati societari

- False comunicazioni sociali – art. 2621 c.c.
- False comunicazioni sociali in danno dei soci o dei creditori – art. 2622 c.c.
- Falsità nelle relazioni o nelle comunicazioni delle Società di Revisione – art. 2624 c.c.
- Impedito controllo – art. 2625 c.c., comma 2.
- Indebita restituzione dei conferimenti – art. 2626 c.c.

- Illegale ripartizione degli utili e delle riserve – art. 2627 c.c.
- Illecite operazioni sulle azioni o quote sociali o della società controllante – art. 2628 c.c.
- Operazioni in pregiudizio dei creditori – art. 2629 c.c.
- Omessa comunicazione del conflitto d'interessi – art. 2629 bis c.c.
- Formazione fittizia del capitale – art. 2632 c.c.
- Indebita ripartizione dei beni sociali da parte dei liquidatori – 2633 c.c.
- Illecita influenza sull'assemblea – art. 2636 c.c.
- Aggiotaggio – art. 2637 c.c.
- Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza – art. 2638 c.c.
- Falso in prospetto – art. 173 bis T.U.F.

1.4 Reati aventi finalità di terrorismo o di eversione ordine democratico

- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico – art. 270 bis c.p.
- Attentato per finalità terroristiche o di eversione – art. 280 c.p.
- Sequestro di persona a scopo terroristico o di eversione – art. 289 bis c.p.
- Pratiche di mutilazione degli organi genitali femminili – art. 583 bis c.p.

1.5 Reati contro la personalità individuale

- ⊗ Riduzione o mantenimento in schiavitù o in servitù – art. 600 c.p.
- ⊗ Tratta di persone – art. 601 c.p.
- ⊗ Acquisto e alienazione di schiavi – art. 602 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.
- ⊗ Iniziative turistiche volte allo sfruttamento della prostituzione minorile – art. 600 quinquies c.p.
- ⊗ Pornografia virtuale – art. 600 quater 1 c.p.

1.6 Reati di market abuse

- ⊗ Abuso di informazioni privilegiate – art. 184 T.U.F.
- ⊗ Manipolazione del mercato – art. 185 T.U.F.

1.7 Reati transnazionali

- ⊗ Si parla di reato transnazionale qualora sia coinvolto un gruppo criminale organizzato nonché:
 - a) sia commesso in più di uno stato;
 - b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;
 - c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
 - d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.
- ⊗ 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 quater T.U. 23 gennaio 1973, n. 43.

✂ Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope – art. 74 T.U. 9 ottobre 1990, n. 309.

✂ Disposizioni contro le immigrazioni clandestine – art. 12 T.U. 25 luglio 1998, n. 286.

² L'art. 25 quater, a differenza degli altri articoli del Decreto, non prevede un numero tipizzato ex ante di delitti ma si limita a fare rinvio per la loro individuazione al codice penale, alle leggi speciali, alla Convenzione di New York contro il terrorismo del 9 dicembre 1999. L'elenco riportato è meramente esemplificativo.

✂ Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria – art. 377 bis c.p.

✂ Favoreggiamento personale – art. 378 c.p.

1.8 Reati di omicidio colposo e lesioni colpose gravi o gravissime

(Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro)

✂ Omicidio colposo – art. 589 c.p.

✂ Lesioni personali colpose – art. 590 c.p.

1.9 Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza

Illecita

✂ Ricettazione – art. 648 c.p.

✂ Riciclaggio – art. 648 bis c.p.

✂ Impiego di denaro, beni o utilità di provenienza illecita – art. 648 ter c.p.

1.9 Reati informatici

✂ 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 quater c.p.

✂ 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 quater 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.

1.10 Delitti di criminalità organizzata

✂ Associazione per delinquere – art. 416 c.p., ad eccezione del sesto comma.

✂ Associazione per delinquere – art. 416 c.p., ad eccezione del sesto comma

- ⌘ Associazione a delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 d. lgs 286/1998 – art. 416, sesto comma, c.p.
- ⌘ Associazione di tipo mafioso – art. 416-bis c.p.
- ⌘ Scambio elettorale politico-mafioso – art. 416-ter c.p.
- ⌘ Sequestro di persona a scopo di estorsione – art. 630 c.p.
- ⌘ Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope – art. 74 DPR 9
- ⌘ 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 sparo³⁾ – art. 407, co. 2, lett. a), numero 5), c.p.p.

1.11 Delitti contro l'industria e il commercio

- ⌘ 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.
- ⌘ Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale – art. 517-ter c.p.
- ⌘ Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari – art. 517-quater c.p.
- ⌘ Illecita concorrenza con minaccia o violenza” – art. 513-bis c.p.
- ⌘ Frodi contro le industrie nazionali – art. 514 c.p.

1.12 Delitti in materia di violazione del diritto d'autore

- ⌘ Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa – art. 171, l. 633/1941 comma 1 lett a) bis
- ⌘ Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione – art. 171, l. 633/1941 comma 3
- ⌘ Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o 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 programmi per elaboratori – art. 171-bis l. 633/1941 comma 1
- ⌘ Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati – art. 171-bis l. 633/1941 comma 2
- ⌘ Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente 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 o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa – art. 171-ter l. 633/1941
- ⌘ Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione – art. 171-septies l. 633/1941

³⁾ (*) Escluse quelle denominate «da bersaglio da sala», o ad emissione di gas, nonché le armi ad aria compressa o gas compressi, sia lunghe sia corte i cui proiettili erogano un'energia cinetica superiore a 7,5 joule, e gli strumenti lanciarazzi, salvo che si tratti di armi destinate alla pesca ovvero di armi e strumenti per i quali la "Commissione consultiva centrale per il controllo delle armi" escluda, in relazione alle rispettive caratteristiche, l'attitudine a recare offesa alla persona.

⌘ Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo 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 – art. 171-octies l. 633/1941

1.13 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci

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

Allegato 2

ALLEGATO 2

1 Regolamento dell'Organismo di Vigilanza

Spetta allo stesso OdV procedere, fra i suoi componenti, alla nomina di un membro con funzioni di Presidente e di un membro con funzioni di Segretario.

L'OdV si riunisce con cadenza almeno trimestrale, su convocazione del Presidente. E' inoltre convocato dal Presidente ogniqualvolta il medesimo ne ravvisi la necessità, nel luogo fissato, a mezzo di apposito avviso trasmesso a tutti i componenti, nonché in caso di richiesta anche di uno solo dei suoi componenti ovvero di uno degli altri organi sociali quali il Collegio Sindacale o il Consiglio di Amministrazione.

La convocazione è effettuata con un preavviso di almeno tre giorni, salvo il caso d'urgenza, mediante comunicazione scritta che riporta gli argomenti posti all'ordine del giorno ed è corredata dalle informazioni necessarie per la discussione. Per la validità della costituzione di ogni seduta, occorre la presenza di almeno due membri su tre.

Il Presidente ed il Segretario redigono e sottoscrivono i verbali delle riunioni che vengono conservati a cura del Segretario in ordine cronologico. Le deliberazioni sono prese a maggioranza assoluta di voti. L'assenza ingiustificata per più di due riunioni consecutive comporta la decadenza dalla carica.

Alle adunanze dell'OdV possono partecipare, con funzione informativa e consultiva, altri soggetti (Responsabile Divisione Internal Auditing, membri del Comitato di Controllo Interno, membri del Collegio Sindacale, Società di Revisione, etc.) qualora espressamente invitati dall'OdV.

I verbali degli incontri dell'OdV devono essere custoditi dall'OdV stesso. Tutte le segnalazioni, informazioni e relazioni previste nel Modello vengono conservate dall'OdV per un periodo di 10 anni in un apposito archivio, il cui accesso è consentito esclusivamente all'OdV stesso.



Cred.it Società Finanziaria SpA

Sede Legale e Direzione Generale: Via Frattina, 89 – 00187 Roma

Tel. 06.92946211 / Fax 06.92931763

Sede Amministrativa: Via Carmine Vecchio, 50 – 71036 Lucera (FG) – Tel. 0881/524210 Fax 0881/526819

www.creditspa.it – cred.itspa@legalmail.it – Iscritta nel Registro delle Imprese di Roma

P.iva: 10954791009 – Capitale Sociale € 6.000.000,00 di cui sottoscritto e versato € 3.000.000,00

Iscritta nell'elenco generale T.U.B. presso la Banca d'Italia al n°41964 del 16/03/2011

Codice ABI: 33667.7